COMPUTERS & LAW

JOURNAL FOR THE AUSTRALIAN AND NEW ZEALAND SOCIETIES FOR COMPUTERS AND THE LAW

Print Post - PP233867/00008

Editors: Elizabeth Broderick, Daniel Hunter
Number 25

ISSN 08117225
July 1994

Computer Crime - Does It Exist?

by Les Lawrence

Preamble

There are many who would argue that computer crime does NOT exist. There is only ordinary crime connected with computers. There is a lot to be said for this argument. Theft, fraud, forgery, blackmail and so on are no more and no less criminal because they use data or programs stored in a computer. So why talk of computer crime? What's so special? Do we really need special acts or amendments to Crimes Acts?

At the risk of sounding platitudinous, the answer to these questions lies in the basic ethical problem of crime. Expressed, in a somewhat oversimplified manner, a crime occurs when someone takes an action which harms another person physically, economically or socially to provide a perceived benefit to the criminal. There is no question of whether the benefit would be seen as such to the 'reasonable man' - it is sufficient to show that the criminal was motivated by his or her perception of some tangible or intangible benefit.

So much for philosophy. It needs to be turned into practical guidelines if it is to be useful. Two routes have occurred. One is Common Law which basically results from the accumulated decisions of judges, who are or were knowledgeable in the area of their decisions; who could relate theft and assault, for example, to themselves as potential victims of the actions concerned. The other route is statutory law which defines what actions are not permitted (in some jurisdictions 'what is permitted') and prescribes penalties for illegal actions.

Overlaying these is a body of legal practice, sometimes codified such as various Evidence Acts, which spell out how it can be determined that an action has occurred, who committed it, and how to adduce the motive behind it. Other factors may also come into play such as where

CONTINUED ON PAGE 3

In this issue ...

Computer Crime

☞ CONTINUED FROM PAGE 1

and when the event occurred, and whether the person was tricked or forced into performing it.

These points of basic philosophy have been raised to establish a base set of definitions that will be used in the rest of this article to review the types of events that can occur in and around computer systems. The key questions which need to be asked are whether the action is criminal, is there a benefit, and how do we prove it. It is the author's view that most of the attempts so far to tackle the issue by legislation or by assuming it can be covered by existing laws will fail, simply because they do not consider these basic questions.

Criminals using computers

Just as normal business needs to keep records, so organised crime may use computers and computer networks to manage and administer their activities. Does this make their crimes computer crimes?

Using the basic principles we would answer in the negative, since the activities involved in computer terms are identical with those of non-criminals and are perfectly legal in themselves. They are processes of data entry, data processing and report preparation. They are no more criminal than the activities of the Australian Institute of Criminology keeping records of crime on its computers.

There is an interesting issue, however, in relation to the question (discussed later) of surreptitious access to systems and data by rival criminals or law enforcement agencies. The law may, in fact, need to protect the criminals from the criminal activities of others! But this situation has also led to attempts in the USA to curtail the use of cryptography as a protection of information from disclosure. The so called CLIPPER algorithm, which has been approved for general use, has a master key which must be registered with the government, so that law enforcement agencies may break into the systems run by criminals (and by anyone else).

This approach has difficulties because it prevents the law abiding computer user from obtaining adequate security and introduces a weak link, which can allow attack by trial and error to find the master key or by theft of the records of the master keys. At the same time it does not really prevent the determined user from developing or coding better algorithms for themselves.

"The key questions which need to be asked are whether the action is criminal, is there a benefit, and how do we prove it"

I hope no-one will be in favour of legislating to make illegal the development of cryptographic algorithms, or the use of algorithms not approved by government. If such a pattern was established the author can envisage lobbying for similar legislation in relation to other processes aimed at gaining a competitive advantage or monopoly position for the developer or owner of that process!

Computer victims or objects

A second class of activities relating to criminals and computers is where the computer, its components or networks, or even key people are used as the object of an action with the intent of causing harm to others for the benefit of the instigator.

Examples are:

- bombs or fire used to prevent the computer owner from using computer and causing the owner financial or political damage.
- an invasion of a building or riots preventing use of computers.
- physical theft of computers or components.
- physical damage to computer communications links.
- demanding cash or other benefits to enable continued operation.
- physically removing key individuals.

Most of these are crimes of theft, malicious damage, extortion, kidnapping and others quite easily dealt with under 'traditional' law. The physical entities involved lead to relatively easy proof of participation and intent. However, there are two problem areas. One is the question of the extent of damage caused which may well exceed the value of the physical objects, and is basically an intangible item. The only intangible covered in the existing crimes acts, without amendments for computer crime, is the theft of electricity! The second, which shows up in extortion demands is that of when the crime was committed and how can it be detected and proven.

In one case, a disgruntled employee changed a VSAM master password of a system, and without the password the operator could not start the sys-

tem. A considerable sum of money was demanded to provide the new password. Did the crime occur when the demand was made or when the original change was made? On the other hand, was the organisation guilty of criminal or contributory negligence in not having a backup which would allow restoration to the earlier status? (The latter would not have helped as the person concerned was allowed too broad an access to facilities and could easily have removed the backup tapes.)

