


Fraud risks & new technology

ISACA – 13 December 2001

Ian Henderson FCA

Haymarket Management Services Ltd


Background:

- Haymarket specialise in fraud investigations
- 70% reactive (usually based on suspicions)
- 20% of our work is preventative
- Almost all will involve Computer Forensics
- Can be used to clear the innocent, or identify the guilty

We will look at:

- The risks
- The FBI / CSI Survey
- The FAP / CBI Survey
- Typical cases
- Solutions that work

New fraud or old fraud?

- Based on our experience
- The method of delivery has changed
- <u>But the fraud is much the same</u>

Typical risks

- Theft of confidential information
- Forgery of credit cards
- Account take-over
- Denial of Service
- Malicious attacks including virii
- Extortion

Other risks

- Reputation
- “Pump and dump”
- Money laundering
- Defamation
- Other legal risks

CSI
COMPUTER SECURITY INSTITUTE

COMPUTER SECURITY ISSUES & TRENDS

VOL. VII, NO. 1 SPRING 2001

2001 CSI/FBI Computer Crime and Security Survey

www.gocsi.com

CSI / FBI Survey March 2001

- 85% of 538 large companies reported security breaches
- 60% had INTERNAL attacks
- Most serious threat – THEFT of confidential information
- 70% of attacks via the WWW

CSI / FBI survey cont.

- 47% do e-commerce
- 23% reported unauthorised access
- 58% had 10 or more incidents
- 78% were subject to Denial of Service
- 13% lost confidential data
- 8% suffered financial fraud

The Fraud Advisory Panel

CBI THE VOICE OF BUSINESS

Cybercrime Survey 2001

Making the information superhighway safe for business

Published September 2001
price £100

FAP / CBI 2001 Survey Main conclusions

- Business growth limited by Cybercrime concerns
- Main threat is from hackers and virii
- Reputational loss is the main concern
- (Based on 148 responses from CBI members)

Cybercrime defined as:

- Threats to e-business (internet) and internal networks
- Includes fraud, hacking, virii,
- theft of confidential information or IP

Perpetrators of Cybercrime (FAP/CBI 2001 Survey)

- 45% Hackers
- 13% Former employees
- 13% Organised crime
- 11% Employees
- 8 % Customers
- 6% Competitors
- 4% Protest Groups / Terrorists

Confidence in e-business retained (FAP/CBI 2001 Survey)

- 2/3 of organisations experienced a serious incident in the last 12 months
- Cybercrime is expected to increase
- Benefits of e-business outweigh the risks
- B2C more risky than B2B

The main threats - incidents (FAP/CBI 2001 Survey)

- Virii (44%)
- Hacking (16%)
- Adverse comments on WWW (10%)
- IP Infringement (9%)
- Unauthorised access to data (8%)

The main threats - incidents (FAP/CBI 2001 Survey)

- "Spoofed" website (6%)
- Credit Card Fraud (4%)
- Legal liability issues (2%)
- DOS Attack (2%)

How was the incident discovered? (FAP/CBI 2001 Survey)

- 43% Internal controls
- 24% Outside information
- 14% Internal whistle blower
- 7% Internal Audit
- 7% Accident / Chance
- 4% Management review
- 1% External audit

The not so good news

- Priority for most companies is operational systems - as quickly as possible
- Not enough resource (or understanding) allocated to management of fraud risk
- "we'll fix it if we have a problem" attitude - usually too late
- Fraud will often involve collusion

The reasonably good news

- Encryption usually works and is not a factor in most frauds
- Good hardware and software products are available
- If you want to become a "hard target" – you can

What the research shows

- 70% of systems don't have the latest security patches
- 90% don't use full audit logging
- 60% don't have contingency plans
- 70% do not have tested "fraud audit trails"
- Many "certified" sites don't meet these standards

It's all about risk management

- Eliminate risk completely – and you won't do any business!
- What level of risk, or loss is acceptable?
- Have we a "shrinkage" tolerant approach?
- If so, concentrate on managing the catastrophic risks and MONITOR the rest

But what are the facts?

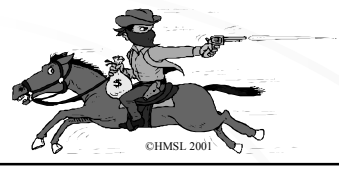
- Who do you believe?
- Is e-commerce fraud less that traditional retail fraud?
- Is it as high as 20% of all transactions?

Financial loss as a % of e-business (FAP/CBI 2001 Survey)

- 69% said less than 1%
- 3% said 1% to 3%
- 6% said 4% to 6%
- 2% said 7% to 10%
- 2% said 11% to 20%
- <u>18% didn't know!</u>

Our experience indicates:

- The risk is real and manageable
- No room for complacency
- Aim to become a hard target



e-commerce has made it easier

- Pressure on market share
- New technology
- Lack of effective anti-fraud measures
- Is it error or is it fraud?
- Identity theft is a real and increasing problem

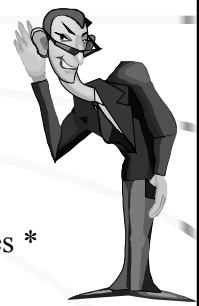
How we see it

- Low level Credit Card fraud will continue and probably increase
- Action must be taken to minimise this
- The big risks, however, are from cyber-terrorism, organised crime and theft of confidential information

Cyber-terrorism

- May involve extortion or ransom demands
- Will probably involve organised crime
- Will probably involve insiders
- Theft of information a likely target

Methods of attack



- External probing
- Denial of Service attacks
- DNS hacking
- Viruses and trojans
- * Infiltration of sniffer devices *

Today's hacking groups

- Well organised with a business focus
- Probably linked to organised crime
- Extremely sophisticated
- Will use encryption and avoid standard audit log detection
- Will probably try infiltration

Typical targets

- Banks and financial institutions
- Anyone in e-commerce
- Anyone with information that can be sold

What can you do about it?

