EDITH COWAN UNIVERSITY

Computer fraud in the banking and finance industry is on the increase.

CONTENTS

1. ABSTRACT 2

2. INTRODUCTION 3

3. HISTORY OF COMPUTER CRIME 3

4. MECHANISMS OF COMPUTER FRAUD 5

1. FRAUD PERPETRATED BY EMPLOYEES 6

2. FRAUD PERPETRATED BY FINANCIAL INSTITUTIONS 7

3. FRAUD PERPETRATED AND/OR TOLERATED BY GOVERNMENT BODIES 7

5. TRANSNATIONAL CORPORATE CRIMINALS: CASE STUDIES 8

1. EQUITY FUNDING 8

2. HERTZ CORP 8

3. ENCYCLOPAEDIA BRITANNICA, WATERFORD GLASS COMPANY 8

4. SAXON INDUSTRIES 9

5. MICROSOFT/NSA CONSPIRACY 9

6. INVESTIGATION, PREVENTION, AND CIVIL PROTECTION 9

7. CONCLUSION 10

8. REFERENCES 10

Computer fraud in the banking and finance industry is on the increase.

> *" The Equity Funding hoax is the most monumental money swindle of all times. Through a spectacular scheme of fakery, Equity Funding had created over $100 million in fictitious assets. It had forged death certificates, counterfeited bonds, and created bogus insurance policies…[…]…tapes were programmed so that computers would reject the incriminating data and accept and produce only what would support the conspiracy."* (Farr, 1975).[1]

1. ABSTRACT

This paper investigates the increasing incidence of computer assisted crime in the banking and finance industries. While concurring with most analysts that incidence of fraud is on the rise, it is intended to demonstrate here that the traditional computer criminals (antisocial elements, hackers, etc.) have largely been replaced, and their activities dwarfed, by institutions, corporations and even governments. By using specific case studies it is shown that transnational corporations and financial institutions, with the tacit compliance of 'pro-big-business' governments, have been able to take over some of the electronic fraud activities previously perpetrated by petty cyber criminals. In many cases they have 'legalised' these activities with the complicity of governments' regulatory bodies, and applied them on a mass scale, thereby defrauding their customers and/or the general public of vast sums of money.

This paper traces the history of computer fraud, its parallel evolution to the development of increasingly more sophisticated software and hardware, as well as researching the mechanisms by which financial fraud can be conducted, investigated and prevented. The complexity of the issues concerned, coupled with the mountains of available data on the topic, pitch an exhaustive investigation beyond the scope of this paper, and research here has therefore been limited to 4 areas of inquiry:

1. History and evolution of computer crime in financial and banking institutions
2. Mechanisms of computer fraud
3. Transnational corporate criminals: case studies of corporate/government financial fraud
4. Investigation, prevention, and civil protection.

The conclusions drawn, on the basis of an analysis of all available resources (lecture notes on ECU network, Virtual Campus webservice, the unit text books, library books, journals, publications, newspapers and online information) indicate that the appropriation of

[1] Farr, R. (1975). The Electronic Criminals. USA: McGraw-Hill

information technologies by large corporations, particularly financial and banking institutions, represents a real threat to the individual's financial security. This threat has been rising sharply, and will continue to rise, with a redefinition of legal frameworks conspiring to perpetuate the fraudulent misappropriation of funds by these institutions.

2. INTRODUCTION

> *"...communications technologies bring many benefits, but they also create new social and ethical problems. Computer assisted crime is one of the most serious, and its apparent growth in recent years demonstrates clearly how new technologies create new opportunities for criminal activity."* Forester and Morrison (1990).[2]

The growth of computer crimes and fraud generally is seldom disputed by anyone today. Most observers agree with Morrison and Forester, quoted above, and evidence in support of this position is presented below, as well as corroboration from other sources, both academic and technical. With the widespread use of computer and Internet technologies in recent years has come a correspondingly large increase in computer crime and fraud. Bank robbers can achieve their objectives with no violence, weapons, fast cars, safe crackers or expensive equipment. Furthermore there is little risk of arrest, or even (in many cases) of the crime being detected. Almost every other traditional criminal activity, from gambling to prostitution can now be conducted online, or has an electronic counterpart. In his book, *Technocrimes: The Computerisation of Crime and Terrorism* (1987)[3], August Bequai alleges that organised crime and the Mafia are using computers for record-keeping, extortion, blackmail and sabotage. Today, we can add *communications* to that list. However, this paper will focus exclusively on establishing that the massive increase in the incidence of electronic fraud in the banking and finance industries is conducted either by rogue employees of these industries, or, increasingly, by the institutions themselves as part and parcel of their economic policies. In many cases, it will be shown, these fraudulent activities have been sanctioned by the *laissez faire* politics of conservative governments wary of offending the economic sensitivities of powerful mega-corporations.

