Parliamentary Joint Committee on the Australian Crime Commission

Inquiry Into Cybercrime

Submission No:12A
Received 18 July 2003
Mr Scott Pobihun
Manager
Investigations & Forensic Services
PricewaterhouseCoopers
53 Blakall Street
BARTON ACT 2607
☎02 6271 9342 🗎
E-mail:
scott.pobihun@au.pwcglobal.com

πωχ

Submission to the Cybercrime Inquiry of the Parliamentary Joint Committee on the Australian Crime Committee

May 2003

Contents

Introduction

This submission is provided by PricewaterhouseCoopers (PwC) in response to an invitation by the Parliamentary Joint Committee for all interested parties to make submissions regarding recent trends in practices and methods of cybercrime. PwC is the world's largest professional services organisation. Drawing on the knowledge and skills of more than 125,000 people in 142 countries, we build relationships by providing services based on quality and integrity. PwC has regular dealings with all facets of industry across many sectors both public and private. We regularly provide hi-tech investigative services to both federal and state law enforcement agencies and departments as well as to private sector corporate clients from banking and finance to legal, manufacturing, retail and others.

This submission seeks to assist the inquiry by identifying recent developments in cybercrime. We provide you with results of our Global Survey on Economic Crime and comment upon the information technology investigations for which we have been engaged in the Asia Pacific region.

We are pleased to provide this submission and hope it provides the appropriate assistance and adequate information. If you have any queries relating to our submission then please do not hesitate to contact us.

Your faithfully

Graham Henley

Graham Henley Director Investigations & Forensic Services	Scott Pobihun Manager Investigations & Forensic Services
Sydney, NSW	***Canberra, ACT***

Who are PricewaterhouseCoopers Investigative & Forensic Services?

This submission has been developed by PricewaterhouseCoopers Australian Investigations and Forensic Services (IFS) team. The IFS is a national team with members in capital cities across Australia and the Asia Pacific region. The nature of our services facilitates multi-disciplined investigations, often combining members from diverse employment and academic backgrounds. Given the nature of investigative work and the global economy, the IFS team has a national and international response capacity

IFS attends to a diverse client base including public and private sector clients such as banks, international corporations and law enforcement agencies. Our IFS specialists provide for a variety of services including:

- Fraud Investigation
- Computer Forensics and Electronic Investigations
- Fraud Prevention and Control
- Forensic Accounting
- Suspicious Transaction Analysis

In the region our Computer Forensics and Electronic Investigations team comprises of members in Sydney, Melbourne, Brisbane, Canberra, Hong Kong Jakarta and New Zealand. The team also regularly communicates with it's colleagues outside of the Asia Pacific region including specialists in the United Kingdom, the United States and South Africa. Like all of the IFS team, the Computer Forensic team often is called upon to quickly respond to incidents which can involve extra-territory travel.

Some of our Computer Forensic specialists have come from a law enforcement background but we also employ specialist individuals with Legal and Accounting backgrounds. The team often undertake investigations into incidents which involve the use of computers, including Corporations law infringement and Corporate disputes, Employment Law, Piracy and Criminal law including Cybercrime offences covered by the terms of this Inquiry

Our team is well known for its capacity to quickly react to the demands of our clients anywhere within the region.

Outline of our Submission

We have broken our submission down into the following sections to facilitate ease of use:

Section 1: Trends & Techniques in Cybercrime

We understand the Inquiry wishes to develop an understanding of recent trends in cybercrime. We therefore provide the Inquiry with recent developments which we have been made aware of through our own research and through our experience in investigating cybercrime. We break them down into four broad areas which we discuss in detail. We provide a more in depth description of each of these methods through Appendix A which is attached to this submission.

Section 2: The Investigative Response To Cybercrime

In this section we discuss briefly the legislative framework affecting our investigations and we provide suggestions as to the effective investigation of cybercrime and the importance of proper investigative techniques.

Section 3: Our Research

PricewaterhouseCoopers has recently released the results of its 2003 Global Economic Crime Survey. We identify the key results as they relate to cybercrime in the Asia Pacific region.

Section 4: Experience Gained From Our Investigations

We then provide the Inquiry with information relating to our experience in investigating cybercrime, particularly relating to access or distribution of child pornography as well as investigations into online fraud.

Section 1: Cybercrime Techniques

A number of factors assist the commission of unlawful conduct upon the Internet and also influence the ability to positively identify an offender. Broadly speaking, these methods and techniques can be categorised into four broad areas:

(i) Anonymous User Activity
(ii) Social Engineering and Deception
(iii) System Exploits

(i) Anonymous User Activity

Anonymous Internet Use

With the rapid population of the online environment has come the increased demand by those who inhabit it to protect their privacy. This demand has arisen from the Internet's very nature. TCP/IP technology, the method which computers communicate within the Internet, presently provides for an unsecured path which can permit an individual user's activities being observed and recorded. Whilst this is very useful in investigations, the common user who is simply traversing the Internet may be left exposed to malicious attacks.

There are a variety of techniques which both the skilled and inexperienced computer user has at their disposal to protect their identity on-line. These range from advanced techniques of accessing the on-line environment through virtual private networks to the use of Internet cafes and web based Internet email facilities such as "hotmail". There are many legitimate reasons why an individual may be interested in doing this, including:

- the protection of their privacy
- the protection of their method of accessing the on-line environment to reduce the chances of their computer being maliciously attacked, and
- to prevent personal information from being accessed by spammers or those seeking to undertake identity theft.

There are also a variety of reasons why an individual may want to utilise such facilities to carry out unlawful conduct upon the web including:

- surf the Internet to access or disseminate inappropriate material such as paedophilic pornography or illegal software such as credit card key generators or pirated software
- use malicious tools against other computers with the reduced likelihood of being caught
- dissemination of slanderous or misleading material, and
- promoting other techniques for social engineering purposes.

Internet technology allows perpetrators to hide their identity relatively easily. This therefore reduces the capability of investigators to adequately obtain evidence to connect an individual's conduct to an unlawful event. Eventually, before either a civil or criminal Court, it will be the task of the investigator to tie the fingers of the offender to the unlawful activity on the computer keyboard.

Anonymous Payment Systems

In recent investigations we have seen the use of private secure offshore payment systems (such as www.evocash.com) to facilitate transactions for unlawful purposes and also to launder ill-gotten gains. Such companies operate entirely out of Australian jurisdiction and control.

Anonymous Computer Use, Data Wiping & Encryption

In our investigations we have seen a steady increase in the use by suspects of Data Wiping tools to permanently erase evidence. The regular operation of computers causes information to be left on the computer's hard drive. For example, information remains even after a document is placed in the 'Recycler' or if a file is deleted. Data can only be considered destroyed once it is physically over-written by other data.

A common way in which data is recovered in a forensic examination of a computer is by analysing the 'unallocated' space upon a hard drive. If data is deleted by the operating system, be it by a user's instruction or otherwise, it is identified as no longer being required by the system and the space which this data occupies returns to an 'unallocated' state. Whilst the data remains in that space, the computer considers that space available for writing to in the future. Drive-wiping software permits the writing of either random data or a particular character or string of characters to a certain area of the hard drive or the entire hard drive. This way a user can effectively erase the contents of a drive. A simpler form may be used by individuals to remove information relating to their Internet activity. This complicates forensic examination as it increases the chances of destroying evidence of a user's inappropriate activity on the Internet.

In addition to this we have seen an increase in the use of strong file encryption. Whilst a vital tool for legitimate business purposes, the strong and cost effective encryption software available to individuals makes it an attractive tool for cyber criminals. We appreciate that recent legislation in the Cybercrime Act moves to address this issue in regard to police powers of search.

(ii) Social Engineering and Deception

Cybercrime is not necessarily 'new' crime. Cybercrime may be old style scams which make use of the Internet as a marketing and contact tool. Typical Internet related frauds include investment frauds, secret market frauds and 'pyramid schemes' where the Internet is used as a new medium to attract a victim, and that hapless victim is persuaded to part with money or credit card details. Many of the frauds that are prevalent on the Internet involve the offering of unrealistically high returns on investment. Secret market frauds are a variation on this theme. Victims are persuaded that there is a confidential and exclusive market for a particular kind of fictitious financial instrument, such as a “prime bank guarantee”, which offers high rates of return. Pyramid schemes again offer high returns for small contributions and invariably collapse leaving the last to join without prospect of recovering any funds.

The Internet exhibits some characteristics which make it attractive to someone wishing to exploit other people:

- it is largely unregulated in so far as who may set up a site. No licence fees are payable to any central authority and no form of vetting is, or in practical terms ever could be, carried out on those persons or entities setting up sites

- an Internet site can be set up anywhere in the world at very low cost and can reach anywhere else in the world at low cost. This means that fraudsters now have "global reach" and can access a far larger market of potential victims than ever before. As fraudsters are always looking for new victims, this is a very attractive feature

- an impressive site with links to established companies or financial institutions may be no more than an empty shell designed to attract and trap the unwary. There is often no easy way of separating the genuine from the false

- the glamour and novelty of the Internet and the spurious credibility claimed by a web site may cause otherwise prudent investors to become involved in fraudulent schemes, and

- a site may, and probably will, operate outside the legal jurisdiction of the country in which the victim of the fraud resides. In some circumstances, a company may give the impression that it is an Australian company through it’s Internet website but may have absolutely no legal or commercial connection with our jurisdiction. In many cases law enforcement agencies will not investigate cross jurisdictional matters due to these difficulties.

The above factors make it extremely difficult to discover, in sufficient time to effect recovery or at all, the identity of a fraudulent web site operator.

Internet related fraud can go as far as the establishment of ‘phoney’ banks in tax havens such as the British Virgin Islands and Cayman Islands. These banks can have very sophisticated marketing campaigns, web sites and so on, which attract depositors with promises of very high rates of return. Such scams reflect the old style “Ponzi” scheme fraud, where initial investors returns are paid from new investors funds, attracting further investment, until such time as the scam operators disappear with depositors funds.

These types of Internet related scams reflect one of the main differences between Internet fraud and traditional fraud – the success of Internet fraud, and the difficulty associated with its ultimate investigation, is reliant upon the anonymity of the fraudster. Traditional fraud relies upon the fraudster’s success in covering up his activities. Internet fraud is far more brazen, however its success lies in the relative anonymity of its perpetrators.

More often than not, our investigations relating to cybercrime indicate that individuals have undertaken social-engineering using the Internet. There are a variety of techniques which one can implement to obtain unlawful gains via the Internet. These include:

- SPAM e-mail such as the original Nigerian Letter technique
- Bulletin Board or Chat postings of misleading information to influence capital markets
- Web Page diverting.

These scamming techniques are very much old techniques dressed up in new electronic guises.

Spam Scams & Phoney Websites

Recently the Sydney Morning Herald reported that a US based group had sent spam email to individuals requesting they access the Commonwealth Bank's Netbank website asking them to update their account details.

In such circumstances individuals can be deceived by being requested to access a seemingly legitimate website. In most cases such activity can only be investigated on a reactive basis as it is virtually impossible to identify these websites prior to the relevant authorities being notified of its existence due to the vastness of the Internet.

Web-page diversion – hijacking

It is possible for users to be inadvertently diverted to another website should that website be modified. Whilst it is common practice in the corporate environment where a company may own multiple domain names (for example www.pwcglobal.com.au will divert you to www.pwcglobal.com through www.pwcglobal.com/au where the Australian information will be displayed to you.). There are circumstances though where websites are 'hijacked' – techniques are available whereby individuals may enter an authentic URL (such as www.pwcglobal.com) but will be diverted to an illegitimate website instead. This may be consequential and may not damage the user in the instance significantly if they were attempting to enter the PricewaterhouseCoopers website, however if they intended to enter their bank's online services and were misled into thinking they were doing so then that user will have exposed their personal banking details to the individuals who administer the fake website.

Cookie Exploits

Individuals may also have their personal information accessed through the accessing of websites. Often websites use a small piece of information called a cookie to identify users and to set viewing preferences accordingly. Often cookies are used in an appropriate manner however cookies can be used to enable foreign systems to obtain information about a user so as to put them on spam mailing lists or track their activity across a broad range of topics including banking activity which could lead to identity theft.

