FORENSIC

Fraud Survey 2004 Report

ADVISORY

in collaboration with
Royal Malaysia Police

AUDIT ▪ TAX ▪ ADVISORY

FOREWORD

We are pleased to present the results of KPMG Forensic's third biennial survey of fraud in Malaysia.

Since 2000, the KPMG Fraud Survey has established a reputation as the most credible and widely quoted survey of fraud in Malaysian business. As a leading provider of forensic services, KPMG believes that it is important to quantify the trend, nature and extent of fraud in today's business environment. The Malaysian KPMG Fraud Survey is our contribution to that end.

Fraud and white collar crime have increased considerably over the recent years, and professionals believe this trend is likely to continue. The cost of fraud to businesses is difficult to estimate because not all fraud and abuse is discovered, not all uncovered fraud is reported, and civil or criminal action is not always pursued. However, the statistics we currently have show the astronomical values associated with fraud. The cost of fraud does not stop at a monetary figure with lots of noughts behind it. Its insidious nature seeps into and erodes the core elements that all business is built upon: confidence and trust.

When fraud is detected within a business, there is usually shock and disbelief that a trusted employee who resembles the "person next door" could have done what they are accused of. The initial response is "How could that have happened?" In light of the cost and characteristics of offenders, it is important to develop strategies to prevent or detect business fraud. It is also essential as the expansion of computer usage in business make organisations more vulnerable to fraud and abuse.

In order to combat fraud and white collar crime in businesses, a concerted effort must be exerted by the management of the business, the external auditors, and by all employees of the business. Everyone must realize that fraud is not a victimless crime. The cost of fraud and theft are shared by all through higher costs and lower corporate profits. A comprehensive strategy for fraud governance is essential if an organisation is to reduce the likelihood and impact of major fraud. Good fraud governance requires more than just ensuring an effective system of internal controls. It also requires a clear message and oversight from senior executives and non executives, clear policies and standards, knowledge of the key fraud risks, effective fraud reporting, fraud awareness training, and the development of a culture of high ethics and honesty.

We are conscious of the fact that our study will be a significant benchmark analysis of fraud in this country. It is, therefore, with a deep sense of responsibility that we share these findings with you. We hope that you find the results of this survey as insightful as we do.

We take this opportunity to express our appreciation to the people and businesses who took the time and effort to participate in this survey and share their thoughts and experiences with us. Without their support, this report would not be possible.

Let us all hope that we have all made a small beginning in the right direction to combat fraud within corporate Malaysia.

EXECUTIVE SUMMARY

The findings summarized below are of particular importance:

- 62% of respondents felt that fraud is a major problem for Malaysian business generally.
- 83% of respondents acknowledged experiencing fraud in their organization. This is an increase of 33% from the 2002 survey.
- 36% of companies suffered total losses of RM10,001 to RM100,000 to fraudulent conduct in the survey period while 17% suffered losses in excess of RM 1 million (the "survey period" is the period from January 2003 to December 2004).
- Good internal controls (44%), management investigation (37%) and internal audit review (29%) rank highly as methods of fraud detection.
- 87% of the frauds were perpetrated internally [non–management employees (69%) and management employees (18%)]. This was a decrease of 10% from the 2002 survey.
- Inadequate internal controls and collusion between employees and third party were cited as the most common reason giving rise to fraud.
- The four most common prevention methodologies were indicated as being review and improved internal controls, improved security measures, pre–employment screening and establishing a corporate code of conduct / ethics.
- 30% of the respondents that experienced fraud indicated that "red flags" or warning signs which should have alerted respondents to the fraud were ignored by either management or supervisory personnel.
- Secret commission / kickbacks (25%) and lapping & kiting* (21%) were the two most common types of fraud encountered. A comparison with the last survey showed an increase of 15% in secret commission / kickbacks and 5% in lapping & kiting.
- The typical fraudster is male within the age group of 26–40 years and has an annual income of RM15,000–RM30,000. Most frauds reported by respondents were committed by individuals employed between 2–5 years.
- 85% of respondents considered computer / information system to be a potential security risk.
- 38% of respondents considered intellectual property to be at the risk of fraud.

* Lapping is the act of fraudulently withholding cash receipts and covering up the current deficiency by depositing subsequent receipts.

Kiting is defined as the act of fraudulently misstating the accounts of an organization by showing the same amount of deposit simultaneously in two of its bank accounts. Depositing in one bank account a cheque drawn on another and recording in the books of the accounts only the deposit on the day of the transfer can accomplish this.

TABLE OF CONTENTS

ABOUT THE SURVEY

In January 2005, KPMG Forensic Malaysia circulated a fraud survey questionnaire to the chief executives of all the public listed companies on the Bursa Malaysia. As it is sometimes difficult and often a sensitive subject, respondents were given the option to remain anonymous.

For the purpose of this survey, "fraud" is defined as a deliberate deceit planned and executed with the intent to deprive another of property or rights directly or indirectly, regardless of whether the perpetrator benefits form his / her actions. Silence, when good faith requires expression, constitutes deceit.

The objective of this survey was to determine the overall level of fraud, fraud awareness and fraud prevention measures amongst senior management. The survey period is from January 2003 to December 2004.

Participants in this survey were asked questions relating to:

- Their opinion as to the extent of fraud in business within their own company;
- Fraud experienced against their organization;
- Actions taken when fraud was detected;
- Their company's vulnerability to fraud;
- How fraud is prevented or detected;
- Business ethics and corporate governance.
- Their opinion on information security within their company and the level of preventative measures in place; and
- Their opinion on the risk of intellectual property fraud and the level of preventative measures in place.

A total of 130 responses were received for this survey, which represented 14% of the total number of companies listed on the Bursa Malaysia as at 1 January 2005*.

* The total number of companies listed on the Bursa Malaysia as at 1 January 2005 is 900 (622: Main Board, 278: Second Board).

PROFILE OF RESPONDENTS

Survey respondents

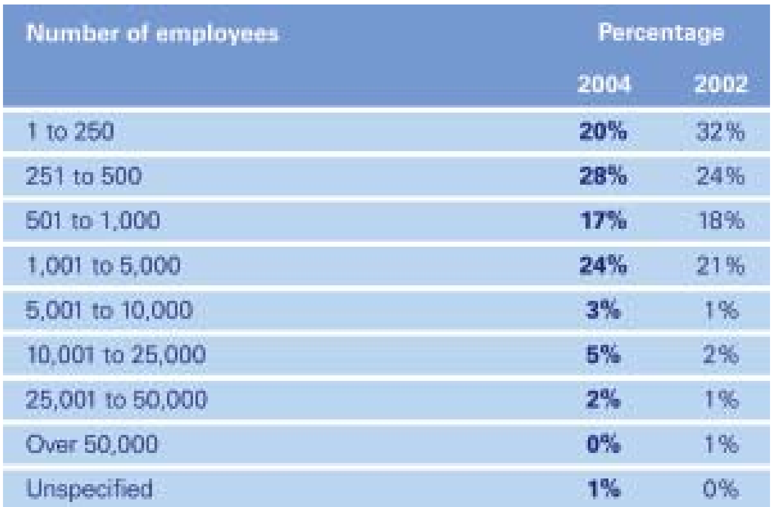
The industry sector profile of the 2004 survey respondents as compared with those in the 2002 survey is as follows:

Industry	Percentage	
	2004	2002
Manufacturing	**17%**	23%
Consumer Products	**15%**	12%
Construction and Engineering	**14%**	13%
Financial Services	**11%**	6%
Real Estate	**8%**	5%
Industrial Products	**7%**	7%
Utilities	**4%**	2%
Electronics / Technology	**2%**	5%
Energy / Petroleum	**2%**	2%
Hospitality	**2%**	2%
Management / Holding Company	**2%**	3%
Publishing / Printing	**2%**	1%
Transport	**2%**	5%
Others	**12%**	14%

The survey questionnaires were, for the most part, completed by Chief Financial Officers / Controllers. The profile of the 2004 participants as compared with those in the 2002 survey is as follows:

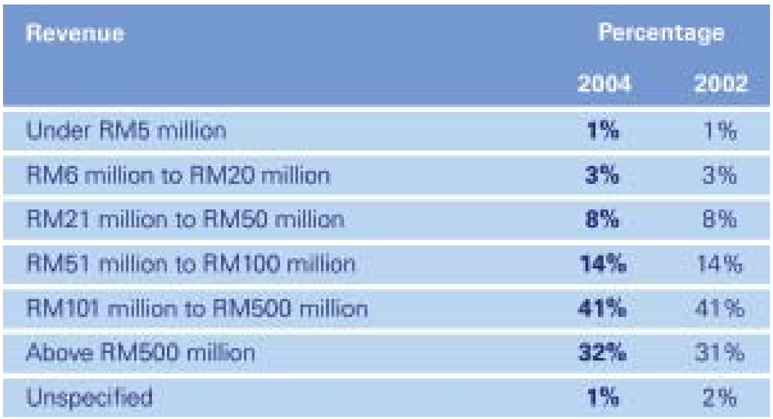
Position	Percentage	
	2004	2002
Chief Financial Officer / Controller	**30%**	37%
Head of Internal Audit	**20%**	19%
Chief Executive Officer	**19%**	10%
General Manager	**5%**	4%
Chief Operating Officer	**2%**	5%
Head of Security / Investigation	**2%**	1%
Others	**22%**	24%

The table below indicates the number of people employed by the respondents' organization:



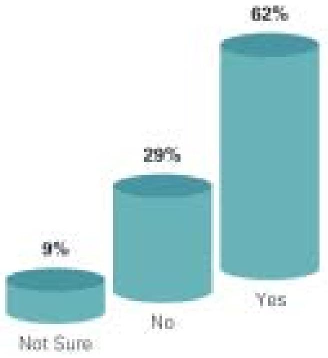
Number of employees	Percentage	
	2004	2002
1 to 250	**20%**	32%
251 to 500	**28%**	24%
501 to 1,000	**17%**	18%
1,001 to 5,000	**24%**	21%
5,001 to 10,000	**3%**	1%
10,001 to 25,000	**5%**	2%
25,001 to 50,000	**2%**	1%
Over 50,000	**0%**	1%
Unspecified	**1%**	0%

This survey included organizations with annual revenues ranging from less than RM5 million to revenues in excess of RM500 million.



Revenue	Percentage	
	2004	2002
Under RM5 million	**1%**	1%
RM6 million to RM20 million	**3%**	3%
RM21 million to RM50 million	**8%**	8%
RM51 million to RM100 million	**14%**	14%
RM101 million to RM500 million	**41%**	41%
Above RM500 million	**32%**	31%
Unspecified	**1%**	2%

OPINIONS OF FRAUD



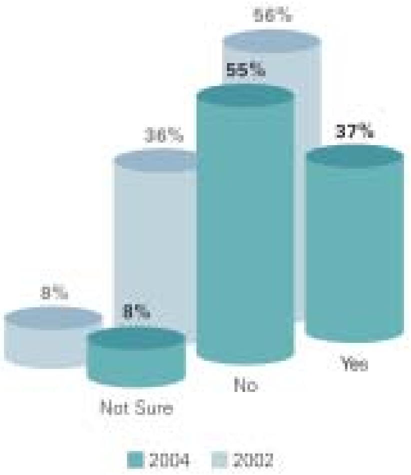
Is fraud a major problem for Malaysian business today?

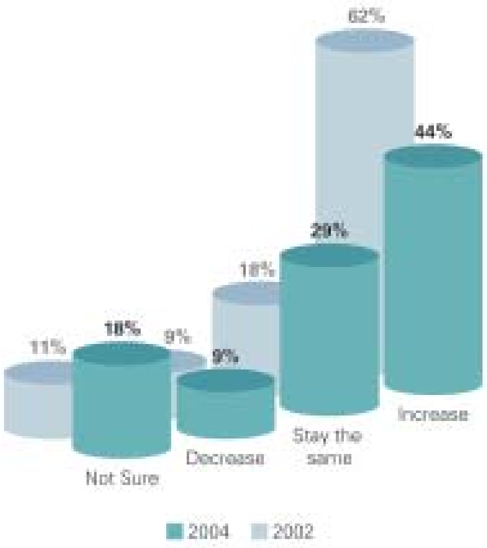
The well–publicized corporate scandals of recent years have brought the issue of fraud to the forefront of management's attention, particularly the threat of fraud occurring within the organization itself. Globally, organizations are beginning to look inward to better understand the fraud risks inherent within their organizations and to proactively manage the risks of fraud.

We were interested to find out the general view of organizations towards fraud in Malaysia today. It is interesting to note that the majority (62%) of respondents felt that fraud is a major problem for Malaysian business generally.

Is fraud a major problem for your business?

Respondents were then asked whether fraud is a major problem within their business. 37% believe it is a major problem. Those who did not view this as major problem attribute this to the effective security in place (76%) and the business (13%) or industry (10%) which does not attract fraud.

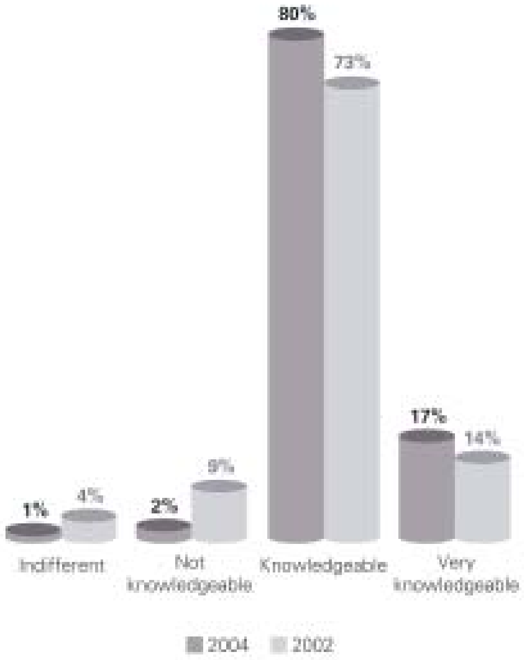




Will fraud increase, decrease or stay the same in the future?

We also asked respondents whether fraud will increase, decrease or stay the same over the next 2 years. 44% of respondents believed that fraud will be on the increase in the next 2 years.

CORPORATE GOVERNANCE

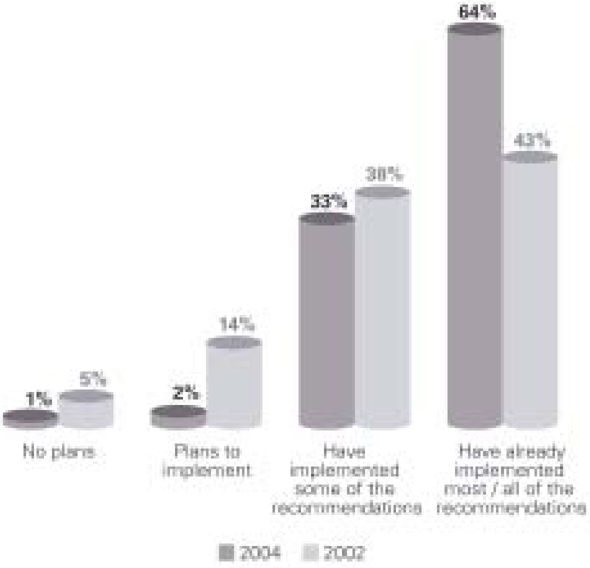


Awareness about corporate governance

Survey participants were asked to indicate their level of knowledge or awareness regarding the Code of Corporate Governance. 17% of the respondents claimed to be very knowledgeable while 80% claimed to be knowledgeable.

Are there any plans to improve corporate governance?

Survey participants were also asked if their organization has taken or plans to take any action towards improving corporate governance. 64% responded that their organizations have implemented most of the recommendations while 33% have implemented some of the recommendations towards improving corporate governance.