3. HISTORY OF COMPUTER CRIME

> *"despite our greater reliance on network computing, the Internet isn't a safer place today than it was in 1991. If anything, the Internet is quickly becoming the Wild West of cyberspace."* Simson Garfinkel and Gene Spafford, (1996).[4]

---

[2] Forester, T. & Morrison, P. (1990). Computer crime: New Problem for the information society. Prometheus, Vol.8, (pp 257-272).

[3] Bequai, A. (1987). Technocrimes: The Computerisation of Crime and Terrorism.

[4] Garfinkel, S. & Spafford, G. (1996) .Practical UNIX and Internet Security: Second Edition.

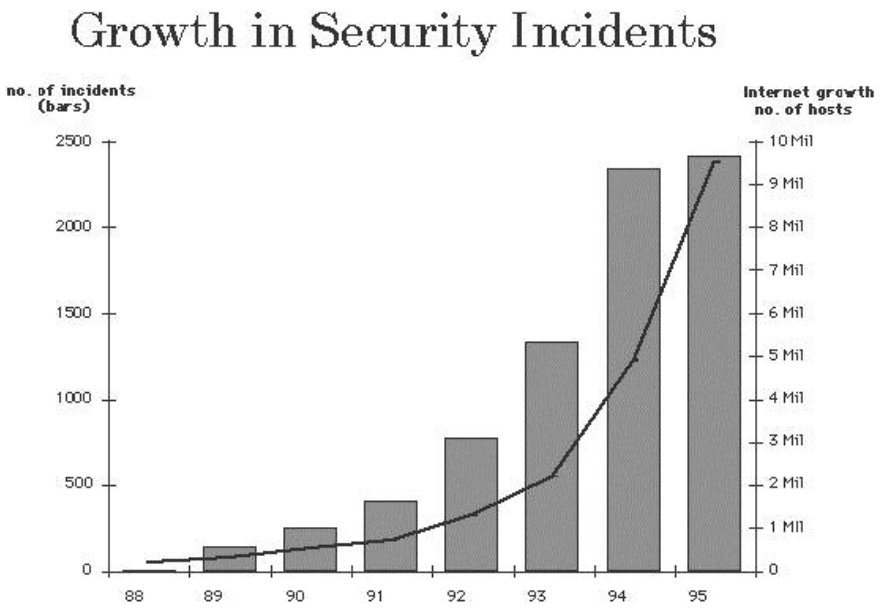
The history of computer crime is arguably older than computers. Even before computers as we know them today could even be conceptualised, science fiction writers had been speculating on their potential abuses. As far back as 1941 John von Neumann anticipated the advent of the computer virus in *Theory and Organisation of Complicated Automata,* proposing that computer programs could multiply on their own. Other examples include the 1950's *Core Wars* game, where programs attacked each other and altered code, and David Gerrold's ScFi in 1972 . The following figures presented by Dr Timo Vuori[5] (quoting a report presented to the National Commission on Fraudulent Financial Reporting), illustrate the evolution and increase of the problem:

- Security Pacific National Bank lost $10.2 million through fraud of its fund transfer system.
- In the 1980's WA Inc reputedly lost $700 million
- BankWest (R&I) lost $28 million during that same time
- US losses due to computer crime were estimated at $3-5 billion/annum in 1992, of which only 5-20% were actually reported
- Stanford Research Institute maintains that computer fraud had been growing at 500% per annum in the 1980's
- Automatic Teller Machine (ATM) fraud is estimated at $(US)1billion + per annum
- The Daily Telegraph newspaper estimated that the 4 main UK clearing banks had made provision for £98 million for computer related fraud using bank cards.
- According to the FBI, the average computer crime is currently worth US$600,000.

The true extent of the problem today is not, and cannot be known as the overwhelming majority of cases are not reported. Banks and financial institutions are reluctant to compromise the reputation of their companies by publicly admitting that their security has been breached; the loss of income resulting from such disclosures would in most cases far exceed the stolen funds. Another reason is that many computer crimes go *undetected*, making it unlikely that we shall ever uncover more than the tip of the iceberg.

