ARTHUR COX

Computer Fraud

A TECHBRIEF SUPPLEMENT IN CONJUNCTION WITH

ERNST & YOUNG

Introduction

Following increased media attention computer fraud is now a hot topic in all levels of corporate management. Computer fraud is a broad term which covers most forms of corporate fraud, given that the computer is the essential tool in most businesses and most corporate data is created, used, and retained in electronic format, quite possibly never committed to paper format.

Given the high level of interest within the business community in all aspects of computer fraud, it was felt that a publication setting out a broad overview of the area would be of interest to Irish business. Arthur Cox has worked closely with the Security and Technology Solutions department of Ernst & Young and is grateful for their assistance in this project. See Statistics Summary to the right for an overview of the prevalence and effects of computer fraud.

Computer fraud may be summarised as the use of information technology resources to commit or conceal a criminal offence or civil wrong. Computer fraud typically includes:

- financial fraud;
- sabotage of data and/or networks;
- theft of proprietary information;
- system penetration from the outside, including denial of service;
- unauthorised access by insiders, including employee misuse of internet access privileges; and
- malicious software (such as viruses, worms, trojans, time bombs, zombies), which is the leading cause of unauthorised users gaining access to systems and networks via the internet.

Typically computer fraud can be categorised as either an internal or external offence. From a financial perspective, the largest threat to business to date has been from insiders. Ernst & Young's global research has found that approximately 85% of all identified frauds were committed by employees, almost a third of which were committed by management (see Statistics Summary in side bar).

Recent financial scandals, particularly in the US, have raised public awareness of fraud largely because of their extent and complexity. Corporate governance has become an issue of interest not just to shareholders but to the public at large. Both employees and corporate officers are now required to bear higher levels of responsibility and accountability for the companies in which they work. Set against this is the all-pervasive nature of the computer and communication technology in business. Business take-up of advances in information technology products has generally not been reflected in a take-up of advances in security products, or, indeed, in a general review of corporate policies and procedures, with a view to minimising the opportunities for computer fraud.

This briefing note will provide an overview of computer fraud, both from a technical and legal perspective, an analysis of how computer forensics works in practice, and a number of recommendations intended to help reduce the scope for corporate computer fraud.

Statistics Summary

Is it Real?

According to US statistics released by the *Federal Bureau of Investigation* (FBI):

- 90% of companies admit to a security breach in the last 12 months
- 80% of companies admit a loss; financial loss and loss of intellectual property are highest
- 78% of companies report abuse of Internet access by ‘ insiders’.

The *National High-Tech Crime Unit* (NHTCU) report that:

- 88% of UK companies face a genuine threat of financial loss from computer fraud.

The *E&Y Fraud Survey* 2003 reports in relation to Ireland that:

- 60% of companies experienced fraud in the last year
- 85% of fraud is committed by insiders of the company (on the payroll)
- 50% of that group was management (up from 33% in 2001 survey)
- 20% only of frauds were made public
- 51% of losses were recovered from insurers, banks & suppliers (up from 29% in 2001 survey)
- 50% of companies have acceptable usage policies in place (up from 33% in 2001 survey).

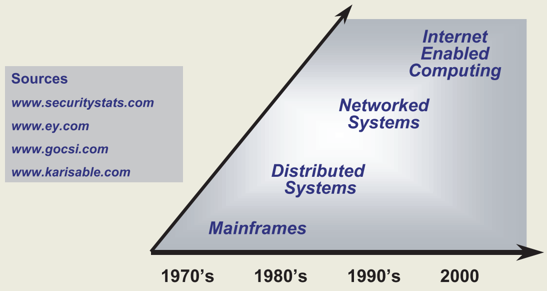
Is it Costly?

The Association of Certified Fraud Examiners (CFE) on international organisation reports the average losses per incident are in the region of:

- €127,000, when an employee acts alone
- €250,000, when an executive acts alone
- €500,000, when an executive and employee cooperate.

The E&Y Fraud Survey 2003 reports in relation to Ireland that financial losses vary from 50% at over €100,000, to 13% at over €1m.

