PROXIMAL CONSULTING WHITE PAPER 4
DIGITAL & ELECTRONIC CRIME: AN OVERVIEW

"EVOLVE OR PERISH"
epigram on the "Hacked Net" Web site

"Although we have not experienced the electronic equivalent of a Pearl Harbor or Oklahoma City as some have foretold, the statistics and our cases demonstrate our (the US) dangerous vulnerabilities to cyber attacks" Michael Vatis, head of the FBI national infrastructure protection center (March 1998).

"There are a lot of ways you can rip off people. Computers make it easier" Jim Thomas, Professor of Sociology and Criminology at North Illinois University and Editor of Computer Underground Digest.

"Anyone can learn to break into a computer. The hard part is how to defend yourself" Carolyn Meinel, a hacker.

"If I want to steal money, a computer is a much better tool than a handgun. It would take a long time to steal $10 million with a handgun" Daniel Geer, security expert to a House subcommittee in 1997

"Computer crime in one form or another could well be part of virtually every investigation in the coming years" US Attorney Donald K Stern

You're not worried by computer crime, cyberspace, technology? Where have you been for the last twenty years....or the last second?

THE RIP OFF TOP TECHNOLOGY

Just because a fraudster uses technology it doesn't mean they're committing computer or cyber crime. The technology may be just a means to an end...but boy does it make the life of fraud easier. In random order here are my favourites:

- The mobile phone: where would we be without this? For the scam artist he or she can be anywhere in the world and, if required, give the believable impression of being anywhere else
- The colour printer: high quality copies of fraudulent documents on demand
- The scanner: very good for producing replicas of original documents but with new details or photographs seamlessly entered
- The humble PC: endless uses from the production of dummy company literature to uploading your hooky website promising "guaranteed returns" on to the Internet
- The fax machine: often taken for granted and forgotten. Who can tell the difference between a legitimate document and a clever forged one when all is received is a faxed copy

WHY COMPUTER CRIME?

Criminals have an annoying tendency to move rather quicker than those they are targeting. Over the past two or three decades the volumes of data, information and money which are being stored and transferred by electronic means have mushroomed beyond anyone's previous wildest imaginings:

- Whilst there is no truly accurate method of measuring the world's Internet population, current estimates (1998) put the total in excess of 112.75 million with 20 million in Europe, 14 million in Asia Pacific and 70 million in North America. It is now calculated that internet usage doubles every hundred days

- In excess of a hundred million messages travel across the world's networks on a daily basis
- 24% of US web users are on-line shoppers
- Computers effectively control transport networks (air, train, buses), hospitals, global weather services, National Security.....

Governments, military organizations, banks and virtually any business could not operate without information technology - hence the attraction for criminals: computers now contain most of both the money and information they want. In the wired age, where connectivity is all no one is safe from computer crime attack.

On top of the existing and developing technologies there is the Internet. More than anything ever before the worldwide web transcends the traditional restrictions of location and security. Geographic location becomes increasingly unimportant - it doesn't matter where you are or where your bank is. The flip side of this coin is that criminals can attack from anywhere across the globe and disappear just as easily. If it hasn't already done so, the Internet will transform the way we:

- Communicate
- Obtain information
- Use financial services
- Conduct business
- Govern countries, states and individuals

Thus the Internet will change the nature and operation of crime beyond recognition, if for no other reason than that's where the money is going to be:

- The global electronic commerce market through the Internet currently (early 1998) is estimated at around £500 million.
- But global revenues are predicted to rise to over £270 billion by 2002

High technology is an ideal forum for crime because:

- Computer crime can be anonymous
- Crime can be transacted at a great distance without any need to meet or confront the victim
- In fact computer crime is viewed as a "victimless" act - which it isn't of course...
- Crimes can be carried out quickly and almost invisibly without leaving traces
- The increasing level of global interconnectivity makes crimes easy to commit
- Vast amounts of technical knowledge are not necessarily required - all hardware and software providers see the creation and development of a user friendly environment as their prime aim - drag and drop, point and click, plug and play

THE COST, LEVEL & EXTENT OF COMPUTER FRAUD & CRIME

"Computer crime may be the subject of the biggest cover up since Watergate"
J Carroll "Computer Security"

"How big is cyber-crime" begins one web site on hacking: and then proceeds to answer (in part) its own question "Well, just to give you an idea: one thief stole twenty thousand credit card numbers. As the web continues to grow and we put more and more personal information on-line, the computer underworld is only getting more difficult to control."

More than any other strain of fraud and crime the "official" reported figures (and even unofficial estimates) are profoundly understated, primarily because many organizations do not want to admit that the integrity of their systems which may power all of their operations have either been compromised or completely blown away - alternatively they might not know that they are the victims of computer crime!

The 1993 UK Audit Commission report into computer abuse reported that there had been:

- An almost five fold increase in reported virus infections
- A 38% increase in the number of reported frauds

- 183% increase in the total value of reported incidents

But remember at the time of writing these statistics are four years out of date!