(iii) IT System Exploits

As our community demands more and more from technology, the operating systems which drive them become more and more complex. Unfortunately, this does not necessarily equate to a more secure electronic environment and may even provide new opportunities for things such as:

- identity theft
- Trojans and Backdoors accessing user's computers destroying material upon the computer, information being stolen or information being placed upon user's computers without them being aware
- Virus infections which spread rapidly to deliver their payload.

Section 2: The importance of an appropriate investigative response

Of utmost importance in any investigation, be it into cybercrime or otherwise, is the awareness of all as to what to do immediately upon its discovery. Organisations who have infrastructure affected by any kind of cybercrime should be aware of how to respond to it from the outset. They should be aware that it is vital to the investigation that whilst being considerate of business needs, evidence must be collected and preserved. We applaud the recent development by Standards Australia of a handbook outlining the guidelines for the preservation of electronic evidence which we feel will be a valuable resource in the private and public sectors.

For persons involved in computer forensics and cybercrime investigations we believe a national standard of accreditation should be implemented to promote core skills. Individuals who undertake these investigations must be appropriately skilled in:

- investigative techniques
- information technology, and
- Legal Issues relating to evidence, information technology and litigation both civil and criminal.

Identification of the Cyber Criminal

The process of identifying a criminal who is determined to maintain his or her anonymity can present many challenges. Computers connected to the Internet are identified by an unique number called an IP (Internet Protocol) address. IP addresses are either Dynamic or Permanent:

- Dynamic IP addresses are given to Internet users using a normal dial up connection. When the user 'dials in' to an ISP, a unique IP address is allocated from a pool of available IP addresses to the users machine. The user is allocated this address for as long as he is connected to the Internet. When the user terminates the connection that IP address is returned to the ISP and will be allocated to the next user that 'dials in'

- Permanent IP addresses are usually given to users that are permanently connected to the Internet.

IP address ranges are unique to each ISP. This makes it easier to locate the specific ISP that the criminal uses to access the Internet. From then, a users identity can be ascertained with the co-operation of the ISP by checking the logs and finding out who was assigned a specific IP address at that point in time.

Many cyber crime investigations concern email, the primary form of communication on the Internet. Email can and often is sent anonymously however information related to the source of the email can often be discovered through careful scrutiny of the e-mail's message header. The message header contains an audit trail of each server the e-mail was routed through to get to the specified email address. Assistance in positively identifying the suspect must invariably be obtained from the ISP. This can be complicated when technology is used to remove or fabricate the audit trail.

The successful investigation of cybercrime involves a heavy reliance upon the assistance of Internet Service Providers. (It is our experience that certain Internet Service Providers limit record keeping for the purpose providing anonymity to their customers. Some parties use this anonymity to engage in dubious activities).

In Australia the private sector investigations firm has a limited civil mechanism by which effective access can be obtained to information held by an Internet Service Provider. Such access may be required in a matter in which there is at that time insufficient evidence for investigation by the police. We have successfully sort such information by court subpoena in the past. However, the lack of an identified respondent requires a civil application for 'preliminary discovery'. Generally such applications are time consuming (weeks) and expensive.

Computer Based Evidence Recovery

Traditionally the collection of evidence in a fraud investigation has relied upon the presence of a physical paper trail. In today's corporate environment, the paper trail largely originates from, and in many cases has been replaced by, personal computer records. In response to this trend, a field known as computer forensics has developed. Put simply, computer forensics is the seizure and analysis of electronic data using a methodology which ensures its future admissibility as evidence in a court of law. As the evidence related to a cybercrime is likely to be in electronic form, computer forensics is an integral part of modern cybercrime investigation.

The fundamental principle of computer forensics is that original data is never altered. For this reason, purpose written 'forensic image' software is used to take an exact copy of a 'target' computer system. From this image the original system can be recreated at any time. It is essential that trained and experienced specialists are assigned to this task. This ensures both the integrity of the target system (it is difficult to put a monetary value on the accidental loss of commercial information), and the integrity of seized evidence. A computer forensic technician must be able to justify their actions in future court proceedings.

Forensic computer images have been accepted by Australian Courts to be 'original' evidence. It is not necessary (in most cases) to seize physical computer hardware. Indeed, in situations where target computer systems contain critical data, such as in a doctor's surgery, physical seizure is never a viable option. Once an image has been taken, hardware that may otherwise have been required to be secured for evidence continuity may be put back into use.

Forensic imaging is also well suited to covert investigations. Much information can be drawn from a suspect's personal computer without alerting him/her to an investigation.

In the analysis phase, computer forensics is concerned with more than existing files. A computer forensic technician will examine the entire structure of a hard disk, looking to collect all possible evidence. During normal PC operation, data additional to that which the user intends to save is 'written' to the surface of the hard disk. On examination this information can be collected and analysed.

On many occasions valuable evidence from these areas has been collected from computer systems which were previously believed to be 'clean'.

In investigations where the suspect is computer literate, these ‘hidden’ areas are sometimes used to hide information. It is common that the actions of a suspect in removing or hiding evidence from a computer system can have the opposite effect, and strengthen the evidence. This is often the case with deleted files, or the non destructive ‘format’ of the computer hard drive.

In common operating systems such as Windows 2000 and Windows XP, there are a variety of ‘cache files’, ‘swap space’, ‘audit logs’, and ‘registry entries’ which all contain information about the actions of the user. An experienced computer forensic technician can quickly put together a profile of computer use, and identify potential evidence.

Computer forensics has proved a reliable, successful, and cost effective tool for the investigator. In cybercrime investigations it is an essential tool.

Section 3: Global Economic Crime Survey

PricewaterhouseCoopers recently released its 2003 global and Asia Pacific economic crime surveys which discussed cybercrime. Key points to come out of this survey were:

- although only 16% of organisations in the survey reported suffering from cybercrime in the last 2 years, increasingly all incidences of economic crime depend on an element of technology

- in the Asia Pacific, 38% of organisations perceive cybercrime as their chief concern over the next 5 years

- globally, the biggest concerns for the future are asset misappropriation and Cybercrime

- over two thirds of corporate cybercrime victims could not quantify the direct monetary costs.

The full Economic Crime Survey reports are attached to our submission as Appendix B & C.

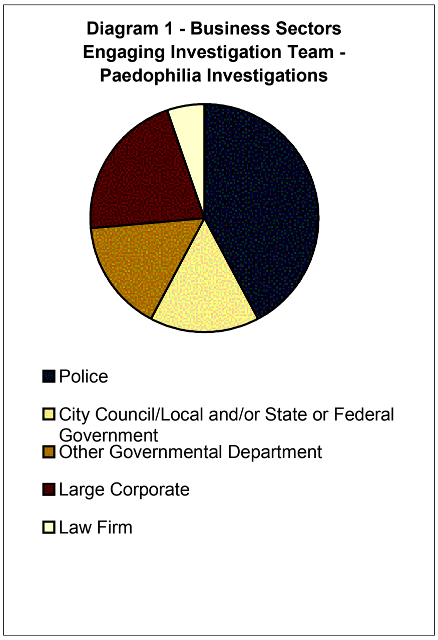
Section 4: Our Investigations Experience

The PricewaterhouseCoopers Computer Forensic team performs a wide variety of investigative work for corporate and government clients. In recent times the most prominent type of investigation has been the theft of commercially sensitive intellectual property. These activities have usually been carried out by, or with the involvement of, persons internal to the victim organisation.

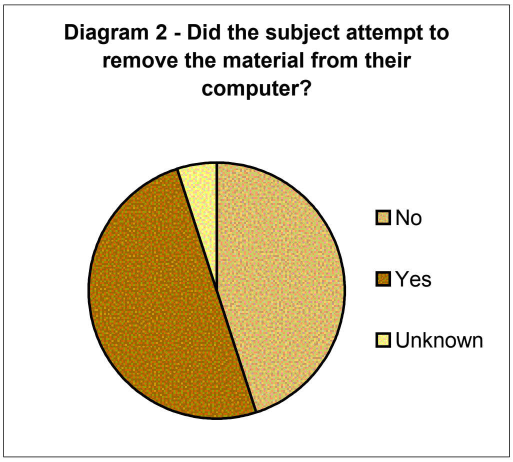
As per the terms of your enquiry, we provide you with a breakdown of our investigations which have involved child pornography and online fraud.

Child Pornography Investigations

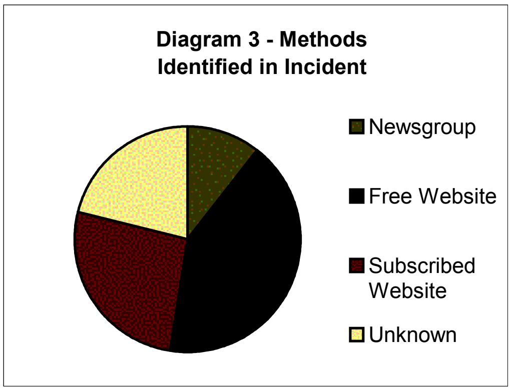
Our major client base of Large corporates were found to be the dominant group engaging us in investigations resulting in the discovery of paedophilic material. Diagram 1 below suggests that there is no one particular client base which provides for any particular significance in child pornography Investigations.



Approximately half of the subjects attempted to remove evidence of their activities by deleting the material (placing it in the recycle bin) or by use of wiping software. Generally these attempts were ineffective.

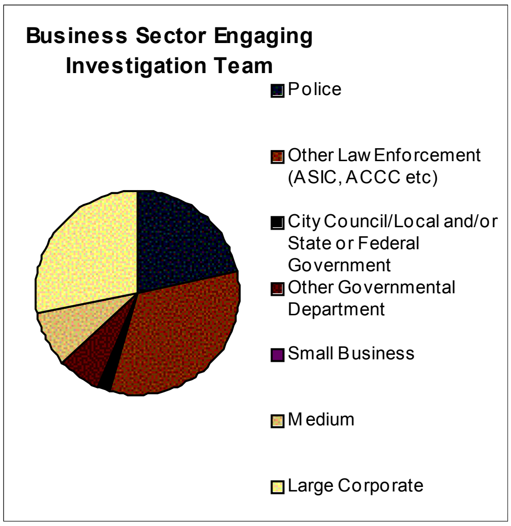


The most common way in which child pornography was accessed involved the use of free or subscription based websites. We have not identified groups of like minded individuals communicating on this subject.



In accordance with relevant state legislation dealing with possession of child pornography, the investigations in which we identify child pornography usually necessitate the immediate referral of the matter to the relevant state law enforcement agencies. This can influence our continued involvement in the investigation.

Banking, Credit Card and Online Fraud



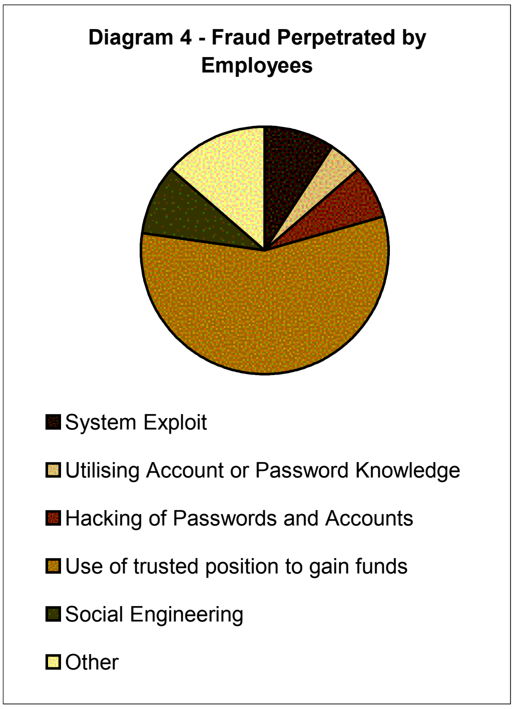
Who engage us in Online Fraud Investigations?

Our online fraud investigations are well distributed between the Police, other law enforcement and the private sector. Most of our private sector online fraud investigations are for large corporate clients.

Fraud Perpetration Breakdown

Approximately 95% of the fraud cybercrime we have investigated involved conduct of an employee or former employee. The remaining 5% involved groups of employees or former employees.

Diagram 4 describes cybercrime of a fraudulent nature undertaken by Employees.