The chart below, however, serves to illustrate the steady growth in discernible security incidents between 1988 and 1995.

[5] Vuori, T. (1999, September). Computer Security, Lecture 2. Lecture presented to Computer Security students, Edith Cowan University, Perth, WA.



Published in *The Froehlich/Kent Encyclopedia of Telecommunications vol. 15.* Marcel Dekker, New York, 1997, pp. 231-255. Available on-line http://www.cert.org/encyc_article/tocencyc.html#SAT

The American Bar Association, in a report published in 1984 stated that losses sustained by US business ranged from US$2 million to US$10 million for each of the top 300 businesses, and concluded that:

> "*if the annual losses attributed to computer crime sustained by this relatively small group are conservatively estimated in the range of half a billion dollars, it takes little imagination to realise the magnitude of the problem on a nationwide basis."*[6]

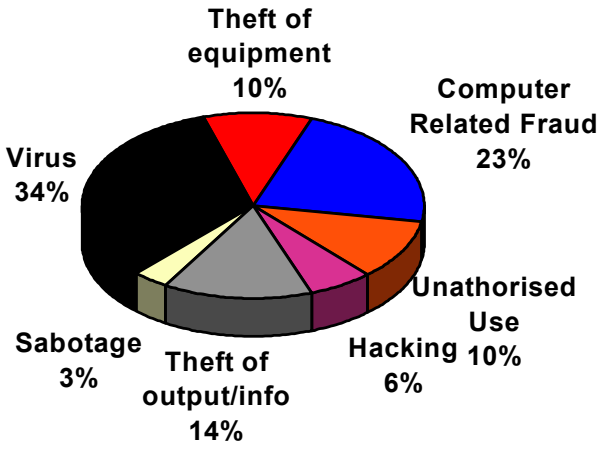
More recently the Cleveland accounting firm Ernst & Whinney estimated that the losses sustained by US companies in total amount to between $3 billion and $5 billion each year[7], while in the UK a survey of 50 British companies, conducted by insurance brokers Hogg Robinson concluded that computer crimes were costing UK firms well over ≤40 million a year. Clearly this is a situation giant financial institutions, obsessed with maximising profits, cannot tolerate. In relation to the computer criminals, the banks and financiers are presented with only 2 options: Beat them, or join them! We hope to demonstrate in this paper that they have elected to adopt a path that is a combination of both of these options.

4. MECHANISMS OF COMPUTER FRAUD

[6] The Financial Times. 22 October 1984. London.

[7] Business Week. 1 August 1998. New York. p.51.

The chart above illustrates relative proportions of various types of abuse over the thirteen-



year period in which data was obtained by ACARB.

There are many ways in which the computer and information systems can be used to perpetrate or facilitate criminal activity. These fall into the following broad categories:

- theft of information, data, software or hardware
- theft of computer time
- disruption of services
- disseminating offensive material (pornography, racism, etc.)
- disseminating destructive programs (viruses, worms, etc.)
- information and software piracy
- money laundering
- distorting, tampering with, or amending data
- electronic vandalism
- industrial and political espionage
- communications for criminal activities

Some of these activities are most commonly perpetrated by unscrupulous individuals. These are frequently disgruntled employees, 'dare-devil' students, or persons presented with the opportunity by virtue of their routine daily access to information. Less frequently, *hackers* or computer enthusiasts with altruistic motives may feel challenged to take on and crack strict security procedures. Most frequently by far, however the motive is *greed*, and that is not the exclusive prerogative of antisocial elements. Corporations and governments suffer from the same syndrome, and as we shall demonstrate below, these have taken over many of the fraudulent activities devised by criminals.

1. Fraud perpetrated by employees

Computer crime by an employee with access privileges can take the form of theft of money (e.g. transferring funds to a secret account), intercepting credit card information, creating fictitious accounts, and a multitude of anecdotal (and entertaining) tricks and turns devised

by entrepreneurial criminals. It is not the purpose of this paper however, to conduct a detailed description of these, but rather to demonstrate how some of them have been adopted by the institutions as policy procedures.
The most notable of these, and probably the most lucrative is known as the "*salami*" attack. This involves shaving small amounts of money (like cutting a salami) usually when calculating interest in financial systems. If an amount is rounded off from a thousandth of a dollar to the nearest cent, and the balance transferred to a secret account, assuming a million transactions per day, this can amount to several million dollars annually. The crime goes largely undetected as account holders and bank customers rarely check their balance to the nearest cent, or care.