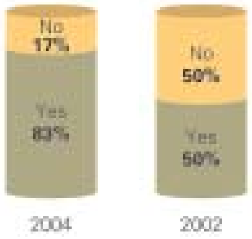
FRAUD EXPERIENCE

Awareness of fraud

To more clearly understand the impact of fraud, the factors that contribute to it, and tell the ways in which it is detected and dealt with, we asked organizations to tell us more about the fraud detected during the survey period.

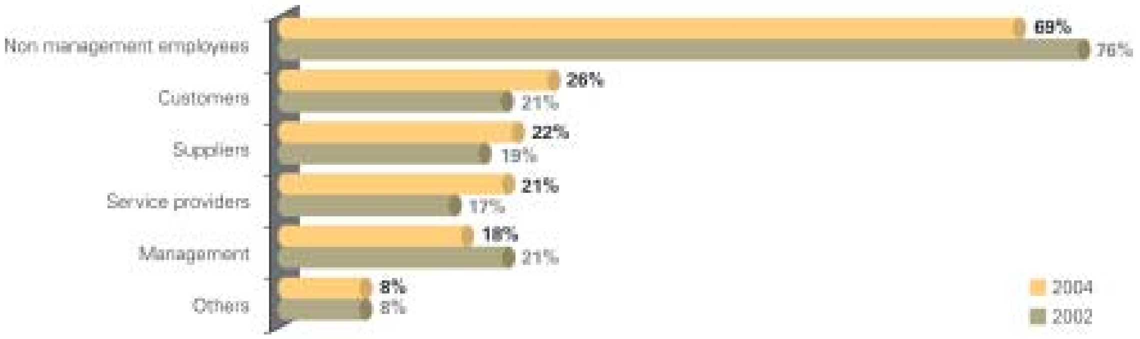
Occurance of fraud

Respondents were asked if they were aware of any fraud that had occurred in their organizations in the last 2 years. 83% of the respondents indicated that their organization had been affected by fraud. This was an increase of 33% from the 2002 survey.



What were the sources for the occurrence for fraud?

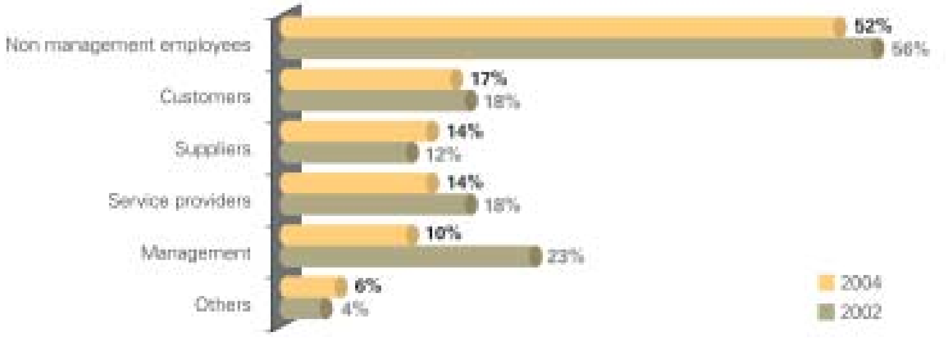
Of the total 109 respondents that expericed fraud, 69% claimed that their non–management employees were the most significant perpetrators of fraud whilst 18% claimed it was their management. On the other hand, external sources of fraud perpetrators were customers (26%), suppliers (22%) and service providers (21%).



[Note that some respondents indicated more than one response]

Sources of the largest financial losses due to fraud

To obtain an understanding of the impact of fraud and in which areas fraud risk was highest, we asked survey participants to comment on the source of losses suffered. Of the sources identified, non–management employees (52%) were the source of their largest financial loss, followed by customers (17%), suppliers (14%) and management (14%).



[Note that some respondents indicated more than one response]

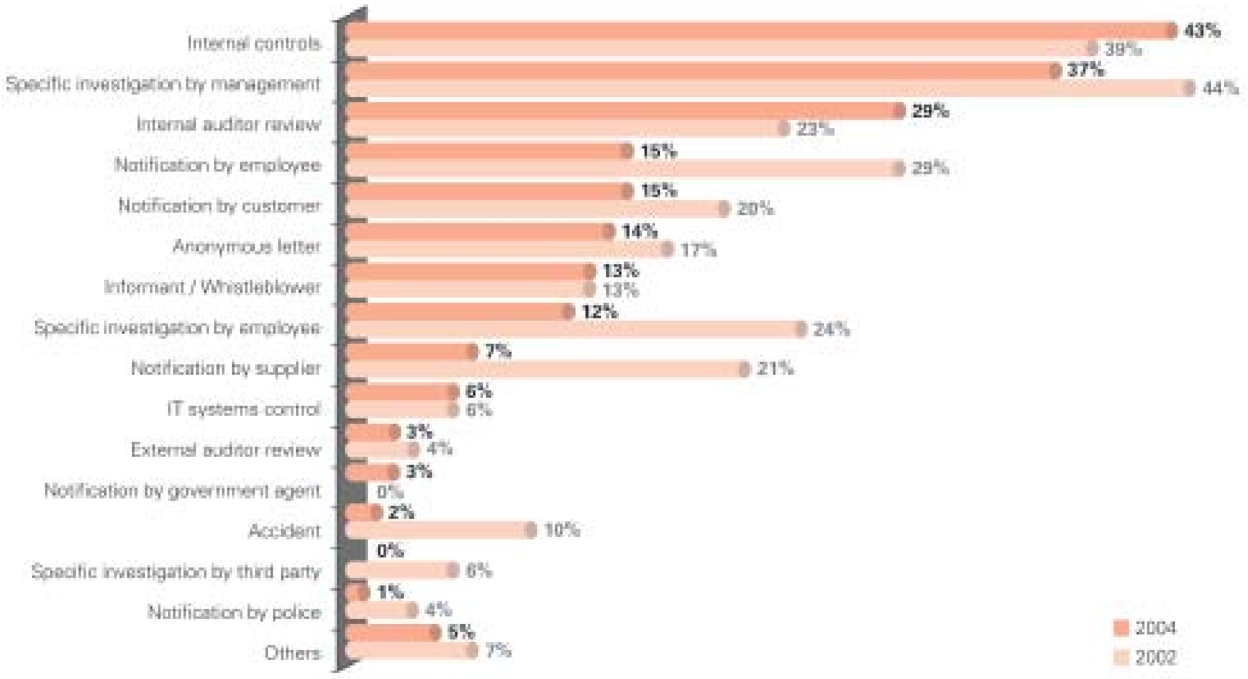
It is certainly a cause for concern that the very people entrusted to run and operate an organization are often themselves the perpetrators of fraud. Our findings underline the importance of implementing a broad–based fraud risk management strategy that extends beyond a set of sophisticated internal controls. A broad–based fraud risk management plan should include:

- A sound fraud and ethics policy;
- A periodic fraud risk assessment;
- An effective internal audit function;
- A well defined and independent whistle blowing hotline;
- Stringent pre–employment screening; and
- A fidelity guarantee insurance policy.

FRAUD DISCOVERY

How was the fraud discovered?

Survey participants were also asked to indicate how the frauds were discovered. In several cases, respondents discovered fraud by more than one method. The most common method of detecting fraud was through internal controls (43%), which increased 4% from the last survey. Investigation by management (37%), internal auditor review (29%), notification by employee (15%) and notification by customer (15%) were the other methods of fraud detection.



[Note that some respondents indicated more than one response]

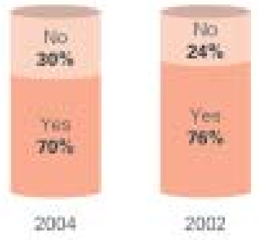
Overall, fraud was detected internally and these internal methods of detection were far more effective than any other external mechanisms.

The findings highlights the importance of implementing a well–defined and independent channel for whistle blowing, developing management's ability to identify "red flags" and establishing an effective internal audit function to enable early detection of fraud.