- Know the threat
- Screen employees
- Detect possible problems and fix them!
- Use effective audit log software
- Have an action plan ready
- Test for vulnerabilities

Beware of the marketing department

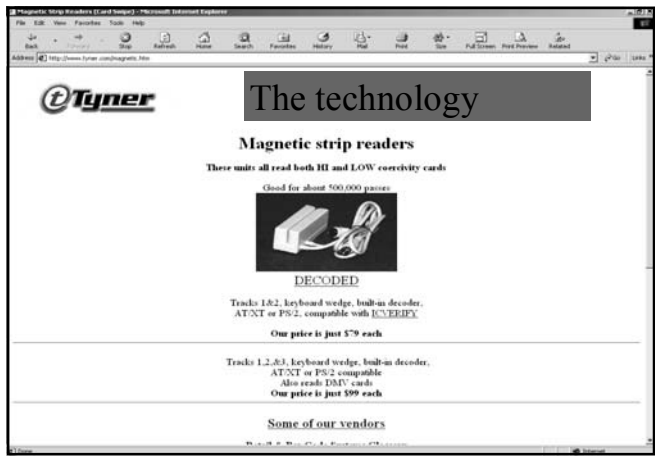
- May set targets for new accounts each day
- Will see security as restricting business
- Little appreciation of risk
- Possibly short term objectives
- Look at full cost of charge-back agreements

Criminals have responded

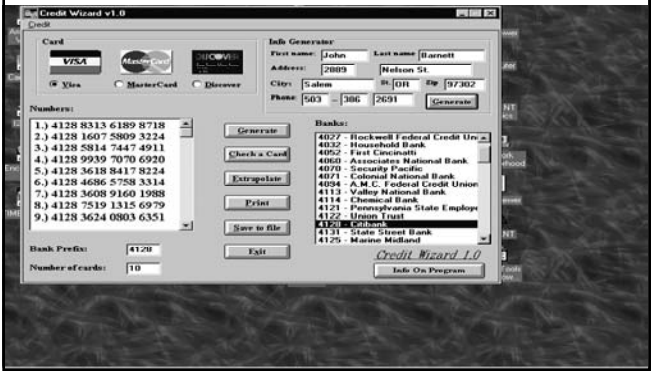
- Traditional bank robberies don't happen any more
- Internet chat rooms / newsgroups share information
- Technology makes it easy
- Legal framework often weak

This doesn't happen any more

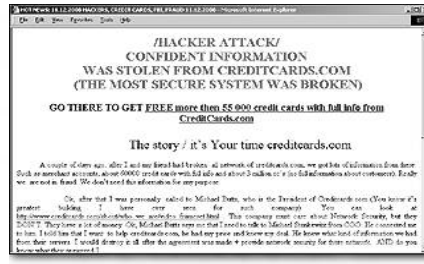
BUT THIS DOES



Credit card number generator



US $20,000 ransom claimed


/HACKER ATTACK/
CONFIDENT INFORMATION
WAS STOLEN FROM CREDITCARDS.COM
(THE MOST SECURE SYSTEM WAS BROKEN)

GO THERE TO GET FREE more then 55 000 credit cards with full info from CreditCards.com

The story / it's Your time creditcards.com

Other reported incidents

- VISA £10 million ransom demand
- UK Bank £10 million extortion
- US Bank lost US $ 50 million in EFT fraud


UK becomes the capital of credit scams

THE United Kingdom has won an unenviable reputation for being one of the world's plastic card fraud capitals because it plays host to a staggering number of criminals eagerly plying their trade.

Losses of almost £300m were racked up by the UK's banking and retail industries last year – a 55% increase on the 1999 total of £188.4m – and expert opinion predicts this figure will continue to soar unless action is taken.

The largest individual rises were found to be in counterfeit card production, which was up a staggering 104% to £102.8m, and card-not-present frauds, such as mail order or telephone purchases where the retailer does not see the plastic, which jumped 94% to £56.8m during

Most of these frauds take place in the United States, which accounts for 22% of such losses, followed by Spain with 16% and France just behind on 15%. The reasons for the surge in foreign fraud, claims Apacs, is a combination of UK fraud prevention methods and the fact that offenders are moving more quickly and easily between countries.

Almost 12% of the world's total card crime takes place in Britain, according to statistics compiled by MasterCard on its branded products, while losses for the first three months of the year are expected to exceed $25m. A more clearly defined picture, however, is expected to emerge as outstanding figures are fed into the data over the next couple of months.

May 2001


Tuesday, October 30, 2001 METRO 9

Barclays 'faced £25m blackmail'

BY DAVID FICKLING

A FORMER Barclays Bank employee threatened to compromise the security of millions of credit and debit cards in a £25million blackmail bid, the Old Bailey heard yesterday.

Graham Browne, 56, headed a security encryption team at one of the bank's computer centres.

The job gave him access to the credit card numbers of all the bank's customers and the encryption codes used on the cards' magnetic strips.

If they became public, the bank's entire security system would have been compromised – forcing it to spend millions of pounds to change its customers' details. Browne was disillusioned with his job and what he saw as the lack of resources Barclays was putting into card security.

In January last year he resigned, thinking his bosses would plead with him to stay. When they accepted his decision, he became resentful.

He began sending letters in which he demanded the bank set up a 'super security team' of 14 experts, including himself, each paid £1.7million.

Otherwise, he warned, he would publicise the bank's lack of security and the codes. The police were called and identified Browne as the culprit.

Browne said the demands he made in a series of four letters to the bank's chief executive were a 'huge joke'.

Sally Bennett-Jenkins, prosecuting, told the jury: 'You may think his allegations of bad security have merit. But that's not the issue. The question is whether he is guilty of blackmail.'

She said if Browne had released any information it would have been 'highly embarrassing' for Barclays.

Browne, of Knutsford, Cheshire, denies blackmail between March and September 2000. The case continues.


Wednesday, October 31, 2001 METRO 9

E-mail scam to hijack company

BY FINIAN DAVERN

AN ACCOUNTANT hatched an e-mail plot with a US businessman to kidnap two rivals and hijack their company, a court heard yesterday.

Peter Rapaport, 55, hired two thugs – one of whom used to guard the Queen – to snatch Philip Mason and Anne-Marie Moore at knifepoint.

They were ordered to sign resignation letters and documents handing ownership of their corporate hospitality business to David Reiss, who masterminded the scheme from his home in Texas.

The victims were handed a list of rules and told their families would suffer if they did not obey them. The couple were then released but, despite the threats, went straight to police.

The next day, officers raided the Affinity Group in Twickenham, Middlesex, and found new 'owner' Reiss already making himself at home.

Middlesex Guildhall Crown Court was told Mr Mason met Reiss more than ten years ago and became friends.

They had an arrangement whereby the American was paid commission for any deals he helped to set up.

But the relationship soured when Reiss demanded £35,000 he had not earned. Mr Mason had no contact with him for months – but Reiss was secretly plotting revenge with help from Rapaport.

Among evidence retrieved from the accountant's home was a string of incriminating e-mails he sent to Reiss.

Rapaport, of Maida Vale, West London, was convicted of conspiracy to rob and falsely imprison and remanded in custody until November 16, with a warning he faces jail.