From a computing viewpoint the crime occurs when the unauthorised change was made. Traditional law might be used by establishing that the process was to be treated as equivalent to creating a forged instrument. However, the proof question makes this a doubtful proposition and a 'computer crime' needs definition to cover the change to an intangible item and establish how the change might be proven.

In another case, an employee stole legitimately made back up tapes. There is no problem in recognising the theft after the event, but there could be some organisational contribution in allowing a person to remove tapes. This employee however had previously ensured that earlier generations of back up which were sent off-site for storage were actually blank tapes, so that the copy he held was the only useful backup. By causing a system error which could only be resolved by restoring from the back up, he was in a position to demand millions of dollars to provide the tapes he had. What crime or crimes were committed and when? Traditional law can cope with the theft of the tapes and the extortion demand, but there are further problems.

- What is criminal about replacing back up tapes with blanks? This is essentially an unauthorised modification, but what record would exist of its occurrence - physical and magnetic tape labels can easily be changed with no external evidence of its occurrence. The criminal in question might not be the one sending the tapes out, just the person who changed the labels. How would we know who did what?
- What about causing the system failure? Many operators can do that easily by accident. In any case, how would we know who did it? Only the latest version of RACF for IBM mainframes allows for operator identification and there are loopholes in its use in practice.

It is tempting to make unauthorised modification a computer crime as has been done in several computer crimes acts. However, unless requirements for unique user identification and immutable audit trails are also included it is all too easy to maintain that the person was an innocent victim of circumstances such as in the case against Dion Barylek in Victoria. Regardless of the real truth, the successful appeal in that case does highlight that the problems of proof of activities and of intent are extremely difficult when it comes to computer systems, particularly when it is only the intent which may separate a legal, but careless or untrained, activity from a criminal one. Few judges would have training in computers sufficient to appreciate the subtleties.

Computers as a tool

The crimes we classify under this heading are basically traditional crimes that are enhanced by the use of computers or because the victim uses computers, or are of such a nature that the criminal cannot cost-justify the crime without using the computer.

The Equity Funding case relied on using the computer to generate records of non-existent policies and on the willingness of the victims (reinsurers) to believe that what comes out of a computer is correct. Part confidence trick and part fraud, it is covered by traditional law, but how can it be proven or prevented? The system itself was not fraudulent but its usage was. Another case of misuse was the transfer of funds from

IN OUR NEXT ISSUE...

Our next issue looks at

EDI AND GOVERNMENT CONTRACTING

✎ Please send all contributions to the Editors no later than 21 October, 1994.

the SBC via New York to the State Bank of NSW. The programs used were the normal ones - it was only that the usage by staff of the Bank was not in accordance with approved transactions.

In another case, reported to the author and hence purely hearsay, special programs were written to deal with payroll. A standard program was used by the DP section to create the information given to employees, but the deductions disbursement program was only run by the CEO's secretary using a special program kept in the CEO's safe. This program took the deductions as given by the normal program and disbursed to a number of locations that had nothing to do with the authorised purpose of the deductions. Superannuation deductions were diverted into other criminal activities via a chain of companies.

Other cases of programs written for fraudulent or other criminal purposes exist. Cases relying on computer processing have also included the so-called salami technique where very small amounts are skimmed off very many accounts and the results credited to the criminals who then go through normal procedures to remove the funds. A case in Texas relating to payroll programs is supposed to have netted the programmers hundred of thousands of dollars over an extended time before it was discovered.

Other programs have been written with criminal intent, but fall more into the next category of activity. These are programs intended to run in place of the correct program and perform a bit extra to the approved activities. The extra may be recording user identities and passwords, or it might be a direct crime in the class we are considering in this section where the transaction entered is diverted to an incorrect account (as in one case, for only three days before being handled correctly), or creates special files of 'interesting' events.

There is nothing the law can do about fraudulent programs written by the criminal and used by the criminal on his own computer. US Wire Fraud laws try to address the problem when the process uses communications links to transmit a fraudulent transaction, but this is really only enabling legislation to use after the event to declare illegal a specific event of a type that is otherwise perfectly legal. Australian Computer Crimes Acts have also tried to address this problem of communications being used as the vehicle for some aspect of the crime. The problem becomes one of proving who was responsible and where and when the event occurred.

"There is nothing the law can do about fraudulent programs written by the criminal and used by the criminal on his own computer"

Legal nightmares abound in cross-jurisdictional definitions of crime and standards of proof, let alone in who can bring the action.

The computer jemmy - enabling actions

Another form of computer crime occurs when the victim uses the computer to gain access to data which the criminal then uses for some other form of crime. The subsequent crime may include those in the previously defined 'computers as a tool' class or a more readily recognised traditional crime.