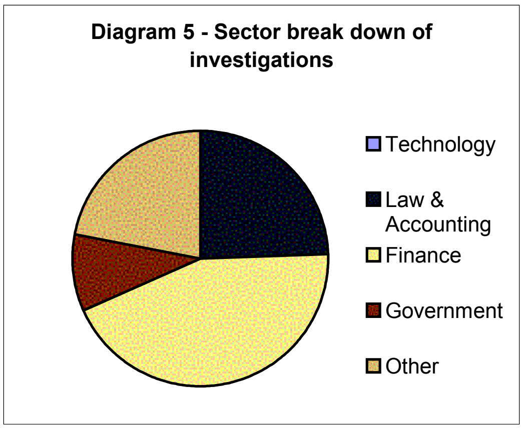


Much of the unlawful conduct by employees still falls into the ‘trusted person’ category where perpetrators gained access to account details.

Sector break down of Investigations

We have found that the finance sector is the dominant sector affected by cyber-fraud. Approximately 10% of all cyber-fraud investigations involved government.

Diagram 5 below describes the sectors of our economy which we have been involved in investigating cyber-crime.



Conclusions

In August 2001 the Parliamentary Joint Senate Committee on the National Crime Authority published its report on the Implications of New Technology on Law Enforcement. The report encompassed the effect of new technology on current legislation, existing law enforcement bodies and the interaction between the two in an effort to combat crime. Particular importance was given to the adequacy of current responses and the implications of developing technology on such responses with regard to the sufficiency/capability of the law. The report culminates an extensive process of investigation and research by a variety of bodies with submissions made predominantly by the public sector.[1] The Committee made nine recommendations, in which . Emphasis was given to:

- nationally consistent approach to multi-jurisdictional investigations
- the ability to address issue of money laundering
- the ability of legislation to keep pace with change.

We consider that these remain the primary issue to be addressed in the investigations of Cybercrime.

In our private sector investigations we have identified a recent increase in cases which involve the theft of commercial intellectual property. We have also observed a steady increase in the use by suspects of technology to erase or secure data, including Internet anonymising software, disk wiping and encryption tools.

We consider that the private sector investigations teams play an important role in the identification and investigation of cybercrime. In many instances it will be such teams that act as the intermediary between the victim and law enforcement. A major hurdle in our efforts to investigate cybercrime in the private sector is the lack of an efficient civil mechanism to obtain timely access to information from Internet Service Providers for investigative purposes.

[1] This is a summary of the *Parliamentary Joint Senate Committee on the National Crime Authority Report into "Law Enforcement Implications of New Technology",* August 2001. Department of the Senate Printing Unit, Parliament House, Canberra.

It is also our investigations experience that there is uncertainty in the private sector about the use of investigations techniques, such as key stroke logging or packet capturing devices and their use in regard to the Telecommunications Interception Act.

A way forward for such issues may be to follow legislation similar to the NSW Work Place Surveillance Act in which private sector organisation can apply to the court to utilise such techniques.

We look forward in Australia to the development of training and accreditation standards for both corporate and government agencies specifically applicable to the investigation of cybercrime.

Appendix A – Methods Facilitating Cybercrime

Internet Mail

One of the simplest ways which unlawful conduct upon the Internet can be undertaken is by using Internet Mail. Examples of such include Hotmail and Yahoo! Mail. On setting up an Internet Mail account, a user may choose whatever name they desire so long as it has not been chosen by someone else. No form of identity verification is required and thus users are free of the constraints caused by their real life experiences.

This way, a user ie John Smith from Canberra may chose say John_Smith@hotmail.com if he wishes to be able identifiable as John Smith in correspondence. Alternatively John may wish to hide his identity and be known as Canberra_Man@hotmail.com. John may then believe he is in a position to communicate more freely with individuals upon the Internet, free of any concern about being tracked down in real life.

Say John dislikes Bill Jones, John may create an account Bill_Jones@hotmail.com and send malicious e-mails in Bill's name.

Having said that though, skilled investigators can in many circumstance review header information within the contents of an email to trace an email back to the computer which was used to send the e-mail.

Fake Email

Software has been created to allow the creation of email without the need to have an email account or access to a particular email account.

In our example above you will recall that John Smith used an Internet account Bill_Jones@hotmail.com to disseminate malicious e-mail. Let's say Bill found this out and knew that John possessed the John_Smith@hotmail.com email account.

Using such software, Bill could create the impression that John smith sent an email using the John_Smith@hotmail.com address. He could therefore send an email that is even more damaging to John than the message sent by John in Bill's name.

The drawback from a malicious user's perspective is that in using this technique the culprit will unlikely receive any response to the 'fake email' sent as it is unlikely the culprit will have access to the real e-mail account.

From an investigator's perspective fake email can in many circumstances be identified as such since the fake email will not provide the appropriate information relating to the originating computer.

Simpler fake e-mail software will use the computer's information as its originating point enabling investigators to discover the originating computer the malicious user operated in their actions.

More advanced fake email software will permit the user to cover their tracks, therefore reducing their chance of capture.

Paging Software

Another form of communication is the use of Paging software. Examples of paging software include Lotus' Sametime Connect, Yahoo! Pager, ICQ. These programs allow for one on one real time communication between users, regardless of their physical location. Many paging programs such as those provided as examples provide advanced utilities including file transfers as well as voice and video software.

In our experience, Paging software is frequently identified on computers used to undertake a variety of inappropriate or unlawful activities including:

- software piracy
- pornography including paedophilic
- commercial fraud

The problem faced by lawful users of the Internet in utilising Paging software is that often it is insecure. The ICQ product, in the past, was an example of a product that had security gaps permitting remote processes to directly access the contents of a user's computer.

Internet Relay Chat (IRC)

IRC is a type of online chat forum where individuals can communicate in real-time. More advanced systems may also provide users with the ability to transfer files. Our experience indicates that there is significant discussion about many kinds of unsavoury behaviour.

In our cyber investigations training, we recommend students utilise this tool (whilst maintaining anonymity) to identify potential cybercriminals.

Web Chat

Like IRC on-line chat environments, Web Chat environments permit users to communicate in real time. The more advanced systems such as that found at chat.yahoo.com.au provides for voice and video communication between users. A user accesses such an environment by means of a Web-browser by means of a previously created account. In the case of the Yahoo! Web-chat, accounts used for chat services also provide other services including email.

Anonymisers Re-director and Diverters

A computer user communicates with another over the Internet not by communicating directly with it but by taking several steps, known as hops, over the network. This way any computer that can find a path to another can do so with the assistance of infrastructure configured to route traffic between separate parts of the network.

Basically, routing hardware is provided with information to permit it to identify where it is itself within the network.

When a computer sends information across the Internet it does so in packets. This is so as to permit the free flow of data across the Internet. Aside from the data transmitted TCP/IP packets contain information including the source and destination computers' location as well as where the particular packet fits in the data to be transmitted. Once the packets are received by the destination computer they are put back together in the required order.

When a Router receive data it analyses it to identify whether it is capable of transmitting the data along the path towards its destination by means of routing tables. This process continues until either the data gets to its final destination or is incapable of being sent to its final destination . As such, packets may not necessarily traverse the same path to reach its destination. Thus if say a computer sent data across the Internet within 30 packets, the destination computer may receive the 3rd packet before the 1st. The destination computer will piece together the packets in the correct order though given that it can verify each and every packet was correctly received.

Anonymisers cause a user's computer to transmit its information via an intermediary proxy server. This intermediary system can replace packet information relating to the source of the data. That way a user going through an anonymizer service will be identified by the replaced source information within the packets received by the destination computer.

Basically this means anonymizers give observers at the destination computer the impression that the data was sent from the intermediary proxy server rather than the true source location.

SPAM

Spam (unwanted email) databases are created through the exploitation of cookie capabilities. Another method which SPAM databases develop is through the accessing of online public directories. One such directory is the WHOIS service which now suffers as a result of SPAM exploitation from bogus or inaccurate information.

Spam filters are available for most email services however they are often ineffective in preventing all Spam mail coming through. It is not uncommon for such mail to contain malicious code.

Spy-Ware

Spy-ware is often bundled with popular free-ware and permits system and user activities to be reported to a remote process. Some of the biggest names in the industry have been accused of including spy-ware within their products.

In Australian Personal Computer's February 2003 edition, the magazine stated that the four main spyware packages were:

- Blackstone Data Transponder
- Cydoor
- Brilliant Door
- Xupiter/Lap.com
- Gator
- Cytron

The most common products affected are the peer-to-peer technologies such as KaZaA, the next generation of products replacing the now defunct Napster.

The magazine also stated that big corporate names such as RealNetworks, Audiogalaxy and Netscape have also been accused of utilising Spyware.

Drive Wipers

The regular operation of computers these days causes information to be left on the computer's hard drive even after it is no longer need. For example, such information remains even after say a document is placed in the 'Recycler' or if a file is deleted. Data is only destroyed once it is physically over-written by other data.

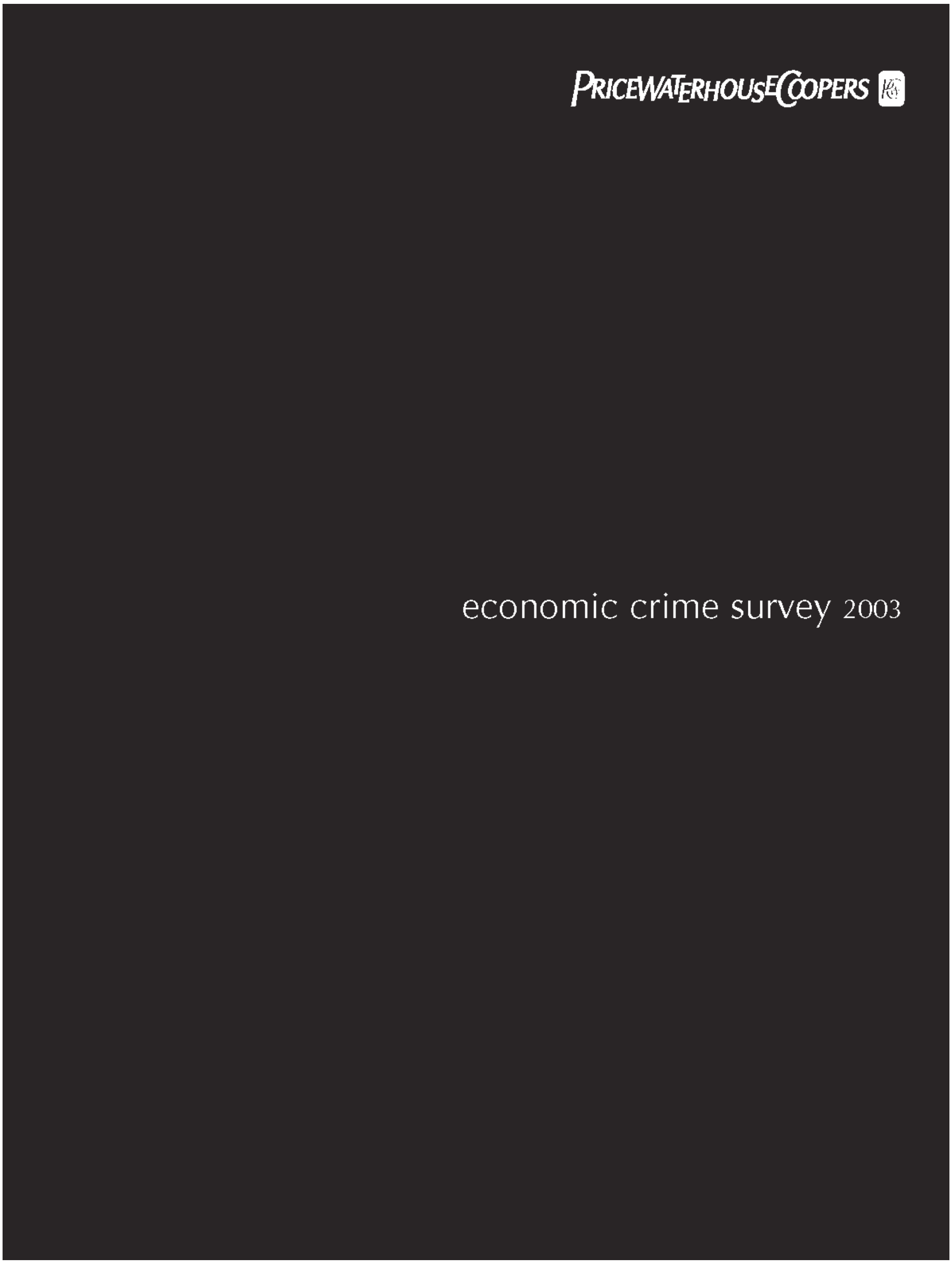
A common way in which data is recovered in a forensic examination of a computer is by analysing the ‘unallocated’ space upon a hard drive. If data is deleted by the operating system, be it by a user’s instruction or otherwise, it is identified as no longer being required by the system and the space which this data occupies returns to an ‘unallocated’ state. Whilst the data remains in that space, the computer considers that space available for writing to in the future.