Reiss, 48, of Dallas, Texas, pleaded guilty at an earlier hearing and has also yet to be sentenced.

THE DAILY TELEGRAPH Saturday, November 10, 2001

Four years for banker who took £1·5m from till

By Richard Savill

A BANK executive who admitted stealing £1·7 million from her firm to fund a life of luxury was jailed for four years yesterday.

Beryl Rowlands, 58, former head of private banking division of Dunbar Bank, a subsidiary of Zurich Financial Services, based in Swindon, Wilts, lavished expensive gifts on friends, her children and grandchildren and treated herself to Rolex watches and exotic holidays.

Swindon Crown Court was told that Rowlands, who took £1·5 million in cash "from the

Beryl Rowlands: luxuries

offered to help the company to identify weaknesses in their system to prevent any possible repetition.

He added that Rowlands had sought to "bolster her self-esteem" by giving "extravagant gifts" and had found admitting her guilt "cathartic".

She was suspended in May last year when a junior staff member stumbled across the fraud when Rowlands was seen inputting financial data without documentation.

Ian Lovett, chief executive of Dunbar Bank, said yesterday: "This was a serious fraud

The threat from within

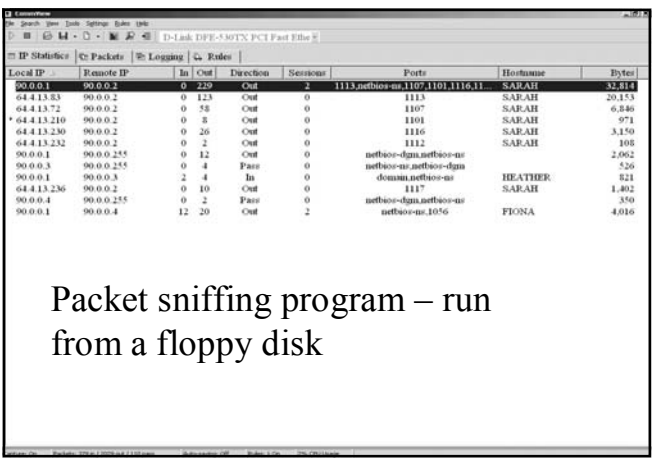
- Employees
- Ex-employees
- Tools readily available
- On-line storage
- "promiscuous" network cards

The response

- Do your homework
- Learn from reported incidents
- Use the WWW for research
- Apply the fixes
- Test for vulnerabilities
- Monitor activity

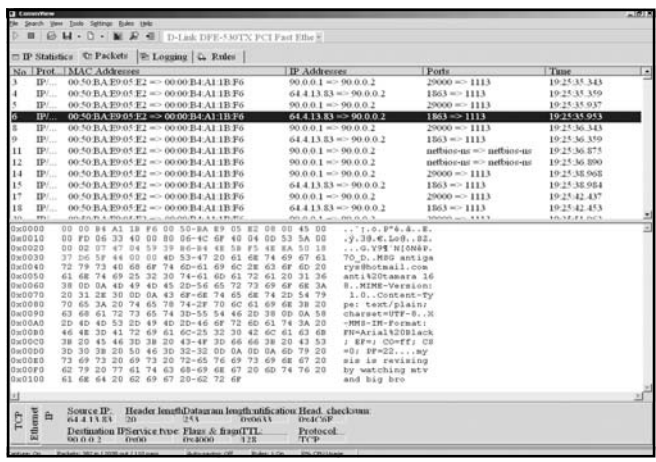
Techniques used (Based on our experience)

- Infiltration of staff
- Probe type attacks
- Packet sniffing
- Keystroke logging (Hardware and Software)
- Trojans / Remote Access Programs
- Email forwarding / capture
- On-line storage



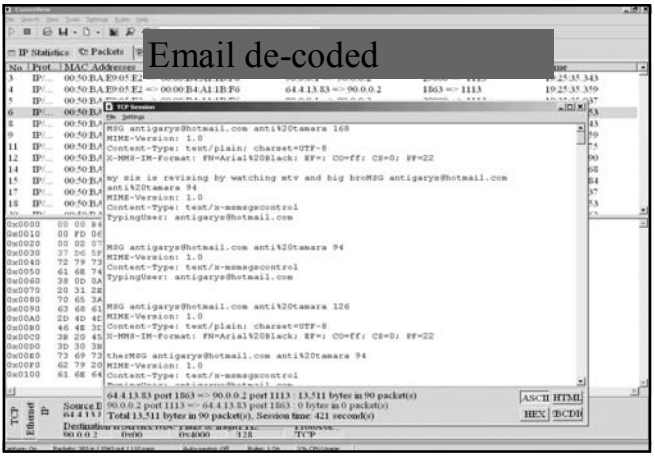
Local IP	Remote IP	In	Out	Direction	Sessions	Ports	Hostname	Bytes
90.0.0.1	90.0.0.2	0	229	Out	2	1113,netbios-ns,1107,1101,1116,11...	SARAH	32,814
64.4.13.83	90.0.0.2	0	123	Out	0	1113	SARAH	20,153
64.4.13.72	90.0.0.2	0	58	Out	0	1107	SARAH	6,846
64.4.13.210	90.0.0.2	0	8	Out	0	1101	SARAH	971
64.4.13.230	90.0.0.2	0	26	Out	0	1116	SARAH	3,150
64.4.13.232	90.0.0.2	0	2	Out	0	1112	SARAH	108
90.0.0.1	90.0.0.255	0	12	Out	0	netbios-dgm,netbios-ns		2,062
90.0.0.3	90.0.0.255	0	4	Pass	0	netbios-ns,netbios-dgm		526
90.0.0.1	90.0.0.3	2	4	In	0	domain,netbios-ns	HEATHER	521
64.4.13.236	90.0.0.2	0	10	Out	0	1117	SARAH	1,402
90.0.0.4	90.0.0.255	0	2	Pass	0	netbios-dgm,netbios-ns		350
90.0.0.1	90.0.0.4	12	20	Out	2	netbios-ns,1056	FIONA	4,016