Whistle blowing is one of the most effective means of fraud detection. Having a well–defined and protected channel for reporting incidents or suspicions of fraud facilitates whistle blowing, which can lead to early detection of fraud. An independent conduit that ensures the anonymity of the whistleblower will further encourage whistle blowing in an organization.

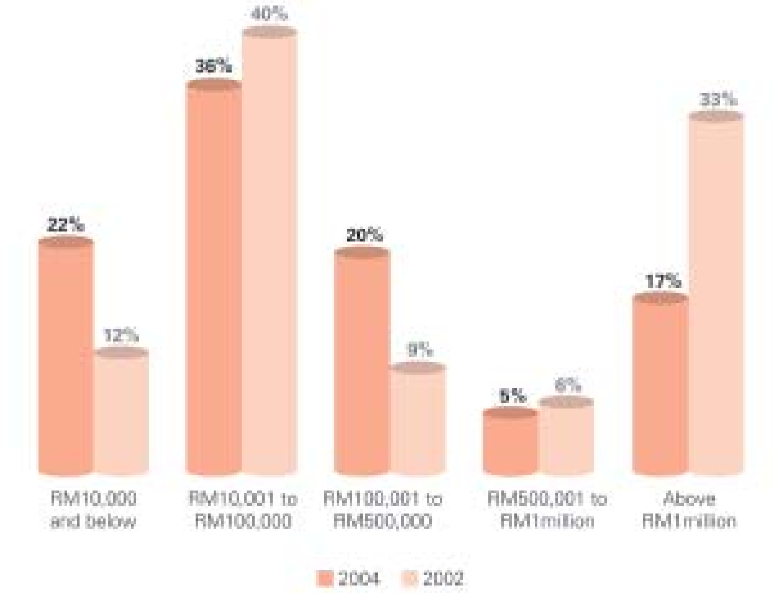
Are you aware of the amount of loss suffered due to fraud?

Out of these, 70% of the 109 businesses who have acknowledge experiencing fraud in the past were aware of the amount of losses their business suffered.



What is the estimated loss due to fraud?

It is revealing to note that 36% of the companies suffered losses in excess of RM10,001 to RM100,000 over the past years due to fraud. 17% of the companies suffered losses above RM1 million, while 22% reported incurring losses of RM10,000 and below as a result of fraud. These findings disclose the growing importance of fraud risk management within organizations today.

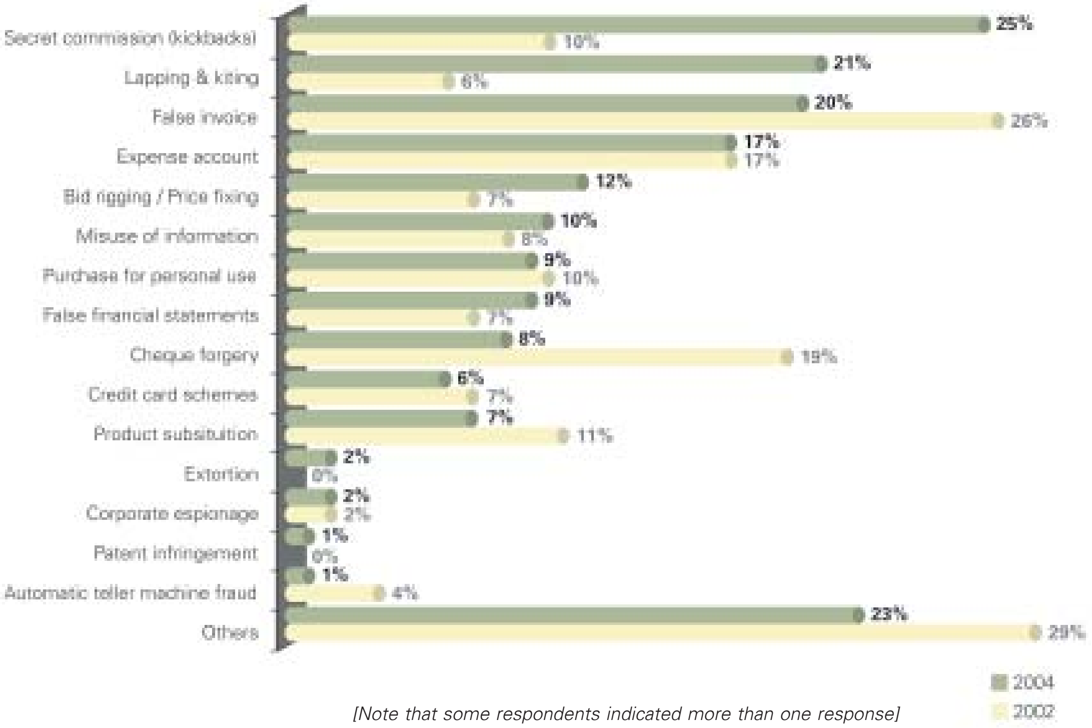


AREAS OF LOSSES DUE TO FRAUD

In which areas did the majority of losses due to fraud occur?

Secret commission / kickbacks (25%) and lapping & kiting (21%) were the two most common types of frauds encountered. Following closely behind were fraud relating to false invoices (20%), expense account (17%), bid rigging / price fixing (12%) misuse of information (10%) and purchase for personal use (9%). A comparison with the last survey showed an increase of 15% in secret commission / kickbacks and 5% in lapping & kiting.

These figures indicate that even in this age of information technology and electronic commerce, businesses should also maintain their guard against traditional frauds. Businesses, which overlook or ignore the physical aspects of security, take on an unnecessary risk.

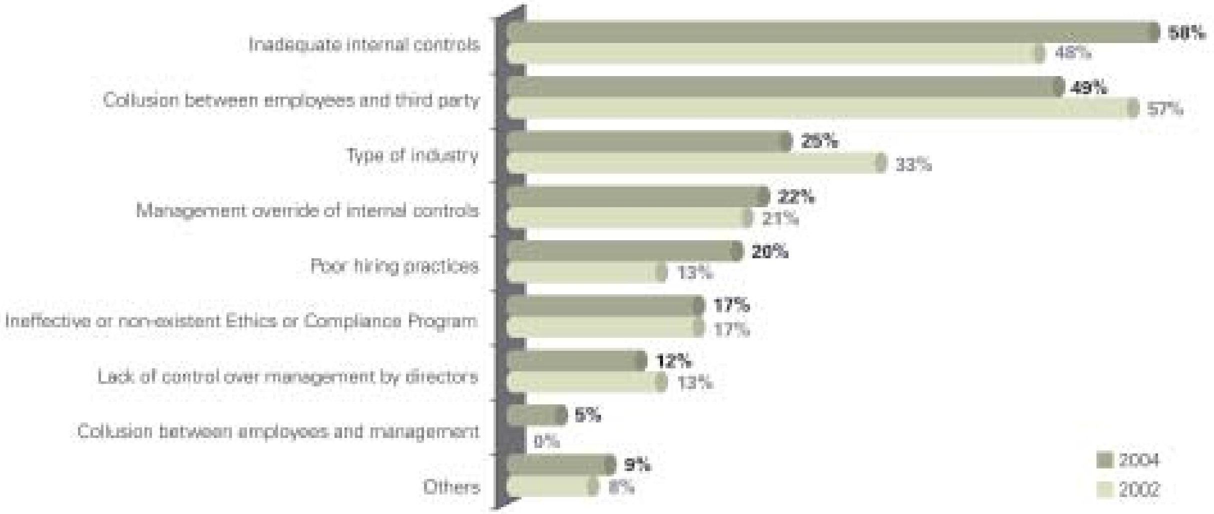


[Note that some respondents indicated more than one response]

WHY THE FRAUD OCCURRED

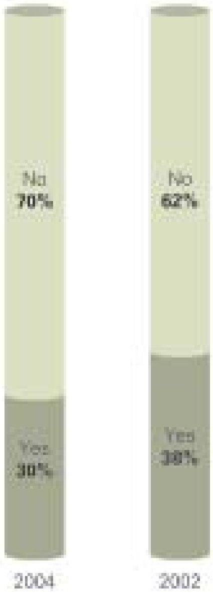
What allowed the fraud to take place?