Trends in Computer Fraud



Computer Fraud – Legal Issues

Know your Enemy & Manage your Risk

Overview

The legal issues associated with computer fraud can be broken down between the criminal and civil law. Fraud has a specific meaning in criminal law, as there is no fraud committed under criminal law unless and until a criminal offence can be identified and proven. Also, it is true to say that not all dishonesty is a crime. Companies should be aware of the position under both criminal and civil law, in order to put in place appropriate preventive and reactive planning to reduce the risk of an event of corporate fraud occurring.

Prevention is better than Cure

Criminal Law

Fraud is not a specific criminal offence of itself. Rather fraud is an umbrella term which includes criminal offences such as conspiracy, larceny, obtaining by false pretences and various breaches of the Companies Acts, 1963 – 2001. The most relevant statutes in the area of computer fraud are the Criminal Damage Act, 1991 and the more recent Criminal Justice (Theft and Fraud Offences) Act, 2001. This article will concentrate on the recent computer fraud specific legislation.

The Criminal Damage Act, 1991, (the"1991 Act") at Section 2(1) introduced the offence of damage to property, defined as – "*a person who without lawful excuse damages any property belonging to another intending to damage any such property or being reckless as to whether any such property should be damaged is guilty of an offence.*" Property includes data and damage to data includes the addition, alteration, corruption, erasure, or movement thereof, or introduction of a virus therein, which causes damage. It shall be noted that the offence requires the absence of "lawful excuse" and, in addition, requires the accused to act with intent or recklessness. Differing penalties apply on summary conviction or on indictment (meaning trial by jury). On summary conviction the penalties are a fine of up to €1,270 or imprisonment for up to 12 months, while on indictment, the penalties are a fine of up to €12,700 or imprisonment for up to 10 years, or both.

As with most criminal legislation, the 1991 Act introduced a range of offences. Section 3 of the 1991 Act introduced the offence of threatening to damage property and Section 4 introduced the offence of possession of any thing with intent to damage property. Both carry the same penalties as a Section 2 offence. Section 5 then introduced the offence of operation of a computer with intent to access data without lawful excuse. The offence is defined as – "*a person who without lawful excuse operates a computer within the State with intent to access any data kept either within or outside the State, or outside the State with intent to access any data within the State, shall whether or not he accesses any data, be guilty of an offence*". The penalties on summary conviction are a fine of up to €6,349, or imprisonment for up to 3 months. The penalties are light and therefore the offence has in the past not been perceived as a serious offence. However, it is the offence which, prior to the introduction of the more recent legislation, was typically relied on by the law enforcement agencies. It can be seen that either (or both) the perpetrator and the data may be located either inside or outside the State. It is also worth noting that the required intention must be to access any data and not necessarily specific data and that the accused need not succeed in accessing data.

The law in relation to computer fraud has recently been updated and augmented with the introduction of the Criminal Justice (Theft and Fraud) Offences Act, 2001 (the "2001 Act"). The 2001 Act introduced a number of new offences into Irish law, the most important of which arises under Section 9. Section 9 states – "*a person who dishonestly, whether within or outside the State, operates or causes to be operated a computer within the State with the intention of making a gain for himself or herself or another, or of causing loss to another, is guilty of an offence*". This section introduced the concept of "dishonesty" into Irish computer-related offences. The perpetrator can be located either inside or outside the State and is required to act dishonestly, meaning "*without a claim of right made in good faith*". The operation of a "*computer*" is required. The 2001 Act is technology neutral in not defining the term, reflecting a general legislative tendency to allow for technology development.

Section 9 of the 2001 Act requires the presence of intent, which could relate to the unauthorised access of another's computer or, alternatively, authorised access of a computer for unauthorised purposes (bad faith use). The intention must be to make a gain, whether for himself, or herself, or another, or, alternatively, to cause a loss to another. Section 9 is a more serious offence than existed under the 1991 Act. It is an indictable offence, carrying a potential fine of unspecified amount, or maximum of 10 years' imprisonment, or both.