Packet sniffing program – run from a floppy disk



No.	Prot.	MAC Addresses	IP Addresses	Ports	Time
3	IP/...	00:50:BA:E9:05:E2 => 00:00:B4:A1:1B:F6	90.0.0.1 => 90.0.0.2	29000 => 1113	19:25:35.343
4	IP/...	00:50:BA:E9:05:E2 => 00:00:B4:A1:1B:F6	64.4.13.83 => 90.0.0.2	1863 => 1113	19:25:35.359
5	IP/...	00:50:BA:E9:05:E2 => 00:00:B4:A1:1B:F6	90.0.0.1 => 90.0.0.2	29000 => 1113	19:25:35.937
6	IP/...	00:50:BA:E9:05:E2 => 00:00:B4:A1:1B:F6	64.4.13.83 => 90.0.0.2	1863 => 1113	19:25:35.953
8	IP/...	00:50:BA:E9:05:E2 => 00:00:B4:A1:1B:F6	90.0.0.1 => 90.0.0.2	29000 => 1113	19:25:36.343
9	IP/...	00:50:BA:E9:05:E2 => 00:00:B4:A1:1B:F6	64.4.13.83 => 90.0.0.2	1863 => 1113	19:25:36.359
11	IP/...	00:50:BA:E9:05:E2 => 00:00:B4:A1:1B:F6	90.0.0.1 => 90.0.0.2	netbios-ns => netbios-ns	19:25:36.875
12	IP/...	00:50:BA:E9:05:E2 => 00:00:B4:A1:1B:F6	90.0.0.1 => 90.0.0.2	netbios-ns => netbios-ns	19:25:36.890
14	IP/...	00:50:BA:E9:05:E2 => 00:00:B4:A1:1B:F6	90.0.0.1 => 90.0.0.2	29000 => 1113	19:25:38.968
15	IP/...	00:50:BA:E9:05:E2 => 00:00:B4:A1:1B:F6	64.4.13.83 => 90.0.0.2	1863 => 1113	19:25:38.984
17	IP/...	00:50:BA:E9:05:E2 => 00:00:B4:A1:1B:F6	90.0.0.1 => 90.0.0.2	29000 => 1113	19:25:42.437
18	IP/...	00:50:BA:E9:05:E2 => 00:00:B4:A1:1B:F6	64.4.13.83 => 90.0.0.2	1863 => 1113	19:25:42.453

0x0000 00 00 B4 A1 1B F6 00 50-BA E9 05 E2 08 00 45 00 ..'1.0.P'é.â..E.
0x0010 00 FD D6 33 40 00 80 06-4C 6F 40 04 00 53 5A 00 .ý.3@.€.Lo@..SZ.
0x0020 00 02 07 47 04 59 39 86-84 4E 58 F5 4E EA 50 18 ...G.Y9†"NXõNêP.
0x0030 37 D6 5F 44 00 00 4D 53-47 20 61 6E 74 69 67 61 7Ö_D..MSG antiga
0x0040 72 79 73 40 68 6F 74 6D-61 69 6C 2E 63 6F 6D 20 rys@hotmail.com
0x0050 61 6E 74 69 25 32 30 74-61 6D 61 72 61 20 31 36 anti%20tamara 16
0x0060 38 0D 0A 4D 49 4D 45 2D-56 65 72 73 69 6F 6E 3A 8..MIME-Version:
0x0070 20 31 2E 30 0D 0A 43 6F-6E 74 65 6E 74 2D 54 79 1.0..Content-Ty
0x0080 70 65 3A 20 74 65 78 74-2F 70 6C 61 69 6E 3B 20 pe: text/plain;
0x0090 63 68 61 72 73 65 74 3D-55 54 46 2D 38 0D 0A 58 charset=UTF-8..X
0x00A0 2D 4D 53 2D 49 4D 2D-46 6F 72 6D 61 74 3A 20 -MS-IM-Format:
0x00B0 46 4E 3D 41 72 69 61 6C-25 32 30 42 6C 61 63 6B FN=Arial%20Black
0x00C0 38 20 45 46 3D 38 20 43-4F 3D 66 66 38 20 43 53 ; EF=; CO=ff; CS
0x00D0 3D 30 3B 20 50 46 3D 32-32 0D 0A 0D 0A 6D 79 20 =0; PF=22....my
0x00E0 73 69 73 20 69 73 20 72-65 76 69 73 69 6E 67 20 sis is revising
0x00F0 62 79 20 77 61 74 63 68-69 6E 67 20 6D 74 76 20 by watching mtv
0x0100 61 6E 64 20 62 69 67 20-62 72 6F and big bro

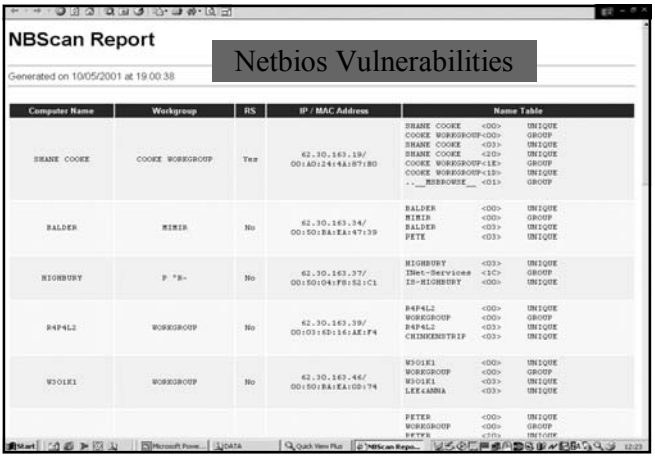


WWW Security holes

- Apply patches
- Test for vulnerabilities
- Approximately 30% of PC's connected to the WWW are open to common hacking tools
- Test for probes and attacks

Typical IDS log

issueName	intruderIp	intruderName
DNS port probe	62.30.92.207	pc-62-30-92-207-st.blueyonder.co.uk
SNMP port probe	62.30.92.207	pc-62-30-92-207-st.blueyonder.co.uk
UDP port probe	206.132.245.76	
Back Orifice ping	62.36.176.201	usuario1-36-176-201.dialup.uni2.es
SNMP port probe	62.30.139.37	pc-62-30-139-37-nm.blueyonder.co.uk
SNMP backdoor	62.30.139.37	pc-62-30-139-37-nm.blueyonder.co.uk
UDP trojan horse probe	212.243.115.20	
UDP port probe	217.80.68.134	pD9504486.dip.t-dialin.net
Echo storm	62.254.53.78	pc78-belfast1.cable.ntl.com
Echo storm	213.48.2.177	usr675-ba1.cableinet.co.uk
Echo storm	210.55.47.133	210-55-47-133.dialup.xtra.co.nz
UDP port probe	208.184.229.157	h208-184-229-157.ibeam.com
Echo storm	212.179.225.228	bzq-225-228.bezeqint.net
Echo storm	172.138.100.250	AC8A64FA.ipt.aol.com
Echo storm	212.23.27.101	adsl-1125.zen.co.uk
Echo storm	203.147.161.230	ae02230.powerup.com.au
Echo storm	62.227.166.147	p3EE3A693.dip.t-dialin.net
Echo storm	202.56.198.163	

