



Quick Links:

Cutting through the smoke and mirrors Forensic Focus



Welcome to our third edition of Forensic Focus for 2009.

Many of you will be aware of the power of forensic technology to identify electronic evidence in cases of fraud, theft of intellectual property and leaking information.

However forensic technology is also playing an increased role in uncovering evidence to help authorities solve violent crimes. **Jon Pearce**, a manager in our forensic team, was involved in a recent case involving serious allegations of violent crime. His analysis of the offender's computer records uncovered critical photographic and video evidence that led to the man's conviction on a host of charges. The offender was sentenced in the High Court this month and will serve 20 years. Jon's role here provides a real life example of how the application of forensic technology services continues to broaden and make an impact.

Elsewhere, in this newsletter we feature:

- Creative accounting – have you seen the red flag?
- Data searches – six degrees of separation
- USB devices – how secure is your data?
- How to spot possible fraud – we've got your number

Kind Regards,
Barry Jordan and team.



Creative accounting

Have you seen the red flag?

Quick Links:

Accounting suffered a series of major reputational blows in the 1980's and 90's. The "creative accounting" practices used made some businesses appear to be more profitable (or less profitable for tax reasons) and financially stronger than they really were. Lenders and investors lost millions as a direct result of these practices.

However, it would be wrong to simply conclude that those were the 'bad old days' and financial reports are no longer manipulated for gain. Unfortunately, 'creative accounting' is not a dying art and is still used by some for financial gain.

Insurers, lenders and government departments rely on accounting information in order to make assessments regarding insurance claims, ability to service loans and the need for financial support. Financial reports that have been manipulated can lead to overpaying insurance claims, lenders and creditors suffering higher levels of bad debts and government providing financial support to organisations that don't require it.

What to look out for?

In our experience, you should pay particular attention if one of the following are identified in an organisation's annual financial statements as the figures for these are easily manipulated:

- Management fees
- Transactions with related parties
- Wages to family members
- Shareholder salaries

Also be wary of significant and unexplained changes in the level of sales, gross profit percentages, expenses, stock, accounts receivable and accounts payable.

If one of these red flags is flying, we suggest you carefully question the organisation. Often this will unlock whether there are valid commercial reasons for these items. If not, it may be necessary to investigate further before you can reach an accurate conclusion as to an organisation's real profitability and/or financial strength.

Please contact Jason Weir if you would like further information on this.



Jason Weir
+64 (0) 9 303 0966
jasweir@deloitte.co.nz

Data searches

Six degrees of separation



Quick Links:

We are often asked “what databases are available to do simple searches”, “where do I begin to run a background search on a company” or “how do I work out the relationships connected to company X”.

There are a number of external databases that host publicly available information. Here are six of the best to get your search started:

1. Companies Office www.companies.govt.nz

Search for a company, director, shareholder or banned director. Other registers can also be searched, including charitable trusts, incorporated societies and building societies.

2. National Insolvency Database www.insolvency.govt.nz

Provides access to a database containing information about insolvencies (companies or individuals) administered by the Insolvency and Trustee Service.

3. Terralink www.terranet.co.nz

Subscribe to a database sourced from Land Information New Zealand, Quotable Value New Zealand and the Maori Land Court. This is an excellent website for finding out who owns property.

4. Personal Properties Securities Register www.ppsr.govt.nz

The PPSR website records parties that have registered an interest in assets (e.g. hire purchase agreements). This is an excellent site for finding non-property assets that have been provided as security. When searching for a vehicle, the registration plate, chassis number or VIN is required.

5. Births Deaths & Marriages www.bdm.govt.nz

Certificates of a birth, death or marriage can be requested by any member of the public. At present, the request must be made by completing a form and sending this to your nearest BDM office at the Department of Internal Affairs. The full name and year of the birth, death or marriage is usually the minimum amount of information required. The disadvantage with conducting this search is that there is a time delay and contact details do not remain current.