Drive-wiping software permits the writing of either garbage or a particular character or string of characters to a certain area of the hard drive or the entire hard drive. This way a user can effectively erase the contents of a drive. In doing so, they may be removing vital evidence necessary in the investigation of a user’s unlawful activity.

Steganography

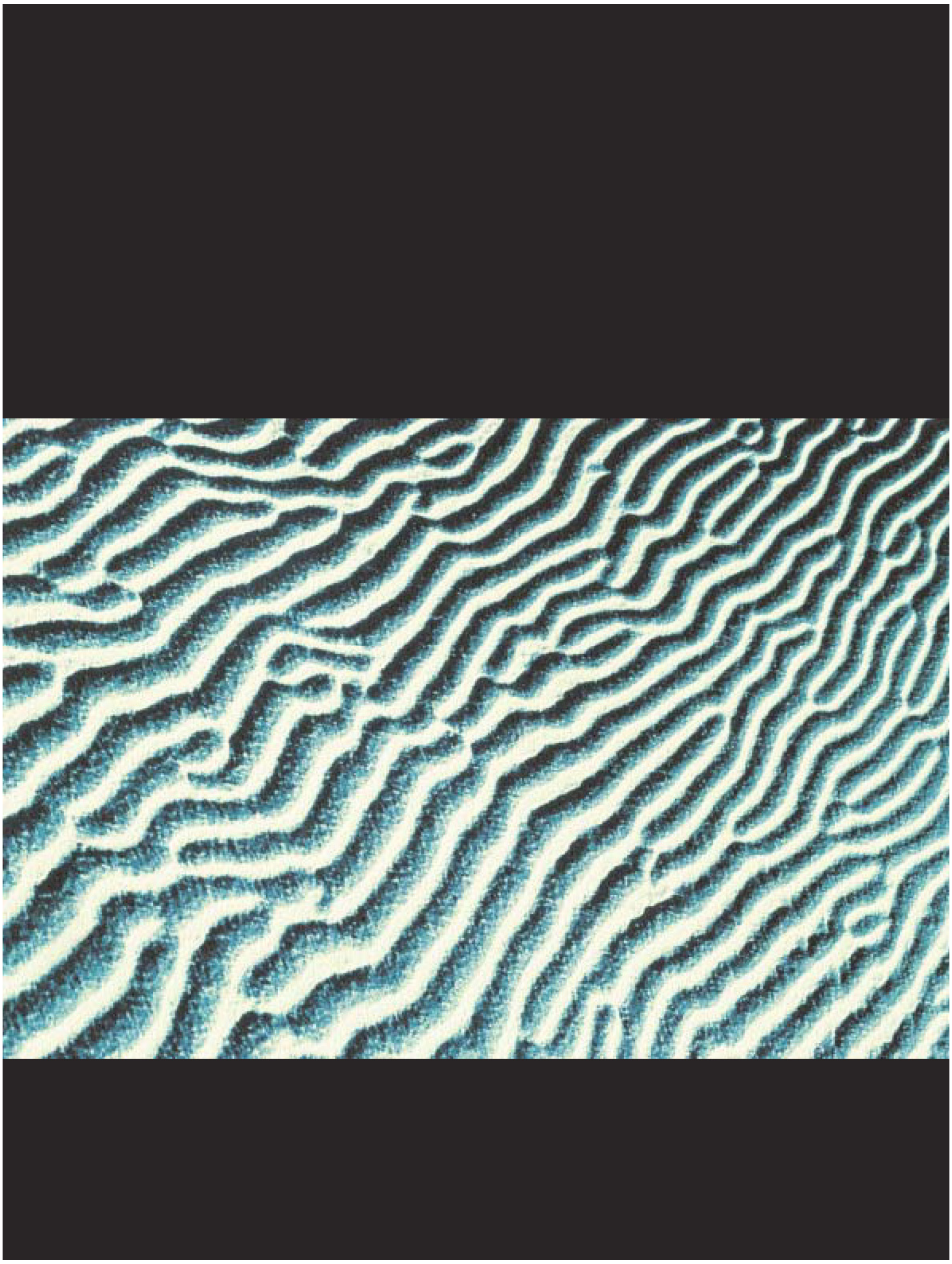
Steganography has recently received media attention as the next weapon which cyberterrorists use to communicate with one another. Stegangraphy, or Steg for short, is the science of embedding data within other, larger data often cryptographically. Discussions regarding Steg often lead to the belief that it is a tool used by those dealing with paedophilic material.

Steganography is notoriously difficult to discover. PricewaterhouseCoopers has yet to undertake an investigation where this technique has been used to assist in the commission of a crime.

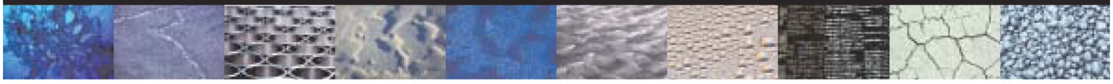


PRICEWATERHOUSECOOPERS

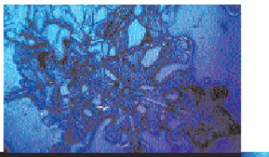
economic crime survey 2003

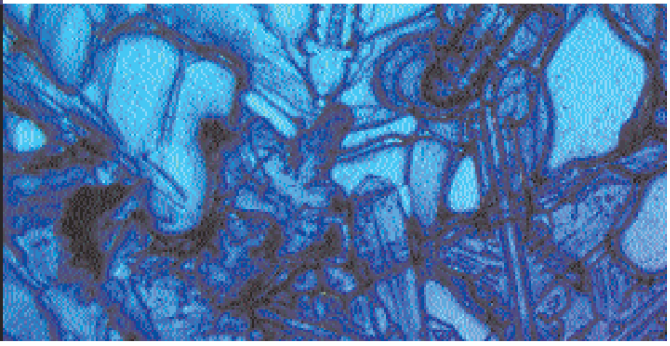


economic crime survey 2003



contents





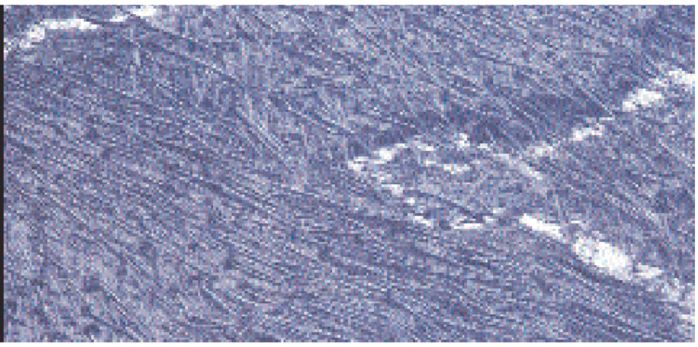
2

introduction

executive summary

- Economic Crime remains a significant threat: 37% of respondents report significant economic crimes during the previous two years.
- The bigger you are, the harder you fall: companies with more employees are more likely to have suffered from economic crime.
- No industry is safe: over 30% of respondents in each of the industries interviewed suffered fraud.
- Asset misappropriation is the most widely reported crime. It is also the easiest crime to detect, with 59% of all victims citing this as one of the frauds that they had suffered.
- Average loss per company: US$2,252,889
- The impact on reputation, brand image, and staff morale can be more important than the direct financial loss.
- Two-thirds of respondents stressed the company's Board had ultimate responsibility for preventing or managing economic crime – but only just over a quarter had given their boards any risk management training.
- Tangible risk management measures reap clear results: those that had suffered fraud took practical anti-fraud measures, from employee screening to active awareness raising; those that had not, relied on passive measures such as a company code of ethics.
- Three quarters of victims of crime recovered less than 20% of their losses; only half of respondents had insurance against economic crime, but they recovered more of their losses.
- The biggest concerns for the future are asset misappropriation – the most visible of economic crimes – and cybercrime.

4



economic crime: a growing global threat

Economic crime remains a significant threat to companies across all industries and territories. Well over a third of respondent companies worldwide (37%) said they had suffered from one or more serious frauds during the previous two years.

Figure 1: Victims of fraud (worldwide)

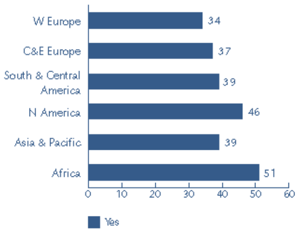
This figure is significantly higher than in our previous European research in 2001. The number of organisations reporting fraud in Western Europe has grown from 29% to 34%, and in Central and Eastern Europe from 26% to 37%. This increase appears to reflect two factors:

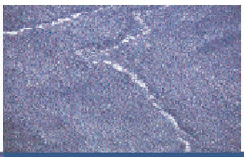
- greater awareness of fraud leading to heightened detection rate; and

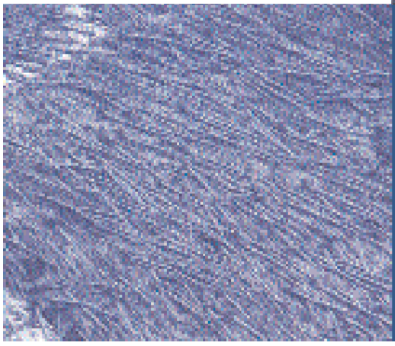
- a growing desire for transparency, particularly in EU 'accession countries'.

The highest levels of economic crime were reported by respondents in Africa (51%) and North America (46%). In contrast, respondents in Russia and Turkey reported no economic crime at all. There is clearly some way to go in both these countries to either improve detection or to promote greater transparency.

Figure 2: Victims of fraud (by region)







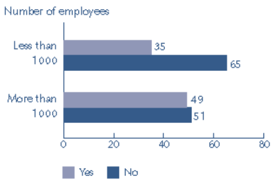
5

The bigger they are...

Our findings suggest a direct relationship between company size and the likelihood of economic crime. Only 35% of smaller companies (less than 1,000 employees in territory) reported economic crime, compared to 49% in larger companies (over 1,000 employees in territory).

Possible reasons for this higher incidence among larger companies include their greater devolution of operational responsibility, tendency to pursue opportunities in unfamiliar markets, higher transactional complexity, and greater opportunities for collusion amongst employees. Staff in larger corporations may also be less concerned about the financial well being of their employer, regarding fraud as a "victimless crime".

Figure 3: Victims of fraud by organisation size (worldwide)



Larger companies also generally invest more in fraud risk management systems. This will increase detection rates for most economic crimes.

6

industries at risk

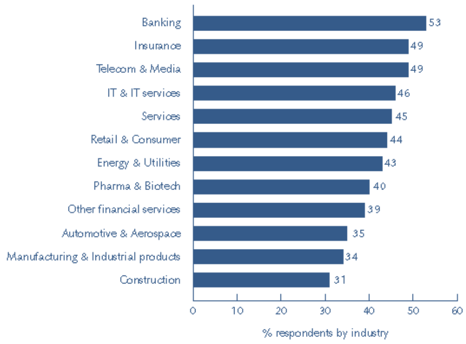
While all commercial activity is vulnerable to economic crime, its incidence varies between industries.

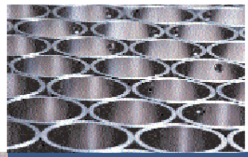
The results of the Global Survey reinforce our findings from the 2001 European Survey. Financial services (banking, insurance) have reported more incidences of economic crime than other industries. The financial services industry is an obvious target for any fraudster, given the significant quantities of physical assets held, and access to financial transactions, many of which may be complex.