As part of a corporate policy of fraud prevention and as part of good corporate governance, it is recommended that companies:

- implement a fraud detection/prevention programme, as mentioned below;
- attempt to avoid criminal investigation by avoiding fraud. A criminal prosecution, which is a matter for the law enforcement agencies of the State rather than a company, will invariably bring bad publicity and make demands on the time of corporate officers and staff.

Common Law

The Statistics summary at page 1 points to the prevalence of computer fraud that could be committed by people within an organisation similar to your own. Fraud should be treated by companies in the same way as any other business risk, meaning that the risk should be scoped, a pro-active approach taken to risk management, corporate plans should be implemented and procedures put in place to prevent, detect, and react to corporate fraud. Finally, the company should check its policies of insurance. A corporate fraud alert plan covering the key issues of detection, reaction, and prevention, would include a fraud prevention plan (prevention), together with a fraud contingency plan (detection and reaction).

Detection

Fraud tends to get detected by accident, at times of change in personnel, as a result of corporate audit process, as a result of corporate risk management procedures, and, finally, due to tip-off (generally a sliding scale).

Prevention

A fraud prevention plan would include the identification and assessment of corporate risk areas and implementation of a controlled programme relating to both corporate personnel and records/accounting. It is advisable that a fraud prevention plan has senior level approval including, where possible, board of director approval. It is also necessary to address corporate awareness, which is an important prevention point. Finally, it is necessary to review and update the plan at regular intervals, as the business develops.

Reaction

A fraud contingency plan should have senior level approval, should be communicated in general terms to staff, and included within corporate training, noting that there will be an element of secrecy in relation to the reaction element of the plan. In terms of administering the plan it is recommended that responsibilities be assigned to key personnel, especially in relation to reaction matters, which would include the preservation of evidence of fraud, maintenance of confidentiality, reporting upwards within the plan structure and (perhaps) taking an initial decision as to whether one should report the incident to the Gardai. The contingency plan should be regularly reviewed and updated.

A financial recovery policy should be included within the contingency plan. Recovery is mainly a civil law matter and the primary aim of the Gardai is to bring the fraudster to justice in the criminal side. Whether or not recovery is possible will very much depend on the circumstances, including the location of the assets. What the Gardai may do is assist in identifying the location of assets, rather than assist in corporate recovery.

Manage the Risk

A number of the key areas in contingency plan implementation and general management of internal fraud are:

- employee contracts of employment – these should be reviewed in light of corporate requirements and employee contractual rights;
- law of defamation;
- requirements of natural justice and fair procedures;
- statutory employment law and, in particular, unfair dismissal law;
- responsibility for liaison with external agencies, including the press, lawyers, security specialists and PR advisors; and
- requirements in relation to preservation of evidence.

Evidence

Evidence is a key risk area which applies to both criminal and civil law. In both cases, the prudent advice upon becoming aware of an incident of computer fraud is to:

- locate and secure the environment;
- consult security specialists and legal advisors;
- be aware of the criminal burden of proof ("beyond reasonable doubt");

- be aware that the ability of the alleged wrongdoer to cover his or her trail could jeopardise the case (both civil and criminal);
- be aware of employee rights, abuse of which could jeopardise the case; and
- Catalogue all electronic devices that the potential fraudster had access to.

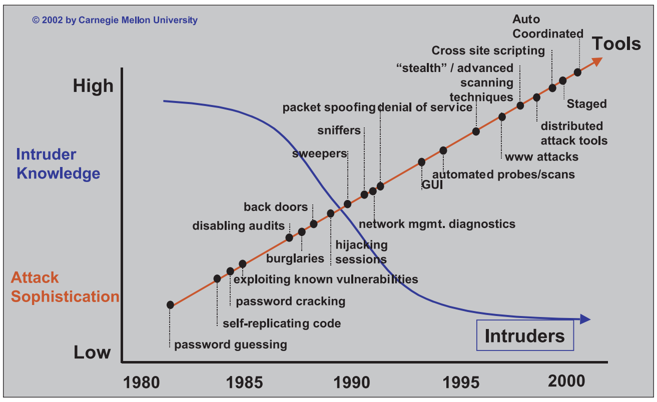
In relation to manual records and documents, original documentation should be exhibited where possible and there will be a requirement to prove documentary information (who made what entries, when and why). This can boil down to an issue for security experts and forensic analysis. It is worth noting that CCTV can constitute admissible evidence.