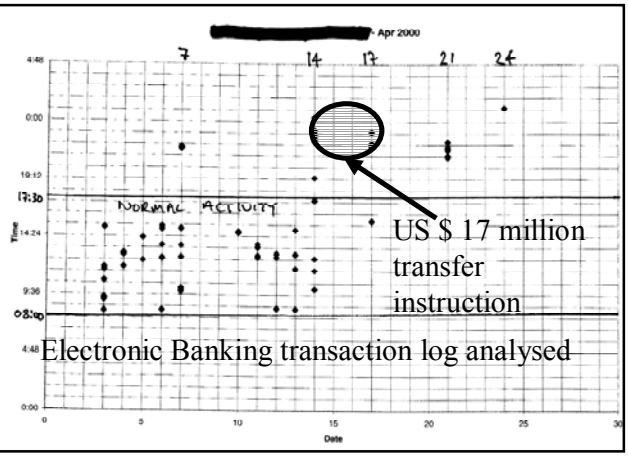


Lets look at an EFT fraud

- Bank reported funds transfer over the weekend
- Company established it was unauthorised
- Implemented Security Incident Response Plan

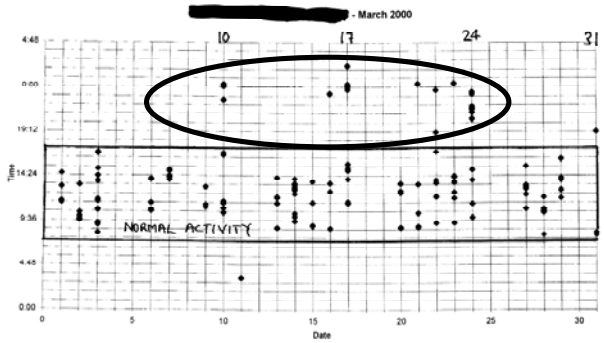
Immediate Action Drills

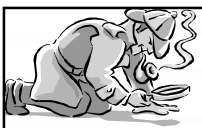
- Suspend EFT facility
- Trace and freeze funds
- Preserve evidence
- Start hard hitting investigation
- Haymarket appointed to advise



Electronic Banking transaction log analysed

EFT transfer attempts every Friday night for 4 months





What we found

- Targeted by organised crime
- IT expert infiltrated into company
- Used automated hacking tools – without success
- Trial and error approach – over 6 months
- Audit logs not fully on or monitored

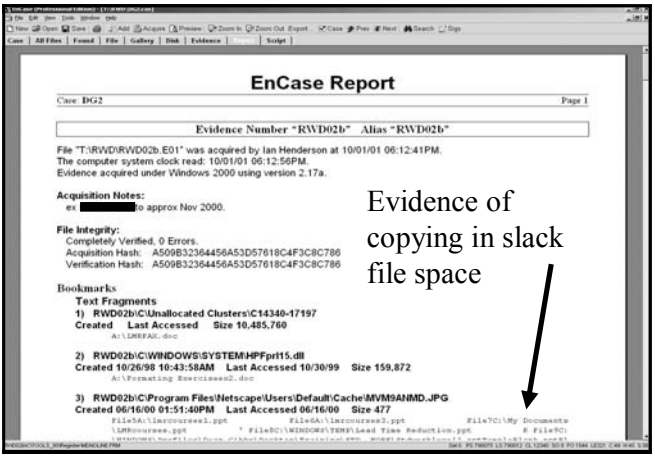
Eventual outcome

- 100% funds recovery
- Method of attack identified
- Perpetrators identified
- Lessons learnt and improved security
- All of this in 3 weeks – based 90% on computer forensics

Let's look at a recent case involving the theft of IP by 2 ex-employee's

Company had suspicions and launched an investigation

- Review of laptops used 6 months earlier
- Review of emails
- Telephone call logs
- Other covert activity



EnCase Report

Case: DG2 Page 1

Evidence Number "RWD02b" Alias "RWD02b"

File "T:\RWD\RWD02b.E01" was acquired by Ian Henderson at 10/01/01 06:12:41PM.
The computer system clock read: 10/01/01 06:12:56PM.
Evidence acquired under Windows 2000 using version 2.17a.

Acquisition Notes:
ex [redacted] to approx Nov 2000.

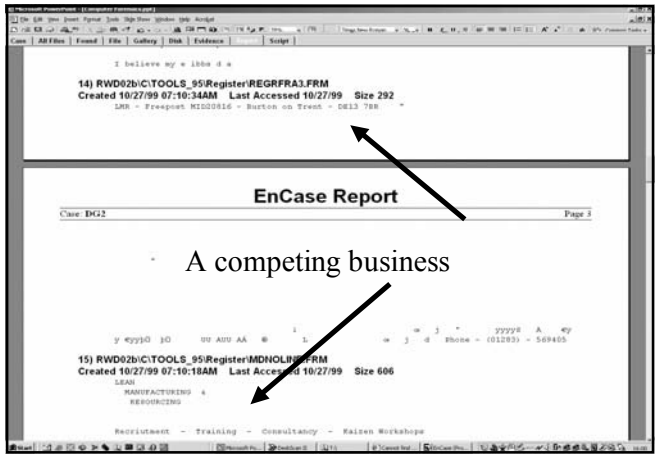
File Integrity:
Completely Verified, 0 Errors.
Acquisition Hash: A509B32364456A53D57618C4F3C8C786
Verification Hash: A509B32364456A53D57618C4F3C8C786

Bookmarks
Text Fragments
1) RWD02b\C\Unallocated Clusters\C14340-17197
Created Last Accessed Size 10,485,760
A:\LMRFAX.doc

2) RWD02b\C\WINDOWS\SYSTEM\HPFprt15.dll
Created 10/26/98 10:43:58AM Last Accessed 10/30/99 Size 159,872
A:\Formating Exercises2.doc

3) RWD02b\C\Program Files\Netscape\Users\Default\Cache\MVM9ANMD.JPG
Created 06/16/00 01:51:40PM Last Accessed 06/16/00 Size 477