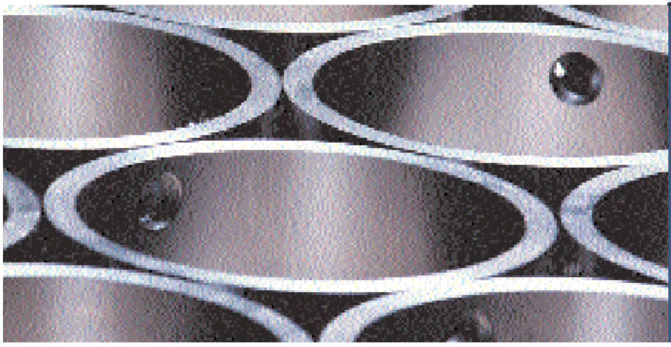
It is also noteworthy that other highly regulated industries, such as telecoms, appear at the top of this league table. Due to their regulation, these companies have usually developed more sophisticated control and compliance systems. The financial services sector in particular is more acutely aware of the threat from economic crime. So the higher reported levels of fraud in these sectors partly reflect higher sensitivity to – and detection of – economic crime.

The lower end of the chart contains less regulated industries such as manufacturing and construction. Whilst these industries are prone to economic crimes ranging from asset misappropriation to product piracy, they may often have less sophisticated control and detection mechanisms, or may accept losses through fraud as inevitable.

Figure 4: Victims of fraud by industry (worldwide)





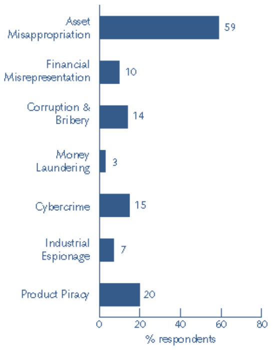


7

types of economic crime

By far the most commonly reported fraud is asset misappropriation, with 59% of those reporting economic crimes claiming this was among them. This type of fraud is generally the easiest to detect, as it involves the theft of tangible items with a defined value. This may help to explain why it is the most commonly reported.

Figure 5: Types of fraud experienced (worldwide)



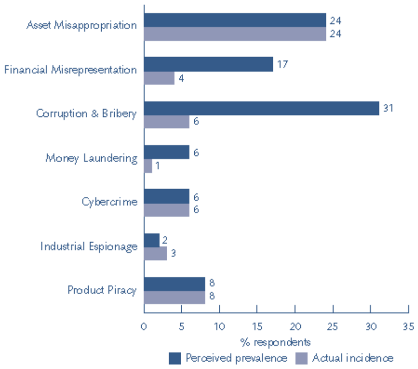
Perception and reality

Further insights can be gained by comparing the perceived prevalence of each type of economic crime with its actual incidence.

With asset misappropriation, product piracy and cybercrime, the perceived prevalence and actual incidence are very similar. This is likely to be due to their greater visibility: lost assets can be counted, counterfeit products seen in the market.

However, with both financial misrepresentation and corruption & bribery, the perceived prevalence is much higher than the reported incidences.

Figure 6: Frauds considered most prevalent compared with their actual incidence (worldwide)

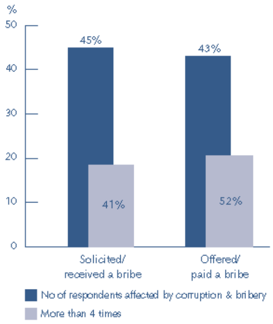


8

With financial misrepresentation, this gap appears to reflect two factors:

- higher awareness following the corporate scandals in North America and Europe; and
- an understanding that it is likely to have an especially dramatic impact on a business.

Figure 7: Types of corruption & bribery (worldwide)



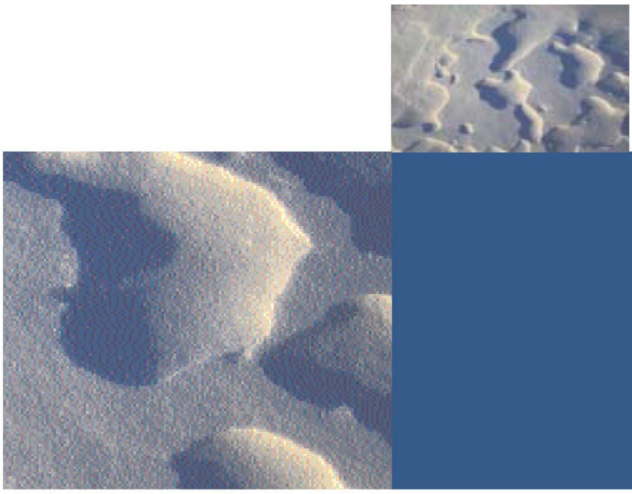
Given the serious implications of financial misrepresentation, it should be worrying that one in 10 organisations reported incidences (figure 5).

The high perceived prevalence of corruption & bribery reflects the hard work of governments, regulators, and certain NGO's to raise public awareness; an important factor in helping to reduce actual incidence.

199 respondents reported suffering corruption & bribery (worldwide). 45% were solicited with or received a bribe, and 41% of those more than 4 times! 43% were required to offer or pay a bribe – 52% of those more than 4 times! The remaining 12% refused to comment.

The incidence of corruption & bribery has a regional bias towards the developing markets of Africa, South and Central America, and Asia Pacific. In these regions such acts are often viewed as an acceptable element of doing business. Increasing pressure from developed economies is forcing many countries to promote increased awareness of corruption & bribery, and many companies operating in those markets to carefully review their procedures.

It is inevitable that the overall figure for Money Laundering incidence will be low. In order to get a realistic impression of the level or impact of money laundering, it should be assessed according to its incidence within the financial services sector. One in six banks reported having uncovered money laundering during the previous two years. 220 financial services organisations worldwide said they had reported suspicious transactions during the two years, with 20% reporting more than 10 suspicious transactions. This almost certainly reflects the well publicised and ongoing efforts to raise awareness of money laundering and stop movements of illegally obtained funds by convincing countries to adopt internationally accepted anti-money laundering regulations, as well as regularly monitoring their performance.



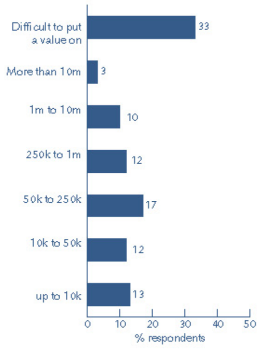
9

the financial cost of fraud

We spoke to over 1250 companies that reported losses due to economic crime in the last 2 years. 793 of these companies were able to quantify their loss.

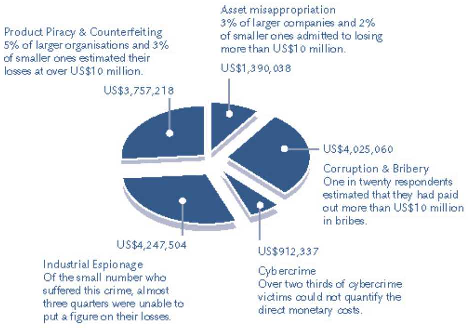
Even when companies know that they have suffered economic crime, they find it difficult to quantify the financial impact on their business. A third of victims cannot even guess how much it cost them. It is clear that the financial cost of less tangible economic crimes, such as bribery & corruption and cybercrime can be especially hard to quantify. Even with a more quantifiable crime such as asset misappropriation, 21% of victims could not put a figure on their losses.

Figure 8: Financial loss through fraud (worldwide)



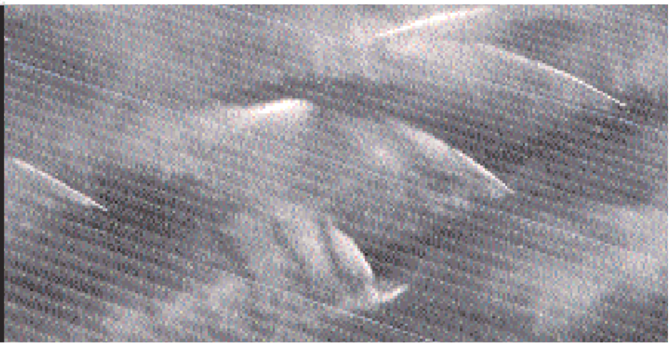
Among the remaining two thirds (793 companies), we estimate the average loss from fraud was US$2,252,889.

Figure 9: Average financial loss by type of fraud over last two years (worldwide)



The average loss per company from fraud – US $2,252,889

10



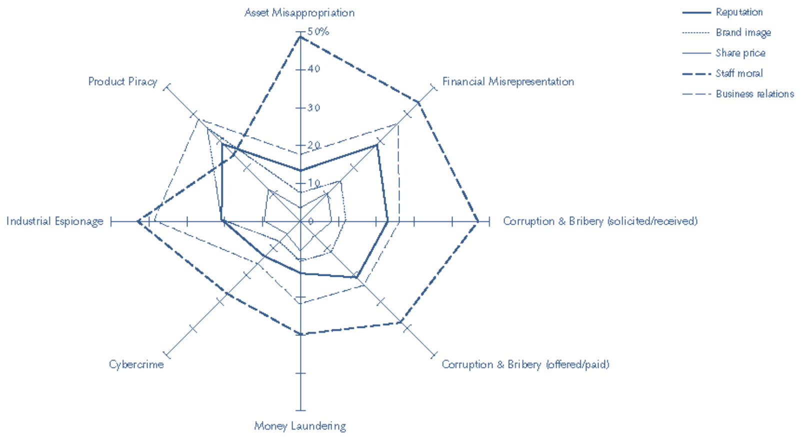
the collateral cost of fraud

The damage inflicted by economic crime goes far beyond direct monetary loss. Intangible assets including business relationships, staff morale, reputation and branding are critical to any business. These can all be undermined by the occurrence or even the perception of fraud.

The reported impact varies depending on the nature of the crime committed. Incidence of economic crime in an organisation invariably raises questions in employee's minds about its leadership and governance, its ethics, or as a secure environment to work. Repeated exposure to such issues can undermine years of carefully built up staff loyalty.

The second most common concern is the effect of economic crime incidence on external business relationships. It is noteworthy that both asset misappropriation and cybercrime are perceived to inflict less damage in this area than the other forms of economic crime. It may be that organisations accept exposure to these types of crimes as part of the everyday risks of doing business, whereas financial misrepresentation, corruption and

Figure 10: The collateral cost of fraud (worldwide)



bribery may be indicative of wider company issues.

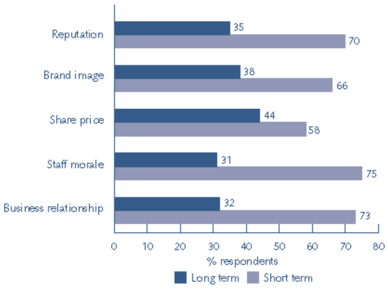
Business relationships and brand image also suffer significantly where product piracy is at play. As a crime extremely prevalent in Africa and Asia Pacific, companies operating in those markets need to be aware of the major impact product piracy can have on product and brand licensing deals by diluting the underlying asset value and creating mistrust among business partners.

The relationship between economic crime and share performance is a complex issue. A relatively small number of victims felt that fraud had affected their share price – even where financial misrepresentation has potentially called previously disclosed information into question. However, the proportion of respondents who reported an impact on share price as a result of economic crime has doubled since our 2001 research, perhaps indicating that the financial markets no longer view economic crimes as a historical offence with limited future relevance.

Overall, a failure to tackle – or at least manage the risk of – economic crime effectively can store up long-term operational problems for any enterprise. The safeguarding of valuable intangible assets such as brand, client relations, and staff morale should be a key objective.

Asked to consider whether the collateral damage had a short or long-term impact on their business, most respondents believed the impact to be short-term (less than one year). This should not disguise the fact that approximately one third of respondents reported long-term effects of economic crime on their business, and in the case of share price 44%. A sure sign that collateral damage should be considered on a par with monetary loss when determining economic crime risks.

Figure 11: Was the impact of economic crime short or long term? (worldwide)

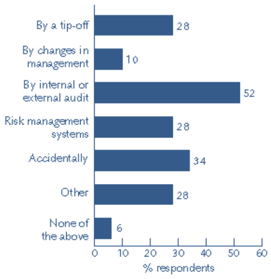


12

detecting economic crime

Fraudsters invariably take great pains to conceal or remove evidence of their crimes. As companies can only report crimes that have been detected, it is not possible to judge how much fraud goes unnoticed. What we can analyse is the means by which fraud is brought to light.