The most up to date statistics from the UK Audit Commission ("Ghost in the Machine" - February 1998) shows:

- Losses from fraud are up 25% from £28,000 per incident in 1994 to £35,000 per incident in 1998
- Over a quarter of frauds were committed by staff in management positions
- The percentage of organizations *reporting* hacking incidents has trebled
- Telephone systems are a new target for fraudsters

"While companies may think that they are spending the requisite amount on information security the dramatic increase in quantified dollar losses indicate otherwise. In addition to hardware and software organizations must ensure that training staffing levels are adequate and that end users are made aware of the seriousness of the situation"

- Patrice Rapalus, Director of Computer Security Institute, San Francisco

In March 1998 the San Francisco based Computer Security Institute published its "Computer Crime and Security Survey" which is authored with the participation of the FBI. The data is taken from 520 respondents and contained the following frightening conclusions:

- 64% of respondents reported security breaches in the previous 12 months
- 72% acknowledged suffering financial loss from such breaches - but only 46% were able to quantify such losses
- The most serious losses were due to unauthorized access by insiders (18 respondents reported total losses of $50,565,000 - which means an average loss of $2,809,166) telecommunications fraud (32 respondents with a total loss of $17,256,000: average loss $539,250) and financial fraud (29 respondents with a total loss of $11,239,000 - making an average of $387,552)
- The number of organizations reporting that their Internet connection as a frequent point of attack rose from 47% in 1997 to 54% in 1998
- 63% of respondents had no policy for preserving evidence for civil or criminal proceedings after a successful intrusion (a further 15% didn't know whether they had one!)
- Only 17% of intrusions were reported to Law Enforcement agencies
- 74% of unauthorized usage came from outside the organization but 70% originated inside the organization
- In the two year period 1997 - 1998 55 incidents of financial fraud generated losses of over $35 million

  In March 1998 the Jeddah Chapter of the Institute of Chartered Accountants of India cautioned banks about the growing number of frauds involving computers, which are estimated to cost the Saudi Banking sector £5 per employee per day
- In March 1998 the FBI told a hearing of Senators that it had recorded a significant increase in its pending cases of computer intrusions in 1998 from 206 to 480 - an increase of 133% and up 250% on two years previously
- The British National Computer Centre 1994 study into IT Security Breaches and failures reported a highest single loss uncovered in their survey as £1.2 million
- The Pentagon suffers more than 250,000 hacker attacks per year
- US telephone companies lose more than $1 billion to hackers annually (the average age of hackers generally is 13-14 years old)
- It has been estimated that Computer Crime in the US exceeds $8 billion each year: fraud exceeds $555 million - Banks are the biggest victims with losses to fraud estimated at $1 billion (these figures are continually updated - a 1997 report for the Democratic members of the House banking Committee puts the loss figure for thefts from US financial institutions by computer attacks at $2.4 billion)
- The US National Computer Crimes Squad estimates that between 85 - 97% of computer crimes are not even detected. Glennok Wahlert, Manger Corporate Planning of the Australian Federal Police commented in 1998 that 80% of companies who had suffered security breaches were not aware that it had happened

- Fewer than 10% of all computer crimes are reported (even this figure may be too high - the true figure of reported computer crime could be less than 5% of the total)
- The British National Computer Centre reported that more than 80% of organizations questioned had suffered a security breach in the previous two years
- As far back as 1993 four out of every five computer crimes investigated by the FBI involved unauthorized access to computers using the Internet
- Even further back in 1987 an American Bar association survey confirmed that 72 out of 300 corporations and government agencies polled had been the victim of a computer related crime in the preceding twelve months. Losses ranged from $145 million to $730 million
- In February 1998 police statistics confirmed that computer crime was costing South Africa more money than armed robberies and cash in transit heists (which are the more publicised events). Losses were estimated at R 326-million. Computer crime is perpetrated by organised crime syndicates, disgruntled employees, embezzlers and hackers. South Africa's computer criminals have an added advantage - there are no laws to prosecute them with that cover computer crime
- In May 1997 Carlos Felipe Salgado was arrested in San Francisco after trying to sell 100,000 credit card data sets to undercover FBI agents for approximately $200,000. The data had been hacked from Internet servers

So quite frankly the scale of the "dark figure" of unreported computer crime is anybody's guess..... However it is important to point out that although the perception of a "cybercrook" is some teenage boffin sitting in his bedroom illegally accessing computer sites to the point of boredom it is just as likely that the people committing these crimes are you own trusted staff.

November 2003 – Adapted from "Hacked, Attacked & Abused: Digital Crime Exposed" by Peter Lilley (Kogan Page, 2002)

Proximal Consulting

Email: enq@proximalconsulting.com

Telephone: +44 (0) 1672 516725

Offices:

Poughcombe Barns
Ogbourne St Andrew
Wiltshire
SN8 1SE
UK

Rue Du Rhone 14
1204-Genève
Switzerland

Proximal Consulting have unrivalled experience in providing KYC enhanced due diligence background reports on individuals and companies on a global basis. We also offer a complementary range of services including AML training, country risk reports and bespoke investigations.

Our enhanced due diligence reports are tailor-made to our clients' specifications. They are totally different from the usual database-led reports that often fail to meet enhanced due diligence requirements. Our reports present clear, accurate and confidential findings which enable our clients to make informed business decisions and to fulfil their AML obligations.

We work with a variety of global clients including regulatory agencies, law firms, individual companies, private banks, trust companies and other firms in the financial sector.