Summary

Computer fraud is best viewed as another business risk. Like all business risks it requires business management. The recommendation is that companies implement both a prevention plan and contingency plan, the details of which will vary depending on the size, complexity and area of company business. In general, companies should recognise the potential for computer fraud, assess the risk and plan risk management. Such planning and it's publicity will, if nothing else, help deter fraud. Finally, in the event of an incident of computer fraud, it is recommended that companies liaise with their security specialists and legal advisors in promptly in order to react in the most effective manner.

Diagram 1

Reduced Technical Skills for Computer Fraud



Computer Fraud & Forensics

Factors causing an increase Computer Fraud in Ireland?

- Ireland's economy is based on Intellectual Property; #1 exporter of software in the world;
- Business reliance on PCs;
- Exponential growth in the use of email;
- A competent workforce that is comfortable with IT;
- The technical skills required to compromise IT systems have decreased and 'hacking' tools have become increasingly sophisticated (see diagram 1);
- Redundancies in the IT sector.

How is Computer Fraud most often 'discovered'?

- 'Stumble' across it as a result of a change in the control of sensitive data or systems;
- Audit or data analysis;
- 'Tip-off' by someone with insider knowledge.

What to do you do if you suspect Computer Fraud

- Don't panic – gather a support team (Legal, Audit, HR, Public Relations, Information Technology, etc.);
- Develop a plan;
- Start documenting: Who? - What? - When? - Where? - How?;
- Identify who will 'own' the investigation;
- Limit information of the incident to people with a need-to-know;
- Get advice from a Computer Forensics specialist.

What is Computer Forensics?

- The application of computer science and legal procedures to identify and collect evidence in a criminal or civil matter.

How is it different from any technical search of a computer?

- There are multiple ways to search computers and recover data using shareware. However, just viewing or retrieving data from computers can alter the data itself or the dates and time stamps associated with it. Although the data can often be found and recovered, it may have little value in criminal, civil or administrative proceedings.

- Computer Forensics uses tools and procedures to make sure the data recovered from the computer will comply with the rules of 'best evidence' and be admissible in any legal proceedings.

How does Computer Forensics find 'evidence'?

Computer forensics exploits the file system of computer operating systems to recover 'evidence'. Think of a modern computer file system as an 'inefficient library'.

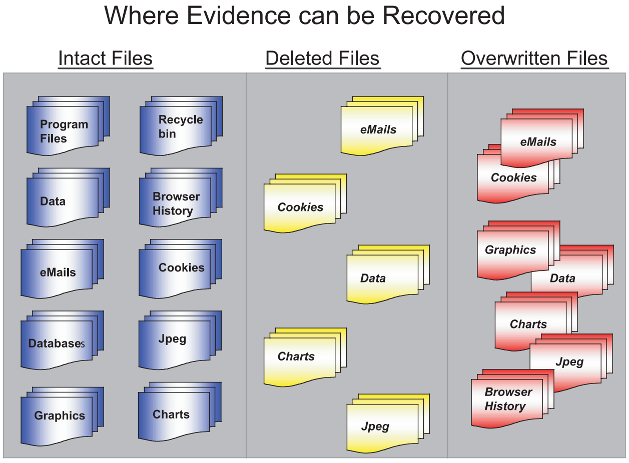
For data stored on the hard drive:

- The file system identifies where to store documents and images in sectors (shelves) and clusters (bookcases) in the hard drive;
- The file system then assigns an entry (an index card) for each document or image in the file system table (card catalogue).

When you type a 'delete' command, the file system only removes the file table entry – it does not eliminate the document or image; in the library analogy only the 'index card' (file table entry) is removed from the card catalogue (file table). Consequently, the 'deleted' file can often be recreated (see diagram 2).