Figure 12: How economic crime is detected (worldwide)



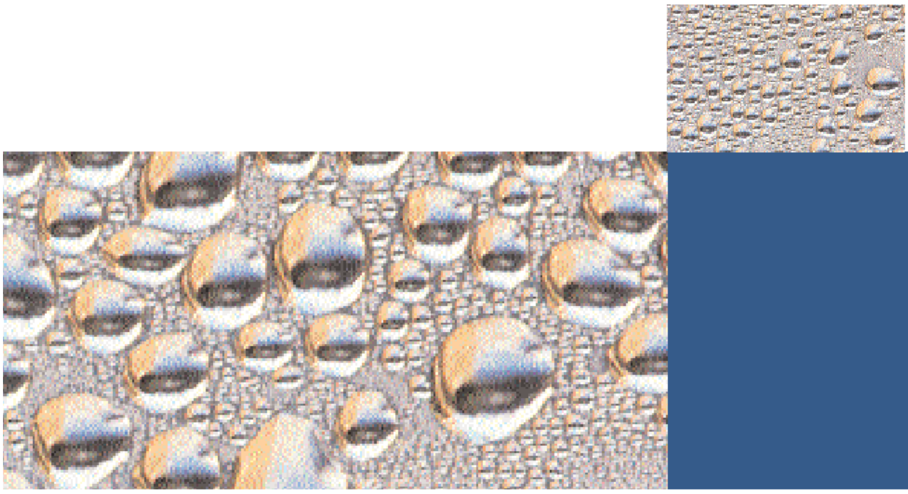
The results vary considerably depending on the size of the organisation concerned. Within larger organisations a combination of factors are likely to be involved in the detection of an incident. Large companies most often detected fraud through their control and risk management systems. However, in many cases this was accompanied by a finding from the internal or external audit function or from a tip-off.

Smaller organisations detected a far greater proportion of economic crime through audit processes than by other means. Given the respective size of the organisations this is most likely to be via the external auditors – a worrying finding that suggests smaller companies may be placing too little attention on the development of effective controls and alternative checks and balances. Over-reliance on a single annual review to root out problems may be playing into the fraudster's hands.

A consistent theme from our previous European survey is that over a third of economic crimes at major companies are uncovered by accident.

Clearly, reliance on luck is not a basis for an anti-fraud regime. However, even where companies have control systems to detect economic crime, these can often be rendered ineffective by management override or collusion. Companies need to do more in terms of:

- Assessing the real risks and vulnerabilities to fraud within the organisation
- Communicating actively the company's stance on fraud and "walking the talk"
- Proactively monitoring risky areas
- Developing policies to encourage (and protect) "whistleblowers"
- Expecting the worst and being prepared – devising a robust fraud response plan



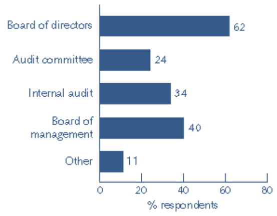
13

managing economic crime

Respondents assign primary responsibility for managing economic crime issues to the board of directors. 62% of respondents stated that the board must be informed of all instances of economic crime. There are significant regional variations however. Within Asia & Pacific (83%) the responsibility is vested firmly with the Board. Significantly fewer companies in North America (45%) and Central & Eastern Europe (47%) rely on the Board to fulfill this duty. In both these regions, company management is just as likely to have responsibility for managing the issues.

Regardless of where the primary responsibility lies it is surprising that only 28% of organisations have implemented any fraud-related training for the Board or management. Given the increasing focus on corporate fraud with regulators, ratings agencies and others now scrutinising companies for signs of misdeed, Boards and management need to consider making this type of training part of their corporate governance regime.

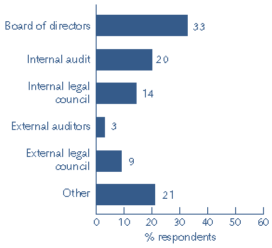
Figure 13: Bodies to which economic crime must be reported (worldwide)

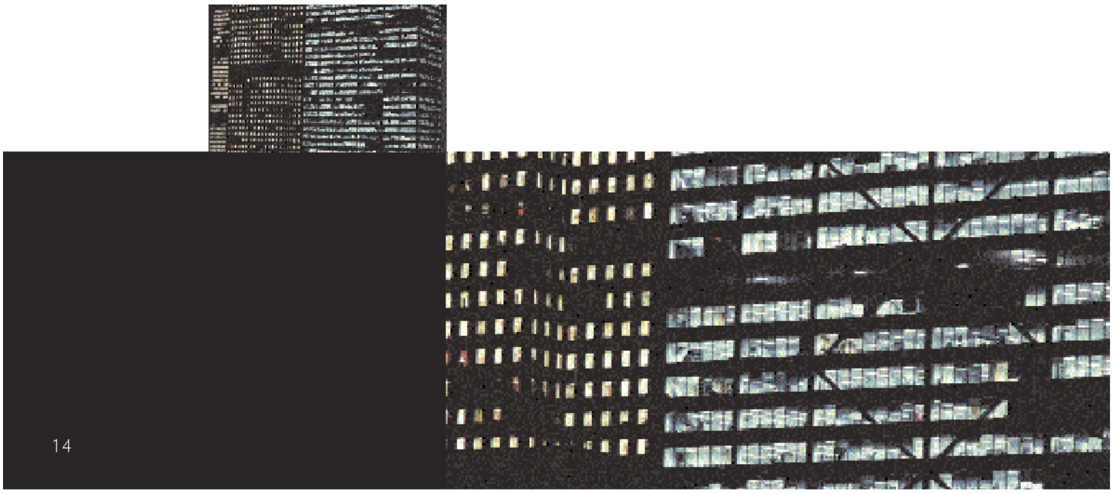


Respondents' opinions varied on how economic crimes should be dealt with once detected. Overall 63% of respondents organisations said they had a requirement to report frauds to an external body. Once more though, regional variations are significant. In the Asia & Pacific region only 48% of companies had a requirement to involve the authorities. In Africa and Central & Eastern Europe over 80% of companies said that they applied this policy.

We are surprised that this figure is so high. Our experience in investigating economic crime for corporations suggests that there are many reasons why an organisation may choose not to report a fraud to an external body. These include the potential impact of negative publicity on business relationships or staff morale. In addition, companies often fear the costs of a drawn-out judicial process, or simply believe there is little chance of recovering the stolen assets. It may well be that companies have a public face supporting a policy of reporting all matters to the authorities, but become more pragmatic when faced with an actual event.

Figure 14: Responsibility for dealing with economic crime (worldwide)





recovering stolen assets

Even if economic crime is detected and prosecuted, it can still prove impossible to recover the assets. Of respondents who had experienced fraud, only 8% had succeeded in recovering more than 80% of their losses, whilst almost three-quarters recovered less than 20%.

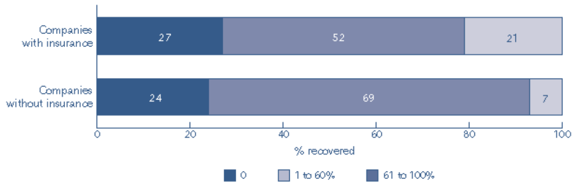
There are many reasons for this relative failure to recover lost assets. Companies are reluctant to embark on long recovery processes with no certainty of success, especially where the assets have been moved across borders. However, there may be good reasons to pursue the assets regardless – firstly because it is not always possible to form a realistic view of the chances of recovery until the process gets under way, and secondly because a policy of always attempting recovery helps to create the right culture of deterrence.

Insurance

Surprisingly, given the high awareness of economic crime, less than half the organisations surveyed had taken out insurance against fraud losses. This may be due to management indifference or scepticism over how much insurance could actually recover.

However, insurance can have a significant impact on recoveries. Companies with insurance reported being 300% more likely to recover more than 60% of their losses.

Figure 15: Recoveries of companies with and without insurance (worldwide).



preventing economic crime

Not surprisingly, companies that have suffered economic crime are more concerned about the strength and effectiveness of their systems to prevent fraud. They are also more likely to have taken proactive measures to reduce future exposure.

Our findings illustrate the impact of fraud on an organisation's mindset. Those that had not suffered fraud tended to rely on more intangible prevention tools such as codes of conduct or ethical policies. In contrast, fraud victims instituted more tangible measures such as employee screening, management training and whistleblowing programmes. They also invested greater effort in raising awareness of the potential for economic crimes.

Organisations that take practical measures to combat fraud, and that effect change on the ground rather than creating the appearance of addressing the problem, will develop a stronger culture of prevention. As a result of such action, companies that had reported economic crime are "quite" or "very" confident that their anti-fraud controls are stronger now than they were two years ago.

Figure 16: Types of corrective measures taken (worldwide)

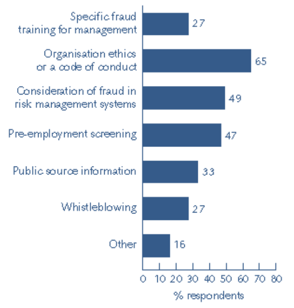
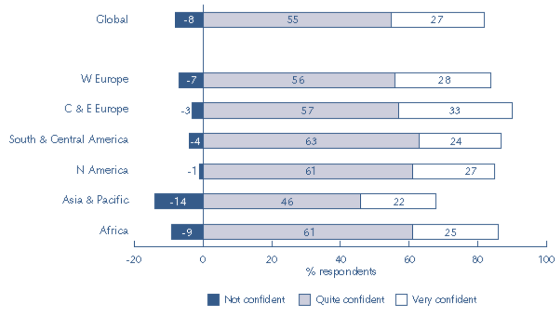
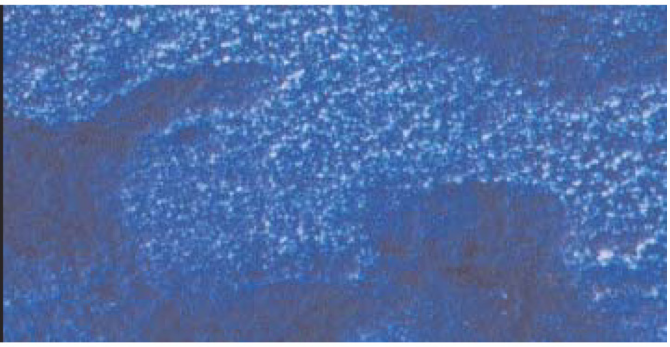


Figure 17: Confidence in fraud risk management systems



16



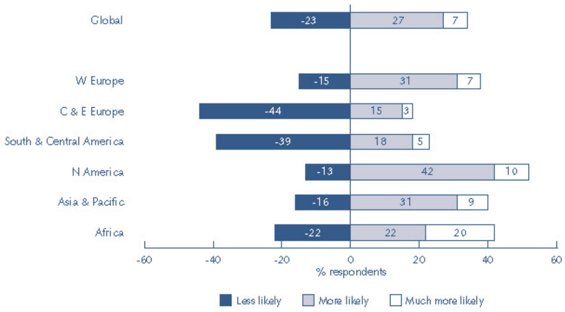
economic crime risks of the future

Most organisations expect the threat of economic crime to increase over the next five years, with respondents in North America and Africa being especially pessimistic. Our findings support this general perception that the risk will increase.

However, companies in Central & Eastern Europe and South & Central America expect the risk to decrease.

The responses from Central & Eastern Europe are in line with our European survey of 2001. Then companies surveyed also showed some optimism for a fall in economic crime risks in that region. In the last two years however, our respondents in Central & Eastern Europe reported significantly more economic crime (2003: 37%, 2001: 26%). In our view it is unrealistic to expect decreases in economic crime risks without substantial actions to tackle the roots of all economic crime: motive, opportunity and a clearly perceived benefit of reward over punishment.

Figure 18: Expectation as to whether fraud risk will increase over the next 5 years



Looking forward over the next five years, 34% of companies expect their greatest economic crime risk to be asset misappropriation – currently the most frequent form of fraud worldwide – and 33% cybercrime.

Compared to our previous European survey where cybercrime was by far the greatest fear for the future (2001:43%) this is a significant decrease. Regional factors do play a role however in this analysis. Asset misappropriation is most noticeably seen as a threat in Africa (48%) and North America (52%). In the Asia & Pacific region however, cybercrime is still seen as the key risk for the future with 35% of companies citing this as their chief concern. 27% of South and Central America companies agreed with them, however a similar proportion believe that the issues of corruption & bribery will remain their greatest economic crime threat.