6. Veda Advantage www.vedaadvantage.co.nz

Veda Advantage combines information from various sources into one report. An issue can be that the report includes all previous searches that have been conducted, so a footprint is left of your search. The minimum information required is a surname, first name and current or previous address.

A logon or registration is required to conduct a number of these searches and in some cases there is a fee charged.

We are familiar with these search tools and a number of others and are happy to either perform searches on your behalf to ascertain information required, or to give you advice on what is the best tool for you to be using to achieve your objectives.

Please contact Lorinda Kelly or Lisa Tai if you would like to discuss searching for information.



Lorinda Kelly
+64 (0) 4 470 3749
lorkelly@deloitte.co.nz



Lisa Tai
+64 (0) 9 303 0943
lisatai@deloitte.co.nz

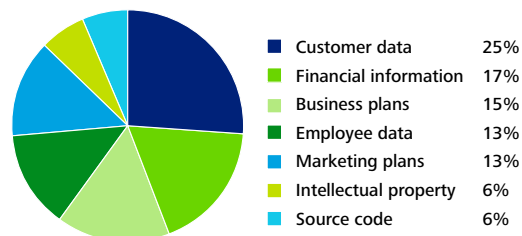
USB device security

How secure is your data?

Quick Links:

USB flash drives have become an increasingly popular data storage option with some devices now holding up to 132gb of data. With the increase of usage we have seen the increase of security challenges that businesses are needing to address and overcome.

A recent survey by SanDisk, a major manufacturer of USB devices, shows that large amounts of sensitive data is stored on USB devices.



Source: SanDisk Survey 9 April 2008

Are USB flash drives a useful tool for sharing data, or a way for malicious users to bypass network security policies and put your data at risk?

Main threats:

- Unauthorised removal of data
- Virus introduction
- Exposure of sensitive information

Key benefits of USB device security :

- Reduced risk of data theft
- Reduced risk of data loss and/or corruption
- Enhanced controls of access to company critical data
- Promotes employee understanding of USB device usage policies

Having established the risks associated with portable storage devices, now is the time for your organisation to consider whether it should:

- Limit the use of portable data storage media and devices except with specific authority
- Automatically record the attempted connection of any and all devices to the corporate network
- Prevent MP3 players, digital cameras and mobile phones being connected to PCs
- Automatically encrypt all data carried outside the network on portable devices
- Amend definitions of 'misconduct' within appropriate HR policies to reflect the new issues facing organisations as a result of these lifestyle devices

Tips for combating unauthorised USB devices

There are a number of countermeasures that can help to reduce, but will never eliminate, the risk of using USB storage devices. These include:

- Disabling the USB and FireWire ports on each computer.
- Introducing encryption technology to protect intellectual property and other data against disclosure on misplaced or stolen USB devices. If the data does leak out of your organisation no unauthorised person will be able to read it.
- Using portable storage devices that feature strong authentication as well as data encryption. SanDisk, Kingston Technology, Lexar and IronKey all produce thumb drives like this.
- Having your IT staff use features within the computer operating system to control access to USB ports and devices.

For more information on USB device security please contact Barry Foster or Jon Pearse.



Barry Foster

+64 (0) 9 303 0974
bfoster@deloitte.co.nz



Jon Pearse

+64 (0) 9 303 0838
jpearse@deloitte.co.nz

How to spot possible fraud

We've got your number



Quick Links:

I was recently talking to a group of senior executives about the seven things you need to know about fraud. One of the topics we covered was how fraud is commonly identified within the organisation. The simple answer is when people act on doubts or suspicions.

However I pondered the question some more and discussed it with the team back in the office. We began to formulate a list of red flags that occurred on investigations we completed. Any of them could set off alarm bells that a possible fraud is taking place. Here's what we came up with:

1. Close relationship with suppliers

Budget managers who have close personal relationships with suppliers.

2. Recurring transactions with a particular supplier for no apparent reason

A large number of transactions with a particular supplier, when many are slightly below an employee's authorisation limit.