2. Fraud perpetrated by financial institutions

It is no secret, nor surprising, that amongst the first businesses to take their activities online have been the banks and financial institutions. The economic rationale of doing this is self-evident: improved profits by a reduced dependence on human resources (clerks, tellers, accountants, etc.) and reduced expenditure on physical installations (buildings, furnishings, etc.). However this has resulted in the increased vulnerability of account holders in relation to improprieties or unethical (not to say illegal) conduct by the institutions. A recent edition of The Australian[8] carried an article in its 'Computers' *pull-out* section which reported "horror tales" in Internet purchasing of financial products. Quoting Consumers International (CI), it stated: "*Customers suffer limited choice, poor or deceptive information about charges, unreliable delivery, overcharging, and difficulty in obtaining refunds.*" (Gengler, 1999).

This is likely to increase with financial institutions prioritising improved profit margins over ethical conduct. When they became aware of the "salami" attack fraud (described above), their response was a two-pronged attack: Firstly, tighter security, compartmentalisation of functions and upgrading of accounting software attempted to reduce the volume of theft; and secondly (and more importantly), by lobbying sympathetic governments, they were able in many cases to achieve the passing of legislation which allowed them to redefine their legal frameworks and to perform the "salami" operation *themselves*, and appropriate the proceeds *legally*! "A Big League is emerging" says Vuori, "who owns the banks?" Many incidents that have come to light reveal Mafia links to major banks, involved in massive money-laundering operations.

3. Fraud perpetrated and/or tolerated by government bodies

Evidence of government involvement in computer-related crime is sporadically publicised by the media, and has involved many of the governments of western 'democracies', such as France, Japan, Russia and the USA. Most recently during The NATO bombing of the former Yugoslavia, both the USA and the Serbian government used illegal Internet procedures during the cyber war that paralleled the military one. Many cases have been brought to light of governments conducting or supporting illegal acts of espionage and sabotage, with the use of technology (from Watergate to Nicaragua; yet perhaps the most

[8] Gengler, B. The Australian. 14 September 1999. p.44

effective involvement of governments in fraud is its endorsing, sanctioning or ratifying of regulations which permit banks and large financial institutions, (who, not surprisingly have broken all-time records in their profit margins) to perpetrate the "legal" fraud.

5. TRANSNATIONAL CORPORATE CRIMINALS: CASE STUDIES

1. Equity Funding

The case of Equity Funding is quoted at the start of this paper, from Robert Farr's *The Electronic Criminals*[9], and occurred in 1973, 26 years ago! The company computer-generated thousands of fake insurance policies which it resold to re-insurers for a total of over US$27 million. Ironically, writes Farr, they chose the hard way. If they had actually employed the computer as a tool they could have acquired millions of dollars' worth of negotiable securities without launching a big promotion. Today the number of similar, or worse, cases of top-end corporate fraud may have increased a hundredfold, with the staggering advances in hardware and software technologies since 1973.

2. Hertz Corp

In another blatant case of systematic fraud by a company, described by Tom Forester[10], Hertz Corp. overcharged customers who damaged rental cars and were liable for repair charges. Their computers were programmed to generate 2 estimates: one for the actual cost of repairs at discount rates, and one with the higher price which was sent to the customers and their insurers. Hertz eventually issued refunds of around US$ 3 million, but are estimated to have raised over US$ *13 million*. Laws have yet to be changed to prevent them from doing it again.

3. Encyclopaedia Britannica, Waterford Glass Company

In the same paper Tom Forester identifies at least 2 more cases: Encyclopaedia Brittanica's resale of it's 2 million client database to a direct mail company, and the Irish Waterford Glass Company, who's unique specifications for their cutting machines were stolen by corporate competitors and probably resold to bootleg Asian factories. Both these cases further demonstrate that corporate business is not always above breaking moral or ethical codes, or indeed the law, if it can be demonstrated to be cost-effective.

---

[9] Farr, R. (1975). The Electronic Criminals. USA: McGraw-Hill

[10] Forester, T. & Morrison, P. (1990). Computer crime: New Problem for the information society. Prometheus, Vol.8, (pp 257-272).