When you type the 'save' command the file system stores the new file, document or image on top of the old data; the analogy is that the new library book may not have as many pages as the old book that was previously on the shelf and the new 'pages' may not completely over-write the pages of the old book. Consequently, the 'old' data can often be recovered (see diagram 2).

Diagram 2



Where do you look for evidence?

- Intact files
- Deleted files
- Unallocated space
- Cluster slack
- Sector slack
- Volume slack
- Swap files
- Hidden Files
- Temporary files
- Browser cache
- Internet history files
- Mail remnants
- Instant messaging files
- Registry entries
- System logs
- Security logs
- Application logs

What can be recovered? (often but not always)

- Hidden files
- Damaged or corrupted files
- Deleted files
- Password protected files
- Some encrypted files
- Email – web mail correspondence
- Evidence of web browsing
- Internet chat data

Case Study

Scenario

Jim, a middle level manager in a large company, goes away on annual leave. Jim works in the marketing department, but not in a position entitling him to possession of sensitive and confidential information relating to planned M&A activity. In Jim's absence the MD required sight of the latest version of the marketing budget document and asked the IT department for access to Jim's PC. In the course of the MD's search sensitive documents relating to planned M&A activities, which should not have been in Jim's possession, were discovered.

The MD did not recover these documents from Jim's PC or secure the PC and did not suspend Jim's access rights. On his return to the office, Jim was interviewed.

He subsequently "wiped" the hard drive on his PC to remove evidence of the incriminating documents. In accordance with the company's employment procedures, Jim was asked to attend a meeting with an internal investigation committee before which he was informed that sensitive documents had been discovered on his PC. At the meeting Jim denied knowledge of the documents and claimed that his computer was "hacked" and the documents placed there. Jim was temporarily suspended, on full pay, pending conclusion of the company's disciplinary proceedings. Jim's access rights were still not removed. A full disciplinary hearing was arranged prior to which it was discovered that the relevant documents were missing from Jim's PC. This put the company in a difficult position.

Computer Forensics

Computer forensics specialists were engaged and the following investigations were conducted:-

- Jim's desktop environment was documented, photographed and secured;
- Jim's desktop drive was removed and a mirror image created in order to conduct a search;
- evidence of "tampering" with the PC logs was identified. In particular, gaps were discovered in the computer audit log and large areas of the hard disk were discovered to have been wiped;
- web mail, internet chat, and browser cache fragments were recovered.

Evidence Recovered

The computer forensics investigations recovered the following from Jim's PC:

- incriminating extracts from internet chat relays involving Jim and another employee, Jenna;
- internet browser cache fragments; and
- webmail.

The scope of the investigations were then extended to Jenna and her PC.

The browser cache fragments recorded from Jim's PC indicated that he was trying to learn how to hack other employees' e-mails and how to eliminate the "evidence" that was found by the MD on his desktop. Jim also made an internet search on how to "read other users' mail on exchange" which was recovered (the company used Microsoft Exchange for their mail system).

Legal Input

The company's solicitors were engaged to assist the company, firstly, in relation to the discovery of the scope of breach of its confidential information and protection of its business assets and, secondly, in relation to internal disciplinary proceedings.

During the course of investigations, it was discovered that company confidential data had been exported from Jim's PC to a third party. Promptly on becoming aware of this, the company sought an injunction before the High Court, which was granted late on a Friday afternoon, with immediate effect. This injunction was addressed to the third party recipient of company confidential information who was ordered to cease use of such information and to surrender up all information in its possession. The purpose of an injunction is to provide interim relief, pending full court proceedings. Given that the third party had misused confidential information, which they could reasonably have determined to be proprietary to the company, the company decided to institute legal proceedings. The financial implications of which could be serious, given that the information related to new product development and the third party was a competitor. The company took a view that, notwithstanding the bad publicity that could result from making a public application for an injunction in the High Court, it was, on balance, necessary to protect the assets of the company and maintain shareholder confidence.