Evidence of copying in slack file space



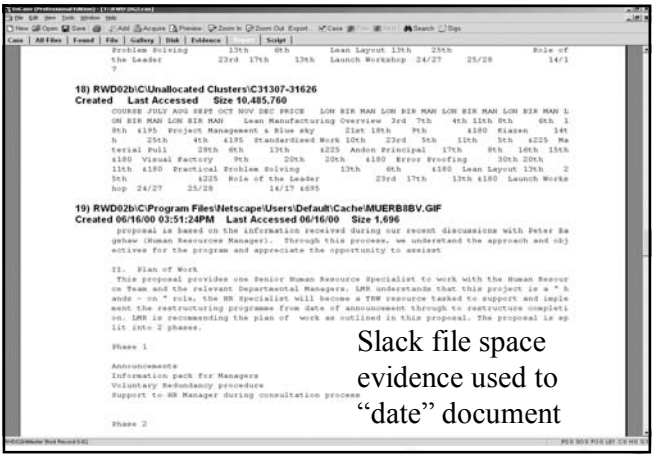
14) RWD02b\C\TOOLS_95\Register\REGRFRA3.FRM
Created 10/27/99 07:10:34AM Last Accessed 10/27/99 Size 292

EnCase Report

Case: DG2 Page 3

15) RWD02b\C\TOOLS_95\Register\MDNOLH~1.FRM
Created 10/27/99 07:10:18AM Last Accessed 10/27/99 Size 606

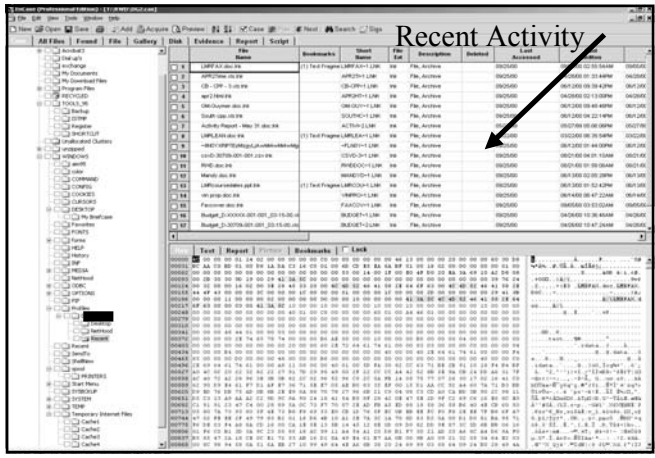
A competing business



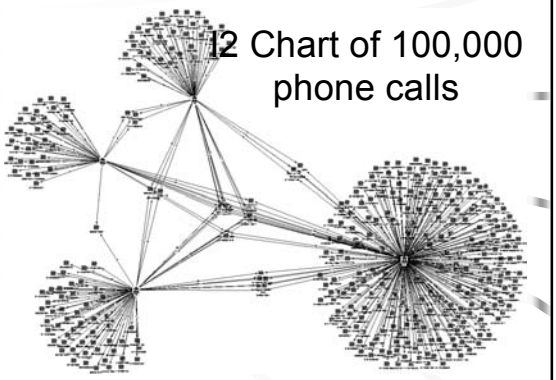
18) RWD02b\C\Unallocated Clusters\C31307-31626
Created Last Accessed Size 10,485,760

19) RWD02b\C\Program Files\Netscape\Users\Default\Cache\MUERB8BV.GIF
Created 06/16/00 03:51:24PM Last Accessed 06/16/00 Size 1,696

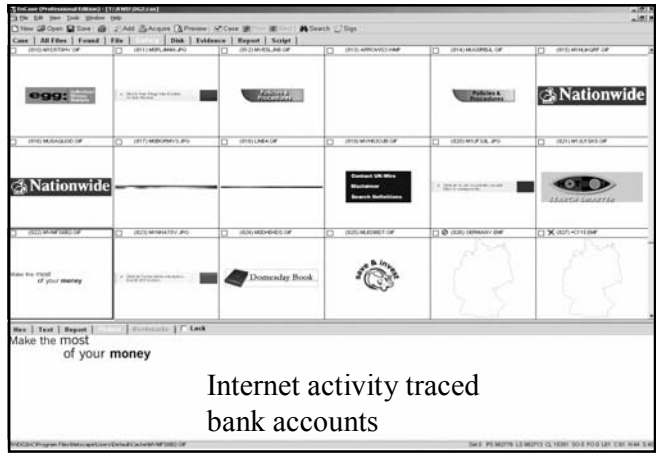
Slack file space evidence used to "date" document



Recent Activity



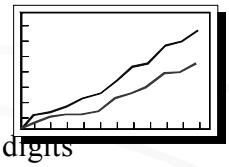
12 Chart of 100,000 phone calls



Internet activity traced bank accounts

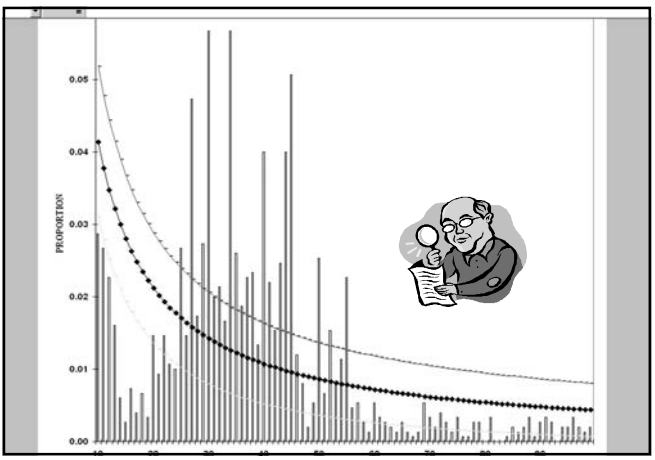
Other types of Digital Analysis

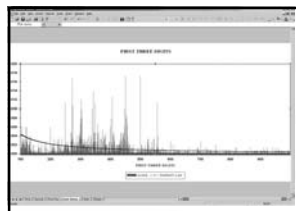
- Data mining
- Relative Size Factor
- Duplicate Payments
- Round Numbers & last 2 digits
- Number Frequency Factor
- Digital Fingerprints



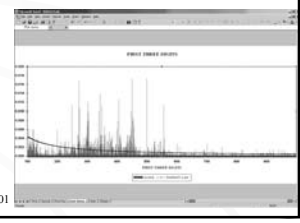
Digital Fingerprints

- Good for continuous audits
- Only just being developed
- Use DATAS™ to profile the data at a specific date
- Then compare it with the profile from a different date