Effective internal controls are crucial in preventing and detecting fraud. The responses indicated that the major factor allowing fraud to occur was inadequate internal controls (58%) and the collusion between employees and third party (49%). These two factors combined represented the most important pre–condition for fraud.



[Note that some respondents indicated more than one response]

Were “Red Flags” or warning signs ignored?



“Red Flags” are early warning signs or indicators that fraud may have occurred. 30% of the respondents indicated that “red flags” or warning signs were ignored by either management or supervisory personnel. Compared to the 2002 survey, there has been a decrease of 8%.

Examples of red flags:

- Refusing to take leave;
- Resigning suddenly or failing to attend work for no apparent reason;
- Drugs;
- Management who take an unusual interest in certain elements of the organization's business;
- Management overriding controls;
- Habitual gambling; and
- Persistent anomalies.

Had these warning signs been acted upon, the earlier discovery of the fraud would most likely have resulted in reduced losses. In this regards, fraud awareness among employees and managers of an organization is a vital component of any anti–fraud strategy.

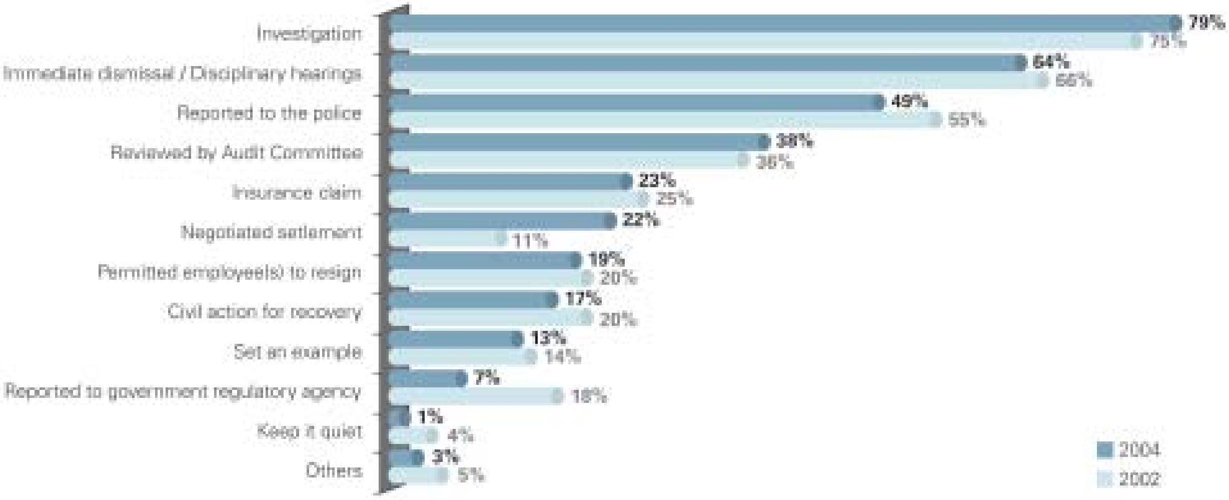
ACTIONS TAKEN CONCERNING DETECTED FRAUD

What did you do regarding the fraud?

When fraud, particularly internal fraud is detected, the victim organization and the organization's leadership invariably find themselves dealing with an unwanted and distracting crisis. The organizational response to this crisis is often marked by conflicting and competing priorities and agendas.

Careful consideration of the cost, benefits and implications of all possible actions when dealing with fraud incidents is important to avoid sending wrong signals to potential fraudsters. Choosing the option of resolving the problem quietly to avoid adverse publicity or save time and costs may give the impression that not a serious view on fraud is taken by management. On contrary, taking stern actions will demonstrate management's commitment to dealing with fraud severely. An appropriate tone from the top is therefore critical to the creation of an ethical environment which will facilitate effective and efficient management of fraud risks.

A significant number (79%) of the companies, responded to the detection of fraud with an investigation to find out what went wrong. The other actions taken included immediate dismissal / disciplinary hearing (64%), reported to the police (49%), reviewed by audit committee (38%) and insurance claim (23%).

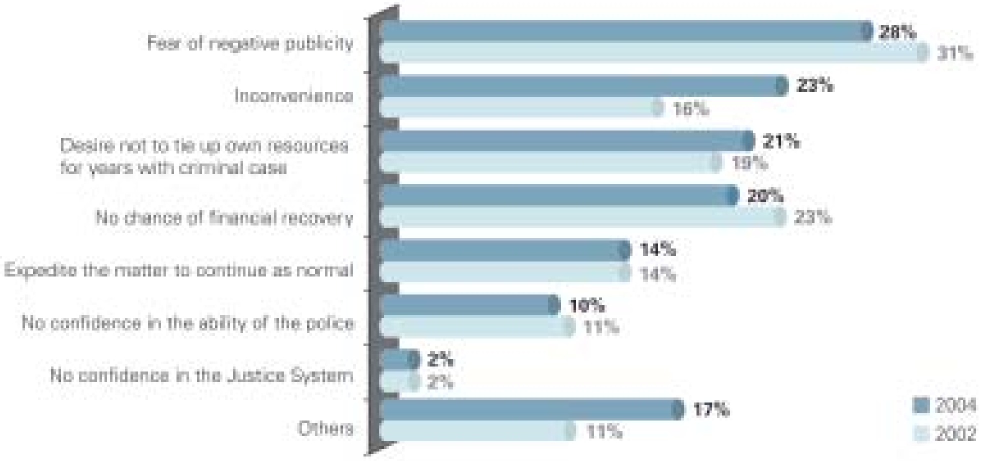


[Note that some respondents indicated more than one response]

What would be the main reason for not reporting fraud detected within your organization to the police?

It is important to note that when investigations are not properly conducted, not only will vital evidence remain undiscovered, but such valuable evidence may also be lost or unknowingly destroyed and the organization may fail to uncover other instances of fraud.

Fear of negative publicity was cited as the most common reason for not reporting fraud.



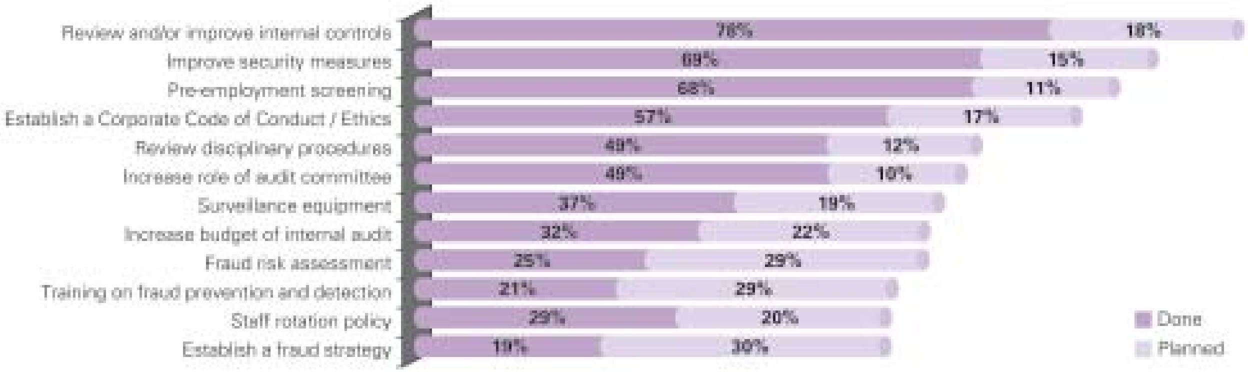
[Note that some respondents indicated more than one response]

FRAUD DETECTION AND PREVENTION

What steps are planned to reduce the possibility of fraud?

By matching fraud risks to existing controls and implementing enhanced controls where existing controls are inadequate, organizations can reduce their exposure to fraud and prevent fraud from taking place.

