

Unravelling forensics @ ferriers



Unravelling the Facts with the Ferrier Hodgson Forensics Team – Issue 8: November 2005

Kazaa made to face the music

In September KAZAA (the file-sharing online service used by millions to swap music) was ordered to stop the flow of illegal music on its system.

Australian Federal Court Judge, Murray Wilcox, ruled KAZAA had infringed music copyright and will be required to pay costs. Damages could be in the billions of dollars.

“The case may involve literally billions of dollars in damages.”

Ferrier Hodgson Forensics played key roles in this watershed case.

Data Collection

Nigel Carson (Forensic IT) conducted the early analysis of KAZAA's software and produced the foundation software analysis, expert report and affidavits that secured Anton Pillar orders against KAZAA offices, various university sites, ISPs and residential premises. The data collected in these 'raids' provided critical evidence in the proceedings.

Critical analysis

Ben Lyons (Forensic IT) executed a technical analysis of KAZAA's international website. His earlier affidavit helped secure funding from key players in the music industry. He helped determine the scope software owners had to central content – a pivotal question addressed by Judge Wilcox to help define two filter technologies, one of which KAZAA will have to choose to prevent the infringement of copyright.

Expert opinion

Nigel Carson also provided expert testimony, mainly refuting the opinions of American academics earlier affidavit of IP addresses to trace users. Again, the evidence went to the core of how to best design filter technologies that would work to prevent copyright infringement in a real world environment.



“The conundrum involved finding a modus operandi that would protect music copyright while preserving the freedom of information rights of legitimate users.”

Nigel Carson, Forensic IT, Sydney



In this issue:

- Kazaa made to face the music
- Reducing the risk of employee fraud
- Smart passwords

Reducing the risk of employee fraud

An accelerating trend

The incidence of internal fraud, theft and corruption is on the increase in businesses, just as it is in most Western economies. The causes of the increase are many and varied. High staff turnover rates, the search for quick riches and instant gratification, a decay of traditional moral values, the failure of staff to express loyalty to their corporate employer, a growing population of 'problem gamblers' are but a few of the factors that have contributed. And it's not a problem that's confined to junior and/or middle level staff. Some of the most costly frauds have been committed by very senior management, people who seemed to have impeccable credentials.

A false sense of security

The problem runs largely unchecked because we tend to think of ourselves as pretty good judges of character when

it comes to assessing an employee's integrity – and because we tend to underestimate the ability of problem employees to spin convincing yarns and feign laudable work styles.

Most businesses, however, only find out about 'a problem' after the horse has bolted. By then it's usually too late. Reactive patch-ups rarely work. Much better to be proactive. When it comes to fraud and theft, prevention is unquestionably better than any cure. *continued over...*

“In the USA it's been estimated that about 500,000 employees have phoney degrees. Scarily, about 10,000 doctors practise with 'invented credentials.'”*

*(*M Finn & J Baker 1996)*



“A key to Ferrier's success was our team approach. It provided depth of analysis, cross-discipline interaction and enabled the internal testing of procedures and its interpretation. Robust evidence is the output.”

Ben Lyons, Forensic IT, Sydney

- Forensic Accounting
- Fraud Risk Services
- Forensic IT

Smart passwords

Improving your first line of defence

We're all tempted to select 'personalised' passwords. They're easy for us to remember – and we intuitively assume that no one could ever work out, or guess, clever little secrets, such as...

- 1414 (my lucky number, repeated)
- BUZZ (the name of my pointer dog)
- POSH (no, not her. It's a nickname for someone in senior management)
- 5 letters and number combinations (eg: passB5) about 30 MINUTES
- 5 letters, numbers and symbol combinations (eg: \$paB5), WEEKS

With little, idiosyncratic 'trickies' like these, we are bound to be safe, right? Wrong. What we believe is our impenetrable first line of defence is often the weakest link in security.

Using specialist password-breaking software available to Ferrier Hodgson, it takes roughly the following times to crack various code types.

A password of,

- 4 letters or numbers (eg: pass) takes SECONDS to break
- 5 letters or numbers (eg: passb) takes about SIXTY SECONDS
- 5 letters, case sensitive (eg: passB) around SIX MINUTES

The 'TIPS' below summarise the lessons that can be learnt from these data. It's rare that the application of such easy-to-do steps can make such a positive difference to your security defences. They're guidelines that are well worth following.

- AVOID using names, dates or words
- Use a MIX of numbers, symbols and letters
- Incorporate CASE SENSITIVE elements
- Use FIVE or MORE characters, and
- DON'T USE the 'remember password' option
- DO change passwords every now and then

Colin Gill, Forensics, Melbourne

Reducing the risk of employee fraud

continued from page 1

Proactive systems minimise risk

Rigorous investigatory and monitoring systems can minimise the future risk of fraud, theft and corruption. Systems that probe beneath the surface can greatly reduce the probability of crime.

In high risk CV fraud situations (ie: where sizeable sums of money or confidential information are involved) we recommend a **high level** assessment system that integrates both information that comes from the applicant and feedback from external sources.