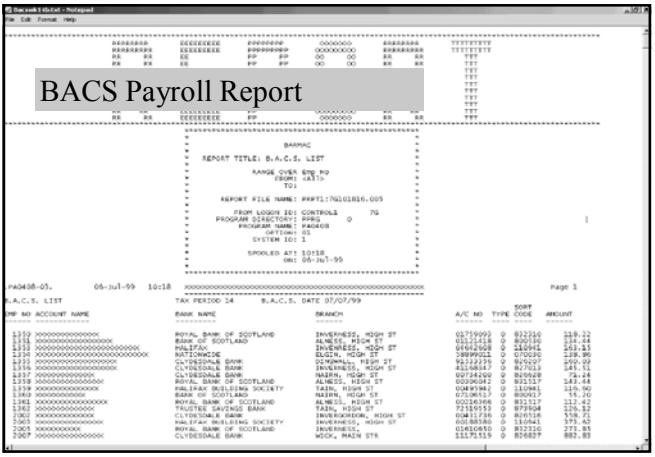


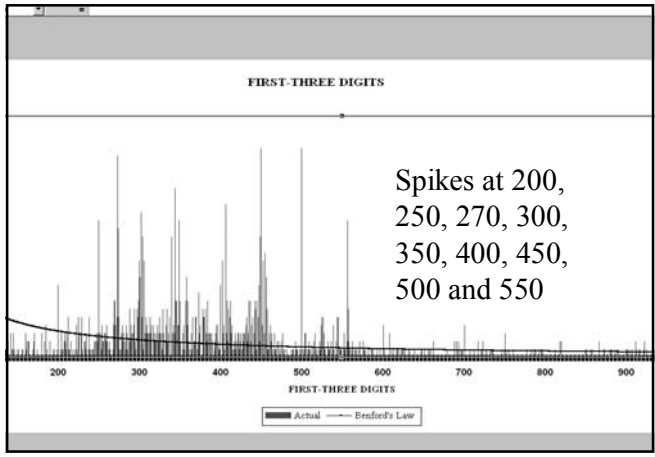


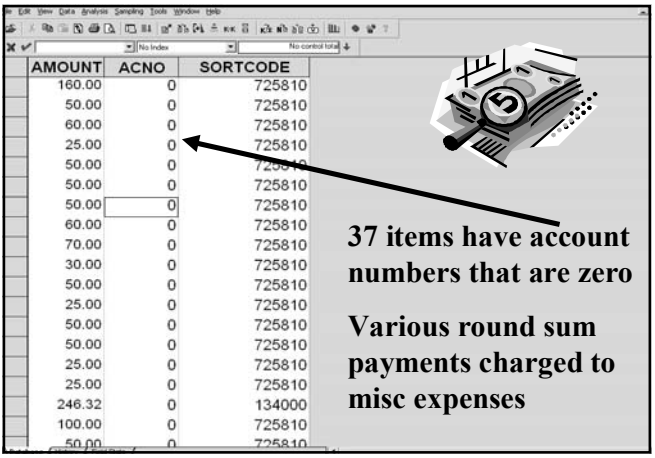
Has the profile changed?



BACS Payroll Report







What have we found?

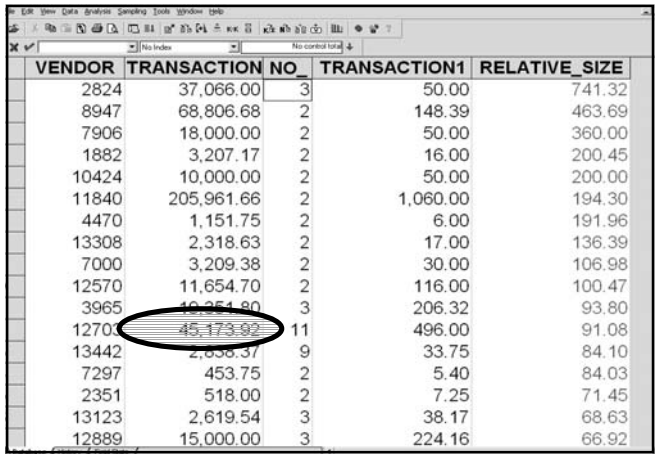
- Deliberate errors introduced into BACS run
- BACS run includes expense payments
- Error report results in cash payments
- Approx £2000 being taken each week and shared between 3 corrupt employees

25,000.00

130.75

Relative Size Factor

- Within a sub-set e.g. Vendor name
- Take largest item and second largest
- Calculate ratio
- Investigate anomalies
- Good at finding mis-postings and errors as well as fraud



VENDOR	TRANSACTION	NO_	TRANSACTION1	RELATIVE_SIZE
2824	37,066.00	3	50.00	741.32
8947	68,806.68	2	148.39	463.69
7906	18,000.00	2	50.00	360.00
1882	3,207.17	2	16.00	200.45
10424	10,000.00	2	50.00	200.00
11840	205,961.66	2	1,060.00	194.30
4470	1,151.75	2	6.00	191.96
13308	2,318.63	2	17.00	136.39
7000	3,209.38	2	30.00	106.98
12570	11,654.70	2	116.00	100.47
3965	19,251.80	3	206.32	93.80
12703	45,173.92	11	496.00	91.08
13442	2,838.37	9	33.75	84.10
7297	453.75	2	5.40	84.03
2351	518.00	2	7.25	71.45
13123	2,619.54	3	38.17	68.63
12889	15,000.00	3	224.16	66.92

Cleaning Company

- 10 regular monthly payments of £496
- Then the big one - £45,173.92
- Awarded maintenance contract in suspicious circumstances
- 3 man company
- Collusion and kickbacks

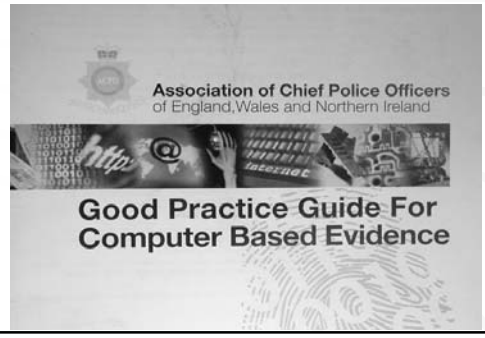
We live in a digital world:

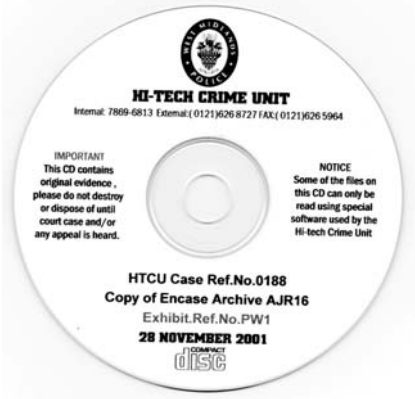
- Traces of what we do are everywhere (Locard's Principle - "Every contact leaves a trace")
- Even if steps are taken to hide the evidence
- Windows OS is particularly good at "covertly" recording the activities of users
- As are many external sources of data e.g. Network Server logs

The digital paradox

- Digital evidence is extremely fragile, and
- Surprisingly resilient!
- But, it needs very careful handling

Best practice guidelines June 1999





The main principles:

- Do no harm – ensure the original evidence is not altered in any way
- Always work from a copy, or a forensic image
- Establish an evidential audit trail
- Ensure any conclusions can be reproduced by the other side

Why use Computer Forensics?