The most significant initiative to reduce the risk of fraud concerns the review of internal controls (78%), improving security measures (69%) and screening of new employees (68%) and establishing a Corporate Code of Conduct / Ethics (57%) are four of the most frequently citied actions taken for prevention of fraud.

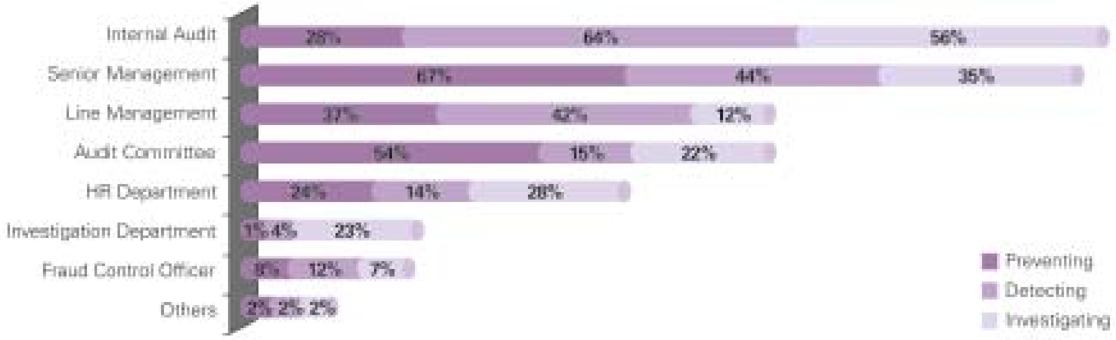


[Note that some respondents indicated more than one response]

Within your organization who takes ultimate responsibility for preventing, detecting and investigating fraud?

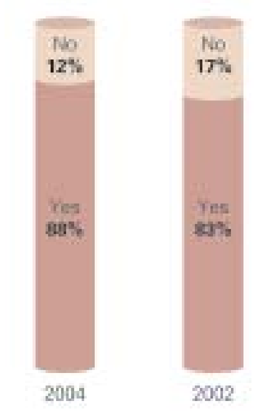
Having well–defined responsibilities for managing fraud risks can help an organization speed up the implementation of preventative measures and the investigation of suspected fraudulent activities. We asked respondents who in their organisations are responsible for overall fraud prevention, detection and investigation.

The majority of respondents indicated that the internal audit of their organization held this responsibility.



[Note that some respondents indicated more than one response]

SCREENING PROCEDURES



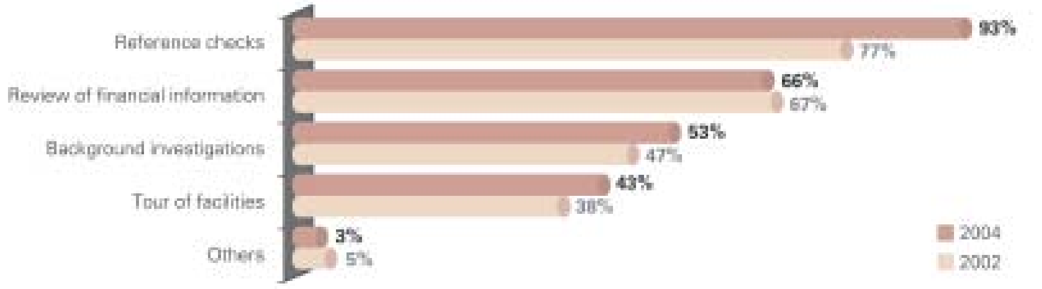
Does your organization have screening procedures in place?

One of the most effective ways of reducing the risk from fraud is by stopping the fraudster from ever joining the employment of your organization through trained personnel and effective recruitment procedures.

88% of respondents indicated that they have screening procedures in place while 12% indicated that they have no such procedures. In the 2002 survey, 83% of respondent confirmed having screening procedures in place. Taking into consideration that most respondents indicated that employees were main source of frauds and were also responsible for the largest financial losses, it would appear that employee screening is an important element in a total anti–fraud strategy.

What screening procedures are in place?

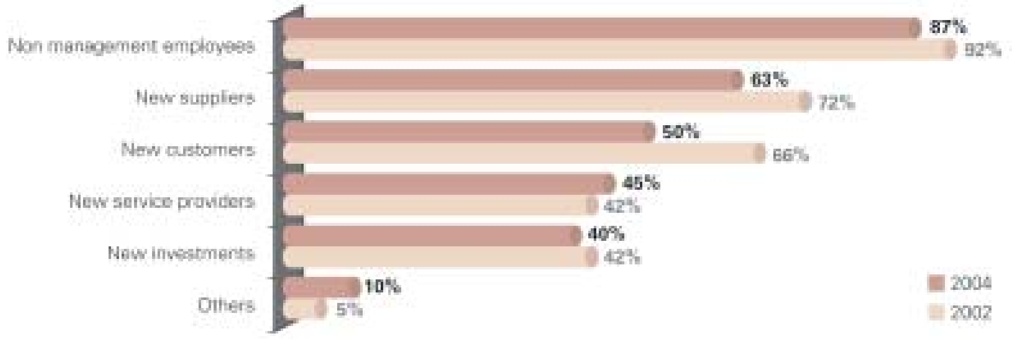
These respondents were then asked to identify screening procedures they have in place. 93% conduct reference checks while 66% review financial information.



[Note that some respondents indicated more than one response]

In which areas have screening procedures been implemented?

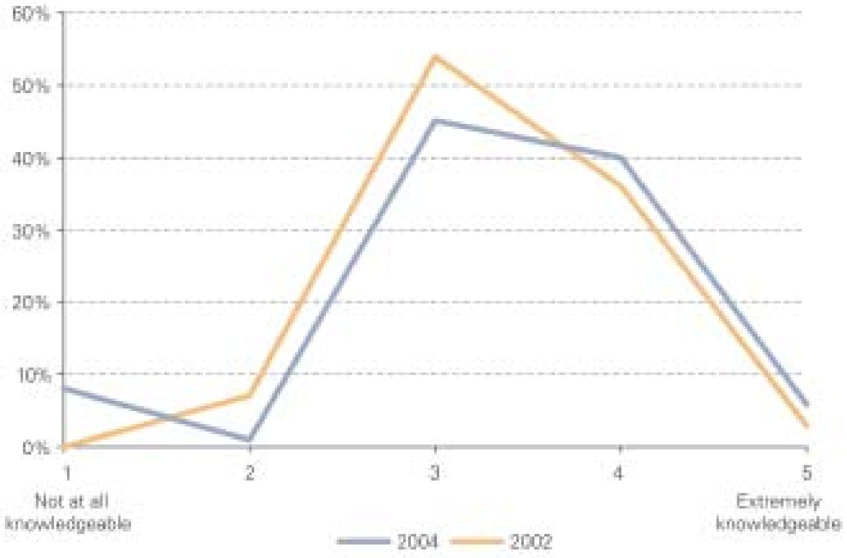
Of the 115 respondents who indicated that they have screening procedures in place, the majority (87%) indicated that these procedures are utilised primarily during the appointment of new employees.



[Note that some respondents indicated more than one response]

FRAUD KNOWLEDGE

Survey respondents were asked how knowledgeable they were about the ways in which fraud could occur in an organization. 6% indicated that they were extremely knowledgeable while 45% indicated average knowledge.



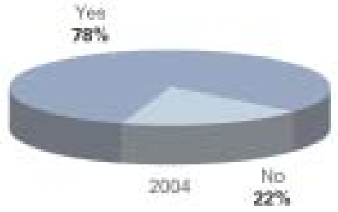
BUSINESS ETHICS

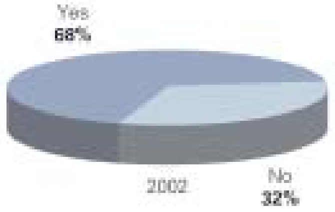
Creating an ethical environment in which fraud is seen as unacceptable is a cost–effective way of to minimise the risks of fraud. To create an ethical environment, it is important for top management to set the right tone for the rest of the organization. Without clearly defined policies, procedures and boundaries, what constitutes acceptable behavior in an organization become blurred.