The basis activities are stealing user access passwords (if they exist) of bypassing security mechanisms, but these might be only a first stage of a process that then followed up with, say, gaining personal information to be used for blackmail.

Stealing a user's password is like a burglar breaking into a hardware store to get the tools for a 'break and enter' job. Or it can be considered like the break-ins that have occurred in video shops to take customer lists so that the burglar knows where to find what equipment that might be worth stealing. When and how the theft occurs is varied and this variation and subtleties need to be appreciated by judges and by legislators. It can be:

- by simple observation as the author has used in testing physical security, or as has been reported in ATM related thefts.
- by wire tapping on computer links to see users' identification and password as then pass to the mainframe or even LAN server.
- by reviewing changes in unprotected or generally available areas of operating systems such as input buffers.
- by using system peculiarities that allow the user to bypass the controls in special circumstances and either substitute his own password for an existing one, or read the passwords directly from where they are stored. There may be some indirection in the latter as when cracking UNIX security by using one's own copy to generate a dictionary of encrypted passwords and comparing that with the file from the attacked system.

Bypassing security mechanisms is also a way of gaining access to computer systems to enable further criminal activity. Again a variety of mechanisms exist, including:

- Stealing the backup tapes which contain copies of the useful information. This is more difficult in mainframe areas using secure storage services and is usually restricted to the operational staff who probably have limited knowledge of what is valuable. It is a different story for LAN operation in the midst of people who know what data is available and where, very often, any back up tapes are left lying on top of the system or on the administrator's desk. Stealing the tapes would be a normal crime, but how would one prove it had occurred? How much more difficult would it be if the tapes only disappeared for a few hours, say overnight, to be copied and were then replaced? Probably only the results, and known availability could be considered circumstantially to deduce what had happened.
- Software vendor access points. AS/400 has about 16 special users hard coded into the system. VAX/VMS has several such users. These are often documented clearly in the system documentation but left by the installation at the default values and hence are useable by anyone who cares to read. They can be used sometimes for direct access to data or to discover passwords of special users. A special case of this type of access is that provided by performance monitors, network maintenance monitors and the like support tools. These have often been designed without concern for access to information and usually display a lot more than is really needed for the job.
- Trapdoors in software, which are points left by developers after being inserted by them to bypass security during the debugging of the program (or possibly deliberately inserted for their later benefit). There are also some which rely on the basics of the operating environment and the expectation that it will be under continual development. The author has been involved in reviewing systems in which an error condition immediately places the user into a maximum privilege mode with systems commands available to look at anything. UNIX systems have been notorious for this type of problem and are particularly susceptible to it since the 'ROOT' user owns everything, can see everything, can switch to any other user's identify, must be active in every operating environment, and must be the exact same identity in all (ROOT is the user identity) systems.

"There is clearly a case for legislative definition to bring some of these computer related activities into traditional law"

In these cases the initial action is an enabling one which probably should be treated as criminal in itself to allow the public a means to prevent further action which will be criminal and perhaps might be dealt with by traditional law. To deal with these activities, specific computer crimes need to be defined to cover unauthorised access to information and unauthorised changes to information stored whether those changes were made by a person authorised to access it or not. This much is in several of the Computer Crimes Acts. However, the law needs to define how to prove that such access occurred and by whom, bearing in mind the fact that the criminal or an accomplice could be in a position to delete any magnetic recording of the event. Computer systems can be set up to provide this information and could be required to record in on WORM drives or other unchangeable (but not undestroyable) media, but they would usually be unable to detect an invalid change made by a properly authorised person and would therefore have to record every action. Since this latter situation is economically infeasible for all people in an organisation it is necessary that information that is to be protected from criminal change must only be accessible for change by a very limited set of people and their actions recorded immutably.

Conclusions

Although this article has classified so-called computer crimes, it should be apparent that these classes need to have key elements addressed. Firstly is the action criminal, can it be treated by traditional law or is covered by the current computer crimes legislation in the various states and federally. The common element is providing the means of identifying what action occurred, who performed it and whether there was intent. To a lesser extent, defining the benefit that is gained (or conversely the damage sustained) also needs consideration.

There is clearly a case for legislative definition to bring some of these computer related activities into traditional law, and for additional com-

puter crime legislation to deal with the intangibles and subtleties of computer operation. The classification approach should show that it is not sensible to lump all of the activities into one and hope to solve 'the problem'. Existing attempts do go part way to defining what is computer crime, but overlook some events which are normally legal but undertaken with criminal intent.

However, the computer crime legislation will prove useless unless it addresses the questions of proof and also places an onus on the computer 'owner' to implement protective measures. It should provide relief only if such controls are (and then only to the extent that they are) implemented. It does not seem reasonable for society, through the law, to protect an individual from becoming a victim of theft when that individual leaves the door open, places out the welcome mat and advises the 'burglar' to use everything as his own. ✍

Les Lawrence has worked in data processing for 30 years and specialises in information security and EDP audit. He is also a founding member of the NSW Society for Computers & the Law.