4. Saxon Industries

The business products division of Saxon Industries was able to deceive shareholders and potential investors over a 13 year period. It eventually filed for bankruptcy even though it had been continually reporting a profit for all that time. According to Dr Timo Vuori(1999)[11], at the time of filing for bankruptcy the inventory balances of $121 million was found to be overstated by $67 million. This computer-assisted fraud was perpetrated by using the computer to maintain and process fictitious inventory quantities and prices. This particular criminal technique is known as the Trojan Horse, and had already successfully been used by a number petty hackers.

5. Microsoft/NSA conspiracy

Only a few weeks ago Research Triangle Park, NC posted a release on the Internet[12] asserting that while investigating the security subsystems of WindowsNT4, Cryptonym's Chief Scientist Andrew Fernandes discovered a *back door* for the NSA in every copy of Win95/98/NT4 and Windows2000. "*Building on the work of Nicko van Someren (NCipher), and Adi Shamir (the 'S' in 'RSA')*," the release states "*Andrew was investigating Microsoft's "CryptoAPI" architecture for security flaws".* In effect, according to the release, in every copy of Windows sold, Microsoft may have installed a 'back door' for the National Security Agency (NSA - the USA's spy agency) making it "*orders of magnitude easier for the US government to access you computer*." As well as representing the worst fears we may have developed about the sinister "big brother" nature of modern society, this is perhaps the best illustration of the posit of this paper: Big business and the government conspiring in an illegal violation of the security of individual citizens.

6. INVESTIGATION, PREVENTION, AND CIVIL PROTECTION.

Computer security can never be fully guaranteed, but can be considerably improved by the adoption of certain procedures. Pitched against the combined might of Mega-Buck Transnational Corporations, unscrupulous governments and organised crime, the ordinary citizen's chances don't look too good! However some guidelines may form part of *hir*[13] Survival Kit :

- There is no substitute for diligence. Most *salami* attacks rely on your inattention to small decimals.
- Use smart passwords, and change them frequently if doing business online. Never share them with anyone but your cat.
- Extreme caution should be exercised if transmitting sensitive information (such as credit card numbers, etc.) over phone or data lines.
- Encryption is the right of all citizens, exercise it to the fullest extent of the law.

---

[11] Vuori, T. (1999, September). Computer Security, Lecture 2. Lecture presented to Computer

[12] Cryptonym Research. (1999). Microsoft, the NSA and You. [on-line]. Available at:

http://www.cryptonym.com/hottopics/msft-nsa.html

[13] Politically correct, gender non-specific form of him/her.

- Back up valuable data, and protect it using appropriate hardware and software technologies (e.g. Firewalls, Virus Shields, etc.).
- Protect access to information by compartmentalising functions on a "need to know" basis.

7. Conclusion

This report has investigated the incidence of computer-related and computer assisted fraud in the banking and financial industries using a wide range of online and offline resources including personal communications, lectures, and newspaper reports of particular cases. The result of analysing all the collected data leads to the conclusion, beyond reasonable doubt, that large banks and financiers have substantially improved their profits in recent years by abetting, condoning or even instigating some fraudulent communications and computer activities. In those cases when they have been the victims, we have shown that they have denied it. This has been possible because of the tacit support of governments' regulatory bodies, and is in conflict with the interests of ordinary consumers and the citizenry.

8. References

Bequai, A. (1987). Technocrimes: The Computerisation of Crime and Terrorism. Lexington,Ma.: Lexington.

Business Week. 1 August 1998. New York. p.51.

Cooper, J. (1984). Computer Security Technology. Toronto: Lexington Books.

Cryptonym Research. (1999). Microsoft, the NSA and You. [on-line]. Available at: http://www.cryptonym.com/hottopics/msft-nsa.html

Farr, R. (1975). The Electronic Criminals. USA: McGraw-Hill

Forester, T. & Morrison, P. (1990). Computer crime: New Problem for the information society. Prometheus, Vol.8, (pp 257-272).

Garfinkel, S. & Spafford, G. (1996) .Practical UNIX and Internet Security: Second Edition. USA: O'Reilly & Associates, Inc.

Gengler, B. (1999, September 14). Horror tales in Net survey. The Australian, p. 44.

Gengler, B. The Australian. 14 September 1999. Perth. p.44

Pfleeger, C. (1997). London: Security in Computing. Prentice-Hall International (UK) Ltd.

The Financial Times. 22 October 1984. London.

Vuori, T. (1999, September). Computer Security, Lecture 2. Lecture presented to Computer Security students, Edith Cowan University, Perth, WA.

Walker, K. (1998). Computer Security Policies. California: A Prentice Hall Title