Does your organization's internal manuals and written policy documents contain guidelines about acceptable ethical behavior?

We asked respondents their views on how well fraud and ethics policies and operational procedures are documented and communicated with the organization.

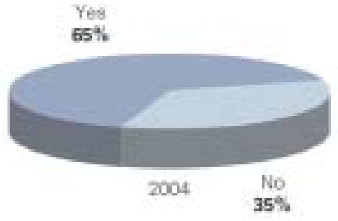
Most respondents stated that their organization have at least some form of documentation (78%) containing guidelines about acceptable ethical behaviour.

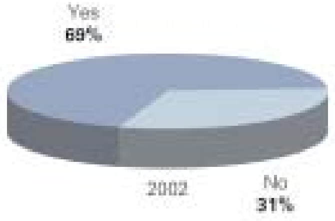




Do you communicate ethical standards to your employees, suppliers and customers?

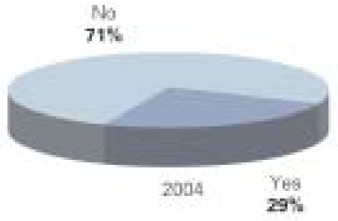
65% of companies communicate ethical standards to its employees, suppliers and customers.

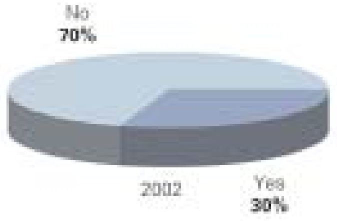




Is there an ethics officer in your organization?

71% of companies do not have an ethics officer or an ethics committee that can deal with the ethical issues in the organization.





INFORMATION SECURITY

Do you transmit sensitive / private information by means of the following media?

Respondents indicated the most common methods of transmitting sensitive material to be:

Type	Percentage
Courier	83%
Telephone	75%
Fax machine	72%
E-mail (non-internet)	67%
Internet	35%
Others	22%

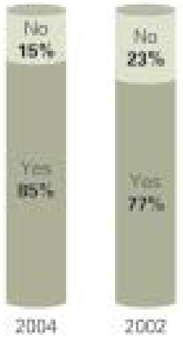
[Note that some respondents indicated more than one response]

Respondents further indicated that they believed the following methods provided inadequate security for the transmission of sensitive information:

Type	Percentage
Internet	77%
Fax machine	69%
Telephone	59%
E-mail (non-internet)	56%
Courier	43%
Others	88%

[Note that some respondents indicated more than one response]

Despite courier, telephone, fax machine and email (non–internet) having a high percentage of use, they have a high percentage of inadequate security in the transmittal of sensitive information. 55% of the respondents indicated that they did not employ caller identification on telephones, 90% do not use mobile phone encryption, 81% do not use fax encryption and 65% do not use internet encryption.



Do you consider your computer / information system as a potential security risk?

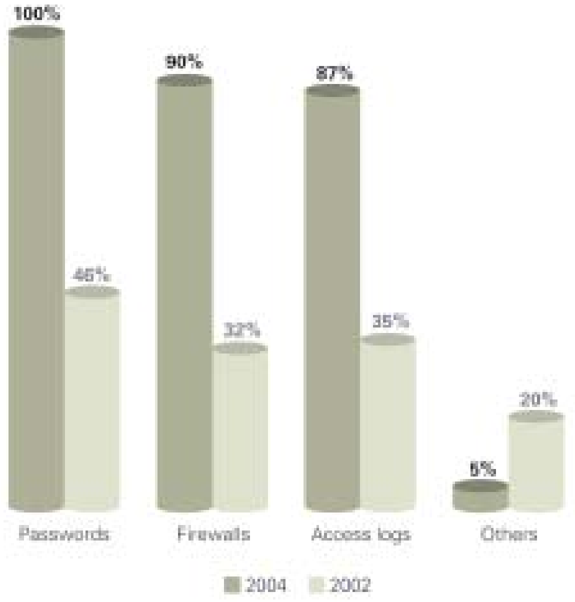
When asked on whether computer or information systems are considered as a potential risk in their organization, 85% of the respondents agreed to that statement while only 15% disagreed. This is a increase of 8% from the 2002 survey.

16% of repondents stated that more than 70% of the companies documentation are kept electronically while 25% stated that 50% to 70% of the companies documentation is kept electronically.

87% respondents cited that they routinely shred or destroy documents in order to dispose of them.

What procedures are in place to minimize security risk?

Respondents who consider their computerized information systems to be potential security risks were then asked to identify all the security procedures they have in place in their organization to minimise these risks. All respondents stated that they use passwords, 90% use firewalls and 87% have access logs as part of their computer information security.



[Note that some respondents indicated more than one response]

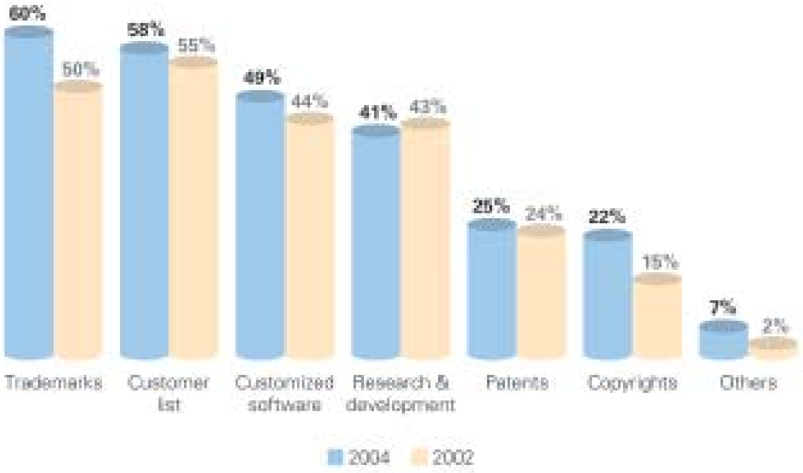
Survey participants were asked if they were aware of any financial or information loss due to security breaches involving their IT System. Of the 130 survey participants who responded to this question, only 17% of respondents indicated that a security breach had occurred. The breaches were caused by abuse of passwords / privileges (55%), lack of segregation of duties (46%), hacking (27%) and manipulation of weakness in the current IT system (23%).

50% of the breaches were caused by normal users followed by IT staff (32%) and external hackers (32%).

INTELLECTUAL PROPERTY

Does your organization have any form of intellectual property?

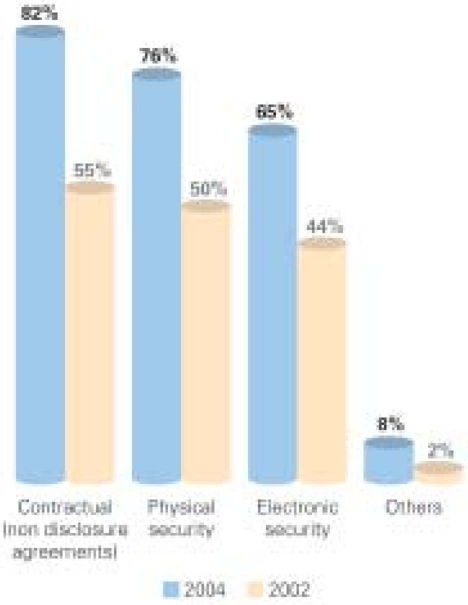
When asked if companies owned some form of intellectual property, 59% indicate ownership of some form of intellectual property, while 38% considered it to be at risk for fraud while 62% considered it to be at no risk.