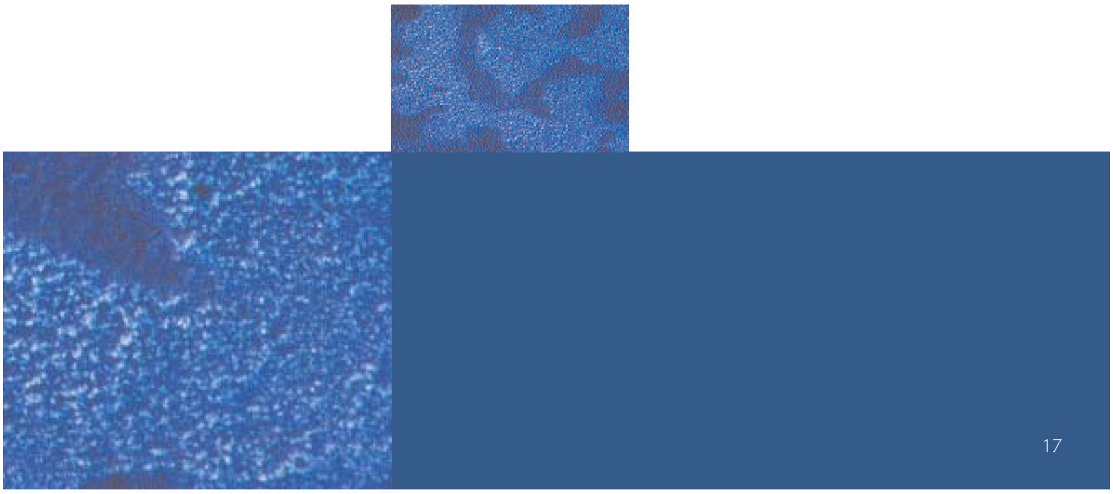
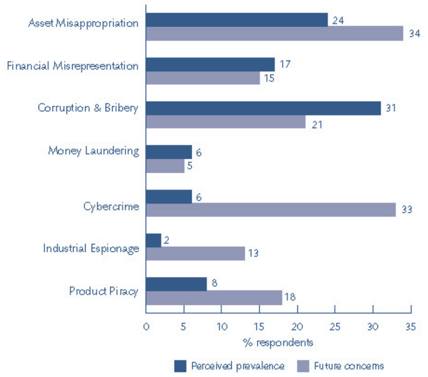


Figure 19: Frauds considered most prevalent compared with future concerns (worldwide)



The lower proportion of respondents anticipating cybercrime as the most significant future threat (figure 19) may reflect two factors. Firstly, much activity initially categorised as cybercrime was in fact 'traditional' fraud conducted by electronic means – for instance, asset misappropriation through tampering with payment data – rather than crimes now clearly defined as cybercrime such as denial of service attacks, theft of electronic data and the use of viruses. Companies now define cybercrime more accurately, and expect fewer occurrences as a result. Secondly, whilst the effects of cybercrime can be extremely severe for those companies targeted, it appears that many cyber criminals are extremely selective in their targets. Companies that have not yet been made a target may be breathing a premature sigh of relief.

18

survey demographics

This survey was the result of 3,400 interviews in 50 countries. The number of interviews conducted per country was:

Western Europe	**1476**
UK/NI/ROI	162
Austria	83
France	156
Germany	150
Norway	90
Portugal	50
Spain	106
Sweden	91
Switzerland	89
The Netherlands	103
Italy	159
Denmark	88
Greece	59
Belgium	90

Central & Eastern Europe	**378**
Czech Republic	50
Estonia/Lithuania/Latvia	25
Hungary	25
Bulgaria	25
Poland	85
Romania	29
Slovenia	27
Turkey	52
Russia	29
Slovak Republic	31

South & Central America	**554**
Argentina	96
Brazil	86
Chile	53
Columbia	48
Dominican Republic	31
Mexico	87
Guatemala	30
Peru	51
Uruguay	36
Venezuela	36

North America	**103**
Canada	103
USA	

Asia & Pacific	**878**
Australia	100
Hong Kong	85
India	85
Indonesia	85
Japan	423*
Singapore	50
Thailand	50

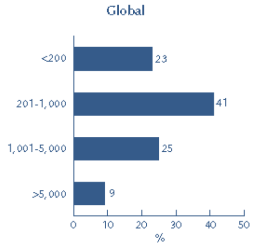
Africa	**143**
Algeria	21
Morocco	17
South Africa	91
Tunisia	14

*weighted in the statistics to reflect a base of 150 respondents

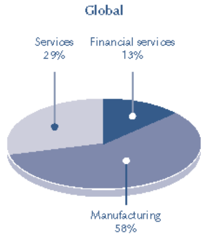
Percentages may total more or less than 100 per cent as respondents were able to provide multiple answers or may have chosen not to answer.

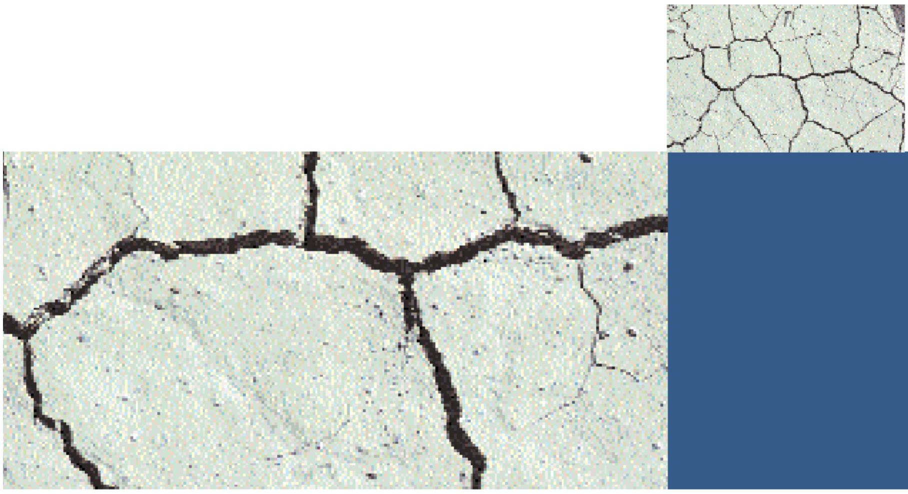
8 companies suffered economic crimes totalling in excess of US$100 million, and have been removed from the "total cost" analysis.

The size of participating organisations was as follows:



Respondents were CEOs and CFOs and those responsible for preventing and detecting fraud. They were drawn from the following industry sectors:





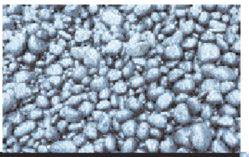
terminology

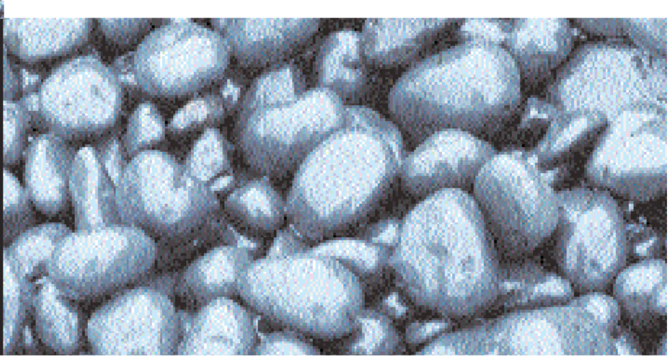
Due to diverse descriptions of individual types of economic crime in countries' legal statutes, we have developed the following categories for the purposes of this survey. The descriptions were read to each of the respondents at the start of each survey to ensure consistency.

Fraud/Economic Crime	The intentional use of deceit to deprive another of money, property or a legal right.
Asset misappropriation (inc. embezzlement by employees)	The theft of company assets (including monetary assets/ cash or supplies and equipment) by company directors, others in fiduciary positions or an employee for their own benefit.
Financial misrepresentation	Company accounts are altered or presented in such a way that they do not reflect the true value or financial activities of the company.
Corruption & Bribery (inc. racketeering & extortion)	Typically, the unlawful use of an official position to gain and advantage in contravention of duty. This can involve the promise of an economic benefit or other favour, the use of intimidation or blackmail. It can also refer to the acceptance of such inducements.
Money Laundering	Actions intended to legitimise the proceeds of crime by disguising their true origin.
Cybercrime (e.g. hacking, virus attacks, denial of service, electronic theft of proprietary information)	The illegal access to a computer or computer network to cause damage or theft.
Industrial espionage & information brokerage	The acquiring of trade secrets or company information by secretive and illegal means and/or the selling of these secrets or information to interested parties.
Product Piracy/Counterfeiting	The illegal copying and/or distribution of fake branded goods in breach of patent or copyright. This also includes the creation of false currency notes & coins with the intention of passing them off as genuine.

Other terms used in the survey

Whistleblowing	The disclosure by an employee of malpractice in the workplace
Tip-off	A hint or indication about goings-on in the organisation
Audit	The formal examination and review of a company's accounts and/ or practices.
Risk management systems	Systems put in place to assess, identify and respond to risks in the company.
Soliciting or receiving a commission	Being offered or given money or other incentives to help influence a business decision in the donor's favour.
Offering or paying a commission	Having to offer or give money or other incentives to help influence a business decision in your favour.





20

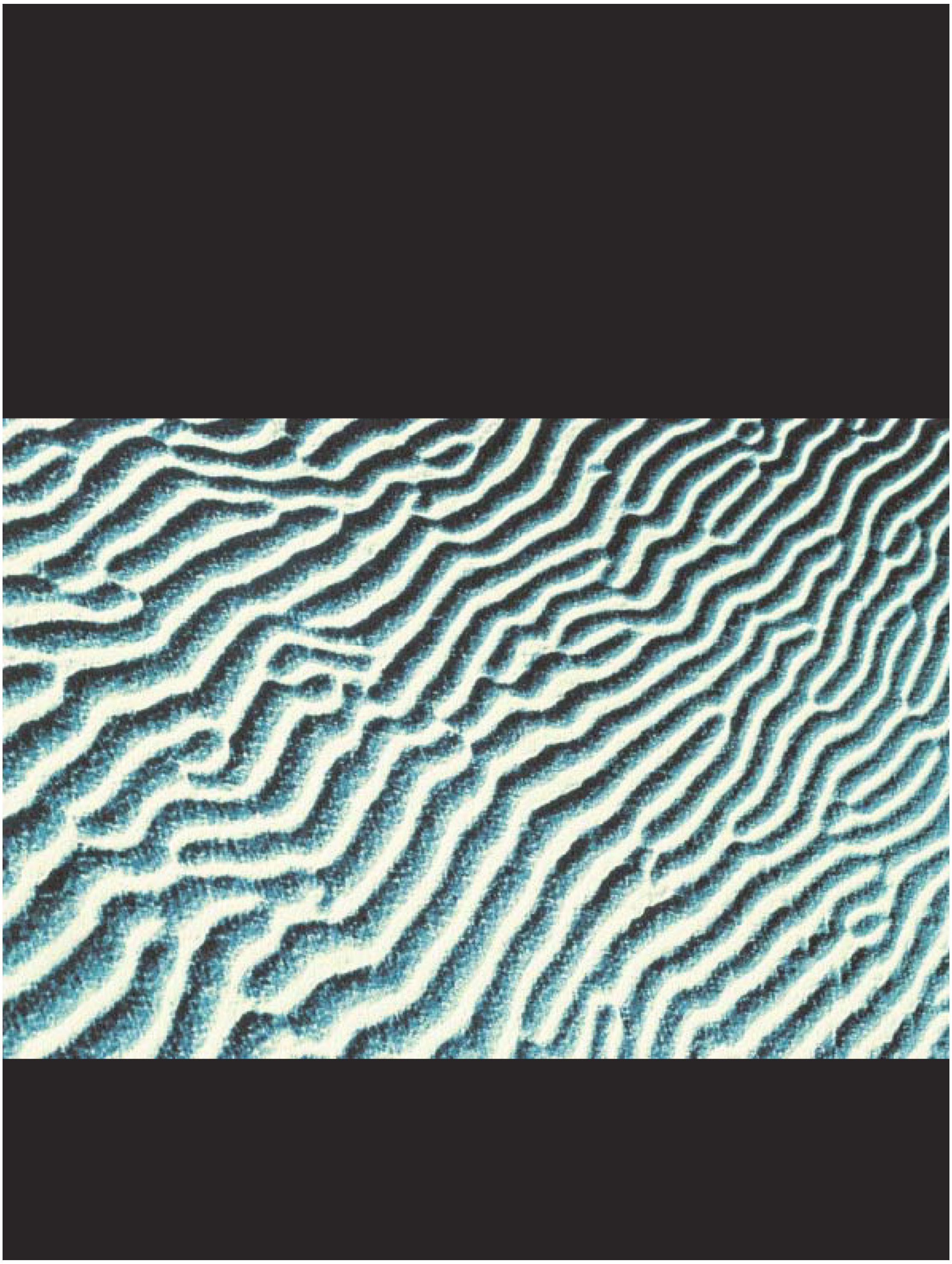
contact details

endnotes

[1] The majority of companies would have found it a near impossibility to quantify exactly the financial impact of a fraud or frauds upon them. In order to facilitate their answering of this question, we provided a series of financial ranges for them to work within:

- < US$ 10,000
- US$ 10,000 – 50,000
- US$ 50,000 – 100,000
- US$ 100,000 – 250,000
- US$ 250,000 – 500,000
- US$ 500,000 – 1 million
- US$ 1 million – 5 million
- US$ 5 million – 10 million
- US$ 10 million – 50 million
- US$ 50 million – 100 million
- > US$ 100 million

The values quoted in the report are estimates derived from a computation that assigned a midpoint to each value range for the frauds which a company reported it had been subject to. This provided a total cost of fraud for each individual company from which was calculated (1) the average figure and (2) the total figure.