3. Unprofessional invoices

Invoices that do not appear to have been generated through a computerised accounting system and the description of what is being invoiced is quite 'light'.

4. Insufficient knowledge of suppliers

Payments made to suppliers, where finance or senior staff do not know of them.

5. Common contact details and bank account numbers

Two or more suppliers and/or employees that seemingly share contact details and/or bank account numbers.

6. Lack of supporting documentation

Lack of supporting documentation for payments, especially those incurred through corporate credit cards. This risk is magnified if there is no review or oversight of the expenditure (e.g. if no-one reviews the CEO's credit card expenditure).

7. An overly dominant management team

Managers with dominant personalities that people rarely generally question.

8. Annual leave not taken

The accumulation of large amounts of annual leave coupled with reluctance to take holidays or to delegate work when away.

9. Working unnecessarily long hours

Employees who work excessive amounts of overtime.

10. Significant observed changes in the attitude and behaviour of an employee

An individual displays feelings of resentment towards their employer or has a perception of being owed something by their employer.

11. Employee lifestyle change

Individuals who appear to live beyond their means.

12. Unavailability of original documentation

Payments to suppliers supported by photocopies instead of originals or not supported at all.

13. Odd transaction patterns

Transaction patterns that are inconsistent with overall business and industry norms.

14. Weak internal control environment

Management does not emphasise the importance of strong internal controls

15. Liberal accounting practices enacted by management that compromise internal controls

Controls such as separation of duties, delegation levels, review of expenditure are ignored or modified in practice.

If you would like to discuss this further, please contact Barry Jordan.



Barry Jordan

+64 (0) 4 470 3760

bjordan@deloitte.co.nz

We hope you enjoyed the read.

We're always keen to hear your feedback, if you have any suggestions for content or topics you would like us to explore in the newsletter please email us on lisatai@deloitte.co.nz >

Contacts

Your Forensics and Recovery team:

Forensics

Barry Jordan - Partner

+64 (0) 4 470 3760

bjordan@deloitte.co.nz

Jason Weir - Associate Director

+64 (0) 9 303 0966

jasweir@deloitte.co.nz

Barry Foster - Associate Director

+64 (0) 9 303 0974

bfoster@deloitte.co.nz

Lorinda Kelly - Associate Director

+64 (0) 4 470 3749

lorkelly@deloitte.co.nz

Recovery

David Vance - Partner

+64 (0) 4 470 3768

dvance@deloitte.co.nz

Rod Pardington - Partner

+64 (0) 9 303 0705

rpardington@deloitte.co.nz

David Levin - Partner

+64 (0) 9 303 0935

davidlevin@deloitte.co.nz

Viv Madsen-Ries - Associate Director

+64 (0) 9 303 0940

vmadsenries@deloitte.co.nz

Garry Clarke - Associate Director

+64 (0) 9 303 0797

gaclarke@deloitte.co.nz

Subscribe or Unsubscribe:

To add other names to the subscription list or have your name removed, please contact Philippa Bell on phbell@deloitte.co.nz >

For further information, visit our website at www.deloitte.co.nz

Deloitte brings together over 900 specialists providing New Zealand's widest range of high quality professional services. We focus on audit, tax, technology and systems, risk management, corporate finance and business advice for growing organisations. Our people are based in Auckland, Hamilton, Wellington, Christchurch and Dunedin, serving clients that range from New Zealand's largest companies to smaller businesses with ambition to grow.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in 140 countries, Deloitte brings world class capabilities and deep local expertise to help clients succeed wherever they operate. Deloitte's 150,000 professionals are committed to becoming the standard of excellence.

Deloitte's professionals are unified by a collaborative culture that fosters integrity, outstanding value to markets and clients, commitment to each other, and strength from diversity. They enjoy an environment of continuous learning, challenging experiences, and enriching career opportunities. Deloitte's professionals are dedicated to strengthening corporate responsibility, building public trust, and making a positive impact in their communities.

This publication contains general information only, and none of Deloitte Touche Tohmatsu, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/nz/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu and its Member Firms.