[Note that some respondents indicated more than one response]

Procedures to minimize intellectual property fraud

Those respondents who considered their intellectual property to be at risk indicated the following procedures in place to minimize this risk:



[Note that some respondents indicated more than one response]

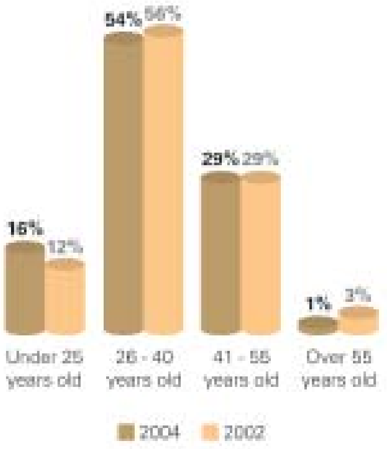
PROFILE OF FRAUDSTER

“A dedicated, intelligent person with sufficient motivation can circumvent any system of control”

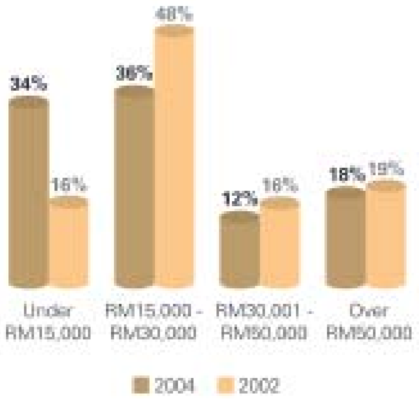
Respondents were asked to provide statistical information regarding the individual(s) committing fraud against their organization. Based on the responses provided, the profile of the typical fraudster is:

- Male (72%)
- 26 – 40 years old (54%)
- Income range RM15,000 – RM30,000 (36%)
- Period of employment 2 – 5 years (46%)

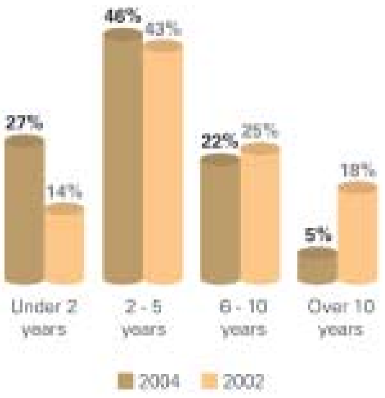
Age profile of fraudster



Income profile of the fraudster



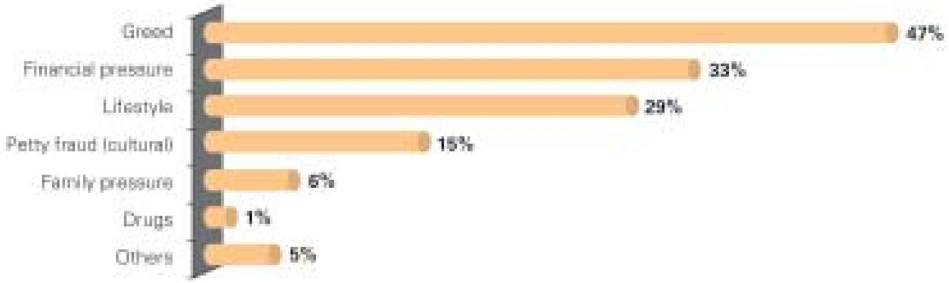
Period of employment of fraudster



Motivation for fraud

Fraud will occur if the right combination of worthwhile outcome, opportunity (which effectively is represented by poor internal controls) and motivation is present. Logically, fraud is more likely to occur when there is strong motivation for financial gain, in other words, the perpetrator has a strong desire to obtain funds that are, in many cases, needed for very specific and compelling purposes.

The 2004 survey, for the first time, considered in detail the issue of motivation. The overall results are set out as follows:



[Note that some respondents indicated more than one response]

The most common motivating factor by value of loss was greed.

INITIAL ACTION IN THE EVENT OF FRAUD

When fraud occurs or is suspected, management is sometimes tempted to resolve the matter internally. This may expose the organization to significant risk. When you become aware of incidents or suspicions of fraud in your organization, we recommend that you consider the following:

Do not

- Respond emotionally or act hastily.
- Immediately confront the suspects.
- Damage or mark any evidence or potential evidence.
- Limit the scope of your concerns to a specific issue.

Do

- Be objective in your assessment.
- Limit the number of people whom you discuss your suspicions.
- Carefully preserve any evidence by removing access to documents and electronic media.
- Call in the professionals.

General investigation rules

- Preserve the evidence – documents, computers, personal laptops, voicemails, emails, phone logs, security camera tapes.
- Focus on the facts. Be objective. Avoid communicating judgments / conclusions and making accusations unless evidence has been obtained.
- Guard against legal exposures to defamation, libel and slander, and also wrongful invasion of privacy (through improper searches of desk, lockers, personal storage), violations of law on audio / videotaping of conversations and the use of threats, promises, inducements, offers to waive reporting to the authorities or to waive prosecution in return for co–operation.
- Act professionally. Guard against other actions likely to be inconsistent with the corporate image or damaging to the corporate reputation.
- Ensure that disciplinary action does not precede the completion of the investigation to avoid the risk of making a wrongful termination, losing the suspect's cooperation and creating a perception of a lack of objectivity.
- Always consider how the investigation will be perceived not only the subject but also by others, both during and after. Consider how it will reflect on the company's reputation for being ethical, against fraud / illegal acts and for treating its employees with respect. Inappropriate actions or a poorly conducted investigation can severely damage employee relations and set back the company's attempts to promote a law–abiding workplace.

ACKNOWLEDGEMENT

We hope you find the results of this survey as interesting and as insightful as we do. The response was extremely satisfying. It is probable, from a statistical point of view that of the sample of companies surveyed; those that had experienced a fraud were more likely to complete the survey. It has been not possible to follow up on those companies that did not respond.

To those who participated and contributed their time towards this survey, we thank you, and for those who would like to utilize these results as a resource, we also wish to thank you for your interest in our survey concerning one of today's major issues.

If you require additional copies of the KPMG Fraud Survey 2004 report or would like information on how KPMG can assist your organization to control the risk of fraud, please contact one of the following individuals on +60 (3) 2095 3388, by fax on +60 (3) 2094 5986 or by email.

Ooi Woon Chee
wooncheeooi@kpmg.com.my

Dato' Mohd Ghazali Bin Yacub
datoghazali@kpmg.com.my

Tan Kim Chuan
ktan@kpmg.com.my

Ruban Murugesan
vm@kpmg.com.my

Sukdev Singh
sukdevsingh@kpmg.com.my

Drummond Siddle
drummondsiddle@kpmg.com.my

KPMG FORENSIC

KPMG Forensic provides an independent, proactive, responsive service, together with credible forensic results by applying accounting, financial and other specialized skill sets to the investigation of alleged fraud and in resolving commercial and legal disputes. Our core management team is innovative, flexible and quality conscious, placing great emphasis on value–added benefits.

KPMG's Forensic team, comprising accountants, former police officers, forensic technology technicians and a lawyer, have the expertise, experience and enthusiasm to help you investigate any form of suspected fraud. From sole–practitioner to vast multi–national conglomerates across all industry sectors, we have the capabilities to determine the nature and extent of potential fraud in your organization.

Our products and services cover a wide spectre of counter fraud and investigative activities which include:

- General fraud investigations
- Breach of contract investigations
- Quantification of damages
- Expert testimony in disputes
- Forensically focused due diligence investigations
- Corporate intelligence
- Forensic technology services
- Anti–money laundering services
- Digital evidence recovery and preservation
- Expert determinations
- Professional negligence claims
- Royalty audits
- Intellectual property disputes / claims
- Assignments requiring objective factual determination for the purpose of dispute resolution
- Arbitration and mediation
- Insurance claims
- Fraud risk assessments
- Fraud awareness training
- Fraud risk workshops
- Ethics hotline

kpmg.com.my

Contact us

Wisma KPMG
Jalan Dungun, Damansara Heights
50490 Kuala Lumpur
Tel: +60 (3) 2095 3388
Fax: +60 (3) 2095 0971
Email: info@kpmg.com.my

Postal address
P.O. Box 10047
50702 Kuala Lumpur

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation. The content of this publication is copyright with all rights reserved. Portions may be reprinted with acknowledgement to the firm. We would appreciate being notified of any reproduction.