- As part of the overall "evidence gathering"
- To eliminate the innocent
- To identify the guilty
- Usually part of an initial covert investigation, or
- To establish corroboration

What can we expect to see using Computer Forensics?

- Activity involving deception
- True picture of lifestyle / pattern of use
- Internet or server activity
- Copying of documents
- Documents / emails that have been "deleted"

Computer Forensics is particularly useful in cases involving:

- Collusion
- Theft of Intellectual Property or Confidential Information
- Receipt of bribes / backhanders
- Forgery of documents / signatures
- EFT fraud
- Blackmail / intimidation / harassment

"Hidden" sources of information

- Windows Swap File
- File Slack
- Unallocated File Space
- Windows Registry
- Cookies
- "Recent" Links and Internet History
- Access and other logs

Some monitoring can be done remotely

- Can be used for a usage audit
- Shows what staff are doing
- File transfers, internet usage
- Use of passwords and encryption
- Key word triggers

Legal Issues

- Concern about intrusive monitoring (particularly on a covert basis and without informed consent)
- Data Protection Act 1998
- Human Rights Act 1998
- Regulation of Investigatory Powers Act
- Lawful Business Practice Regulations

LBPR allows

- Covert investigation (without prior notification)
- If the circumstances can be justified
- If a less intrusive method can't be used effectively
- In order to prevent or detect crime

Action Points

- Actively consider how to use Computer Forensics within your company
- Make use of the evidence you didn't know that you had!
- Set up contingency plans to capture forensic evidence

Useful websites

- www.haymarketco.com
- www.cifas.org.uk
- www.cardwatch.org.uk
- www.grc.com
- www.sans.org
- www.e-commercetimes.co.uk
- www.wirednews.com
- www.mail-archive.com (cyber crime alerts)

Where to go for further help

Ian Henderson

irh@haymarketco.com
020 7730 3244 Direct Line
020 7823 4141 Office
07940 540 399 Mobile

Haymarket Management Services Limited

Biographies of key consultants

Ian R Henderson FCA

Ian Henderson is a Director of Haymarket Management Services Ltd ("Haymarket") and is also responsible for Haymarket's Forensic Accounting and Forensic Computer services.

After 7 years as an Army Officer specialising in covert operations and intelligence work, he qualified as a Chartered Accountant with the London Office of Binder Hamlyn, now part of Arthur Andersen. He specialised in investigations and computer audit at an early stage and worked on a number of Government and Department of Trade investigations.

Mr Henderson joined the regulatory division of Lloyd's of London in 1986 and was subsequently appointed Head of Investigations, where he was responsible for investigating suspected fraud or misconduct world-wide. He also managed a team dealing with contractual disputes within the London Insurance Market. He personally led field teams in the United States and Caribbean in order to recover financial assets on behalf of underwriters. He regularly provided affidavit and expert witness evidence to law enforcement authorities in the United Kingdom and overseas and was a member of the Hendon Police College lecture panel. He was also responsible for a number of highly technical reports covering insurance losses totalling more than £3 billion. These reports were quoted extensively in the press and in proceedings in the High Court.

In 1996 Mr Henderson was appointed Head of Investigations at the Personal Investment Authority, the U.K.'s leading Financial Services regulator. He was responsible for many high profile investigations covering such diverse areas as pensions mis-selling, money laundering, mortgage fraud and theft of client funds. He was also responsible for negotiating settlements in disciplinary cases. He was appointed by the Bank of England as a full member of FFIN, the Financial Fraud Information Network and had regular contact with senior officials at the Treasury, the DTI, the SFO and other Financial Services regulators.

In 1998 Mr Henderson moved into the private sector and was appointed Investigations Director of a company specialising in the prevention, detection and investigation of corporate fraud. In addition to this role he was subsequently appointed Director of Forensic Accounting. Mr Henderson was responsible for a number of complex investigations and other work on behalf of private and corporate clients in the U.K., Europe, the Middle East and North America. These cases included a risk review on behalf of a FTSE 100 listed company, an investigation into a company that had received a clean audit report from a "big five" accountancy firm, but where Mr Henderson was able to demonstrate material mis-statement in the published accounts due to a fraud by the executive chairman. Mr Henderson was also appointed by the High Court and it's equivalent in Scotland, the Court of Session, in order to obtain and analyse computer forensic evidence on a number of occasions. This work inevitably led to substantial financial recoveries.

Ian R Henderson FCA (continued)

Since joining Haymarket in March 2000, Mr Henderson has managed a number of major investigations for blue chip clients. These included an electronic funds transfer fraud involving over £500,000 which resulted in a successful recovery, the identification of over £40 million of excessive payments on a £200 million construction contract, the detection of sexually explicit internet messages leading to dismissal of a senior member of staff and the recovery of evidence that allowed a claim for unfair dismissal to be successfully defended.

A particular professional interest is the recovery, analysis and presentation of digital evidence. Mr Henderson has developed a number of innovative techniques in this area, which are particularly appropriate in cases involving the theft or transfer of intellectual property, the loss of confidential information, or when conducting due diligence enquiries.

In January 2001, Mr Henderson was appointed Special Advisor to the Criminal Cases Review Commission, where he provides professional advice on high profile fraud cases.

In addition to his client work Mr Henderson regularly speaks at conferences organised by bodies such as the Institute of Chartered Accountants in England and Wales and the Institute of Internal Auditors. He has written a number of articles on fraud and compliance matters for specialist publications and the Financial Times and is often interviewed by the BBC.

Mr Henderson is a Fellow of the Institute of Chartered Accountants in England and Wales and an active member of the Audit and Information Technology Faculties of the ICAEW.

Contact details

Ian R Henderson FCA
Director

Haymarket Management Services Ltd
27 Eccleston Street
London SW1W 9NP

Telephone: +44 (0)20 7823 4141
Facsimile: +44 (0)20 7823 4144
Mobile: +44 (0)7940 540399
Direct Line: +44 (0)20 7730 3244

Email: irh@haymarketco.com

Website: http://www.haymarketco.com