In relation to internal employment proceedings, Jim was sent the report prepared by the computer forensics specialists, based on the evidence gathered by them, and was informed of the allegations against him arising from the report. He was called to a disciplinary meeting and was invited to submit, in writing, prior to the meeting the reasons why disciplinary action, up to and including dismissal, should not be taken against him. Following the meeting a decision was taken to dismiss Jim summarily. Following a similar investigation and disciplinary procedure in relation to her alleged involvement Jenna received a written warning. Also, Jim, on foot of a company threat to immediately apply for an injunction ordering surrender up of company proprietary data, surrendered all company data in his possession, and undertook in writing not to have any further dealings with company proprietary data. Needless to say, Jim did not receive a reference from the company.

Conclusion and Lessons Learned

It can be seen that, based on the company taking prompt action, and, in particular, engaging computer forensics specialists and lawyers, the company was able, firstly, to discover the extent of damage caused by the actions of its employees and, secondly to take steps to recover proprietary confidential data removed from the company. The company subsequently carried out a thorough investigation, which concluded that:

- internal technical computer controls were poor, allowing unauthorised access to determined employees;
- the company's internal failure to secure Jim's PC and remove access rights caused loss of key evidence;
- company terms and conditions of employment required tightening up in relation to obligations to safeguard company proprietary data; and
- strategic proprietary information should be protected against copying to external devices.

DO's and Don't's of Computer Fraud

DO

- Have an IT acceptable usage policy.
- Ensure that the policy is included in employment terms.
- Document your activities: Who? What? When?
- Determine who will 'manage' the investigation
- Control information about the incident
- Get technical advice
- Gather evidence 'legally'
- Document the 'chain' of control of the evidence
- Secure the suspect's computer and work area
- Disconnect the suspect's computer from the network / modem
- Remove the suspect's computer access
- Verify the accuracy of the computer's internal clock
- Write protect all diskettes and removable media

DON'T

- Conduct interrogations without all facts
- Gather electronic evidence without expert advice
- If the computer is switched-on do not switch it off
- If the computer is switched-off do not switch it on
- Save data on the screen to the hard drive
  - do save to a diskette (A:drive)
- Examine original computer media - do use copies

Good Practices to Prevent Computer Fraud

- Conduct Periodic Technical Security Testing
  - Internet
  - Intranet
  - PBX
  - Applications
- Data Analytics of Accounts Payable - Accounts Receivable
- Make Computer Fraud part of your Employee Awareness program
- Conduct background checks on sensitive positions in IT
- Audit IT processes; Access authorisation, Change management,
- Establish clear 'Acceptable Use' policies for eMail, Internet, computers
- Educate Management
- Establish a Fraud 'Hotline' for employees and business partners

Contacts

Greg Glynn, Partner, Arthur Cox gregory.glynn@arthurcox.com Tel: +353 1 618 0470
Greg's practice involves commercial and civil litigation, including IT fraud related disputes.

Pearse Ryan, Associate, Arthur Cox pearse.ryan@arthurcox.com Tel: +353 1 618 0518
Pearse specialises in information technology and technology related intellectual property law. Pearse's practice areas include IT supply and procurement, outsourcing, computer fraud, IT related PFI/PPP and IT related disputes.

Dan Quealy, Director, Ernst & Young daniel.quealy@ie.ey.com Tel: +353 1 475 0555 ext. 848
Dan is Director of the Ernst & Young Advanced Security Centre, Dublin. Dan has an advanced degree in Computer Science and 20 years experience in Telecom, Computer Security and Forensic Investigations.

Andy Harbison, Manager, Ernst & Young andrew.harbison@ie.ey.com Tel: +353 1 475 0555 ext. 819
Andy is a manger with the Ernst & Young Advanced Security Centre. He holds advanced degrees in Electronics Engineering, Business Administration and IT Management. Andy leads the Computer Forensics Team for Ernst & Young.

This document contains a general summary of developments and is not a complete or definitive statement of the law. Specific legal advice should be obtained before taking action.