© 2003 PricewaterhouseCoopers. All rights reserved. PricewaterhouseCoopers refers to the network of member firms of PricewaterhouseCoopers International Limited, each of which is a separate and independent legal entity. Designed by studio ec4 15404 (05/03).

PricewaterhouseCoopers

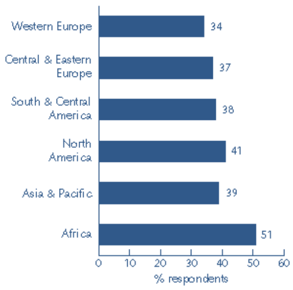
economic crime survey 2003
asia pacific

economic crime: the harsh reality

Introduction

Economic crime is an undeniable fact of business life, affecting both large and small organisations across all industries. This has been reinforced by PricewaterhouseCoopers Global Economic Crime Survey 2003, which has revealed that 39% of organisations in the Asia Pacific region have been victim to economic crime in the past 2 years.

Victims of economic crime



The Global Economic Crime Survey found that, in particular, corruption & bribery, product piracy, and cybercrime have been identified as present and future risks for organisations in the region. However, asset misappropriation and financial misrepresentation have been identified as significant risks and are far more widespread across the entire spectrum of business and industry types in the region. Unlike disaster losses, a loss resulting from employee dishonesty can accumulate over time and thus reach a disturbing magnitude. Notably, in the Asia Pacific region, 9 out of 10 organisations that suffered from economic crime recovered less than 20% of the amount lost.

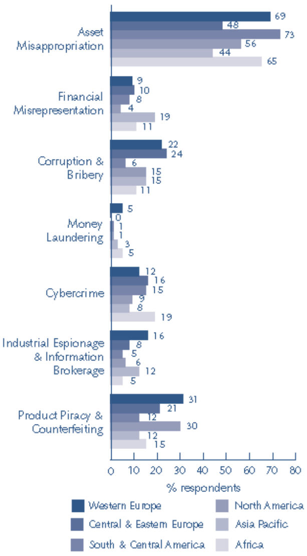
Financial loss is not the only adverse effect of economic crime on organisations. Economic crime also affects staff morale and motivation, business relationships and reputation, brand image, share price and financial market opportunities.

There is no single foolproof method for preventing economic crime, although there are a range of preventative techniques which have proved to be successful. The effective application of fraud risk management techniques will reduce the instances and impact of economic crimes in the region.

Incidence of Economic Crime in the Region

Economic crime often involves a range of activities that permeate traditional categories of crime.

Types of fraud experienced over the past two years



Corruption & bribery

The survey has revealed that 24% of organisations in the Asia Pacific region have been victims of corruption & bribery over the last two years. Moreover, 27% of organisations perceive that corruption & bribery will continue to represent a risk in future. In the region, corruption & bribery was often viewed as an acceptable element of business. It continues to be a major concern for business operations due to the increased pressure from authorities and expanding economies that are promoting and reviewing standards in relation to these crimes.

Corruption & bribery poses a risk to business performance not only in financial terms but also in the damage that may be sustained to business relationships, reputation, brand image, and potentially to financial markets confidence.

Cybercrime

The computer is a witness to an event and can be the scene of the crime

Computers are now frequently the tool used in the commission of a crime or a breach of company policy. Although only 16% of organisations in the survey reported suffering from cybercrime in the last 2 years, increasingly all incidences of economic crime depend on an element of technology. Cybercrime not only includes external threats such as viruses and denial of service attacks and credit card fraud, but also includes internal threats such as illegal or inappropriate access to computer systems to aid in the perpetration of industrial espionage, information brokerage, financial misrepresentation and product piracy.

In the Asia Pacific, 38% of organisations perceive cybercrime as their chief concern over the next 5 years. Correspondingly, the field of computer forensics has emerged and developed. Computer forensic techniques, which form a crucial part of organisational crime management strategies, enable the seizure and

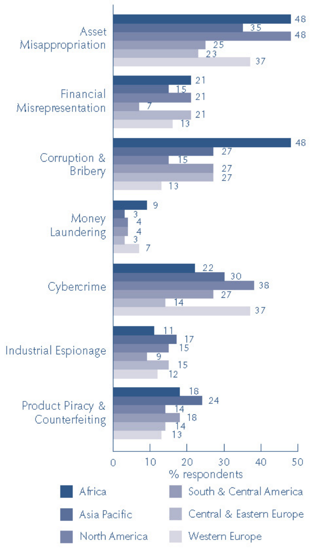
analysis of electronic data permitting the detection of, and response to, a variety of economic crimes.

Product piracy

In the survey, 24% of organisations identify product piracy as one of the chief vulnerabilities of their organisation over the next 5 years. Product piracy is one of the major economic crimes facing manufacturers and distributors of luxury brand goods and software in the Asia Pacific region. Estimates of the cost of product piracy vary considerabl. However, it is possible that up to 30% of some products are counterfeit. The Internet has created a ready environment for the advertising and distribution of counterfeit products on a global basis.

Organisations that are more susceptible to product piracy need to employ additional corrective measures to combat the risks of brand damage and lost sales. Such specific risks require particular solutions including tailored investigatory solutions (monitoring and surveillance of pirate product distributors and importers) and assistance with injunctive relief and civil restitution from product pirates.

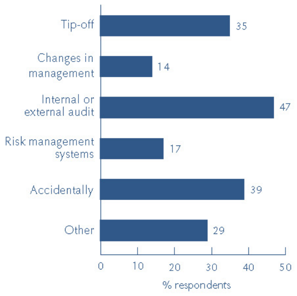
Perception of fraud risks over the next five years

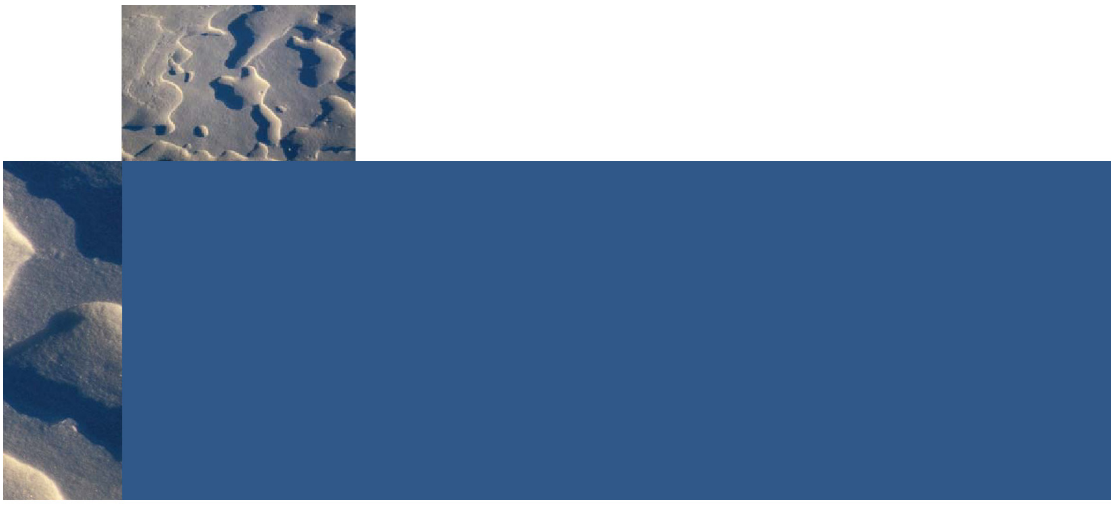


Economic Crime Prevention and Detection

Although 46% of survey respondents were "quite confident" that their controls were stronger than a year ago, only 16% of economic crimes in the Asia Pacific region were detected by risk management systems. The survey results highlight the fact that in most cases economic crimes were not detected by specific preventative or detective measures, but rather they were revealed through external or non-related business functions. The vast majority of incidences of economic crime were detected by accident, tip off, and/or internal & external audit.

Detection methods

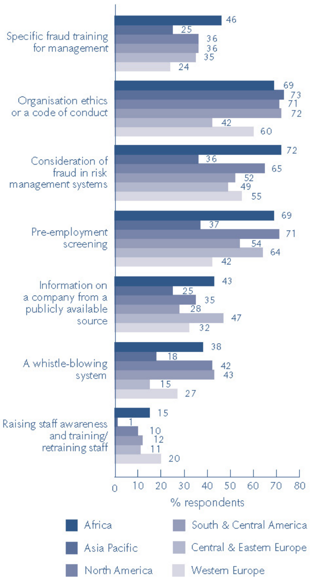




Reassuringly, the survey has shown that 75% of organisations in the Asia Pacific region have taken corrective measures to ensure that the organisation is less exposed to economic crime. In these organisations, codes of conduct were observed in three quarters of the respondents and are the most common measure employed to prevent such crimes. Other measures applied in markedly fewer instances are:

- Pre-employment screening (37%);
- The consideration of fraud in risk management (36%);
- Fraud training for management in (25%);
- Due diligence from public sources (25%); and
- Whistle-blowing (18%).

Types of corrective measures taken



These measures, if applied together, encompass part of an effective fraud risk management system. Other critical factors to consider are:

- an integrated policy that draws on every element of organisational strategy, including insurance;
- the establishment of relevant structural responsibility within an organisation;
- fraud risk assessment;
- a dedicated fraud reporting system;
- investigation standards;
- external notification procedures;
- employee awareness;
- conduct and disciplinary standards, and;
- customer and community awareness.

These factors provide a best practice standard for the prevention, detection and management of economic crime.

PricewaterhouseCoopers
Investigations & Forensic Services

Territory	City	Contact	Telephone	Email
Australia	Sydney	Malcolm Shackell	+61 2 8266 2993	malcolm.shackell@au.pwc.com
Hong Kong	Hong Kong	Tony Parton	+852 2289 2466	tony.d.parton@hk.pwc.com
India	New Delhi	Ashwani Puri	+91 11 23389483	ashwani.puri@in.pwc.com
Indonesia	Jakarta	Elizabeth Goodbody	+62 21 521 2901 6	elizabeth.goodbody@id.pwc.com
Japan	Tokyo	Peter Greaves	+81 3 3503 4015	peter.greaves@jp.pwc.com
Korea	Seoul	Hwa-Joo Bae	+82 2 709 0916	hwajoo.bae@kr.pwc.com
Malaysia	Kuala Lumpur	Yim Fun Chan	+60 3 4041 6390	yimfun.chan@my.pwc.com
Singapore	Singapore	Tim Reid	+65 236 4048	tim.j.reid@sg.pwc.com
Thailand	Bangkok	Charles Ostick	+66 2 344 1167	charles.ostick@th.pwc.com

www.pwc.com/crimesurvey

© 2003 PricewaterhouseCoopers. All rights reserved. PricewaterhouseCoopers refers to the network of member firms of PricewaterhouseCoopers International Limited, each of which is a separate and independent legal entity. Designed by studio ec4 15404 (06/03).