Such a system would incorporate many of the steps outlined below:

High level assessment

verify:

- CV details
- Check for a criminal record
- Make a credit bureau enquiry
- Check academic qualifications
- Check driver's licence and passport/visas

check:

- References (and consolidate feedback from different referees)
- Talk with previous work colleagues
- Think about the questions you're going to ask in the interview, the questions that are going to 'test' the answers provided by applicants

conduct:

- A lifestyle assessment to see if the candidate's income can support their material lifestyle

consider:

- Psychometric testing to get behind the 'good guy' façade of the clever candidate

In low risk CV fraud cases (where the consequences of fraud etc would not be as detrimental) a less extensive – and less expensive – checking system is more appropriate. It only verifies information supplied by the candidate (plus any documentation submitted).

Low level assessment

verify:

- Key CV details
- Check for a criminal record
- Conduct credit bureau enquiry
- Validate university qualifications
- Check driver's licence/passport

conduct:

- Integrity test which provides an estimate of risk potential
- Consistency checks when personally interviewing candidates

consider:

- Using a simple-to-score personality test

Monitoring existing employees

Extensive research has enabled the construction of invaluable 'defaulter profiles'. This understanding has, in turn, produced a battery of symptoms that can be used to **red flag** problem people, before the event. Such flags include:

Behavioural flags

- An increasing reluctance to disclose details of one's work
- Increasingly negative reactions to supervision
- Atypical leave patterns
- Withdrawal from contact with close work colleagues; deteriorating relationships with work colleagues (though not necessarily clients)
- A significant lift in 'lifestyle' affluence

Situational flags

- More than 3 years tenure in a position of trust/authority
- A decline in formal supervision

Attitudinal flags

- Exhibits symptoms of a very strong need for recognition and status
- The presentation of an obviously 'self-centred' personality

Making systems operational

Many corporations have the HR resources and expertise to design appropriate screening and monitoring systems. Or you can call us to do it for you. Either way, an investment in prevention will produce handsome dividends.

Jean-Pierre du Plessis, Forensic IT, Adelaide

"It's been estimated that around 30% of applications contain inaccurate information, embellishments or downright lies."

"Integrity – soundness or moral principle, the character of uncorrupted virtue, uprightness, honesty, sincerity."
Oxford dictionary

"Integrity is associated with other traits, mores and attitudes that can be explored in psychometric tests that make it hard for a candidate to consistently pick the 'right' answers."

About forensics@ferriers...

forensics@ferriers is a newsletter issued by Ferrier Hodgson discussing current issues in the area of Forensic Services – forensic accounting, forensic IT and fraud risk services. For comments please contact john.temple-cole@syd.fh.com.au Alternatively you can read forensics@ferriers on our website.

Australia Please note – the material contained in this newsletter is merely general commentary. The facts of each particular situation vary as does legislative and judicial interpretation of any law commented upon. The comments and information herein do not constitute and must not be relied on as legal or professional advice. Advice tailored to your specific situation should be sought from any Ferrier Hodgson affiliated office before acting in any of these areas.

Ferrier Hodgson is committed to respecting the privacy of your personal information. We are bound by the Privacy Act 1988 and the National Privacy Principles, which set out a number of principles concerning the collection, storage, use and disclosure of personal information. You have the right to access and request correction of your personal information that we hold. We may use your personal information for our own advertising and marketing purposes. If you wish to contact us concerning any issues relating to privacy, to obtain a copy of our privacy policy, or if you wish to be removed from our database and do not wish to receive future mail outs, please email us at privacyofficer@syd.fh.com.au or telephone Mr Robert Fitt on (02) 9286 9999.

Hong Kong If your details have changed or you would like to subscribe or unsubscribe to this publication, please contact fh@fh.com.hk

For more information about our Forensic Services please contact:

Forensic Accounting

Sydney: John Temple-Cole
+61 2 9286 9999
john.temple-cole@syd.fh.com.au

Melbourne: Greg Meredith
+61 3 9600 4922
gmeredith@melb.fh.com.au

Brisbane: Greg Moloney
+61 7 3831 4833
gmoloney@qld.fh.com.au

Adelaide: Peter Holmes
+61 8 8100 7655
pholmes@sa.fh.com.au

Perth: Garry Trevor
+61 8 9221 2460
gtrevor@perth.fh.com.au

New Zealand: Grant Graham
+64 9 307 7865
grant.graham@ferriers.co.nz

Hong Kong: Rod Sutton
+852 2820 5600
rsutton@fh.com.hk

Singapore: Tim Reid
+65 6416 1400
timr@fh.com.sg

Fraud Risk Services

Sydney: Bill Bradbury
+61 2 9286 9876
bill.bradbury@syd.fh.com.au

Hong Kong: John Tudorovic
+852 2820 5610
jtudorovic@fh.com.hk

Singapore: Paul Curby
+65 6416 1417
paul.curby@fh.com.sg

Forensic IT

Sydney: Nigel Carson
+61 2 9286 9933
nigel.carson@syd.fh.com.au

Melbourne: David Caldwell
+61 3 9604 5120
dcaldwell@melb.fh.com.au

Adelaide: Jean-Pierre du Plessis
+61 8 8100 7655
jpduplessis@sa.fh.com.au

Or find out more about Forensics at:
www.ferrierhodgson.com