Counter-intrusion Strategies for I.T. Networks in the Building Industry

M J OSTWALD and S E CHEN*

ABSTRACT

During the development of a building project all decisions are reliant on information, its transfer and interpretation. As IT networks are crucial to the efficient management of the building process, the security of these links is critical to the assurance of quality and success in a project.

This paper considers counter-intrusion strategies for maximising security during the design, development and implementation stages of a building project. Through an analysis of documented intrusion strategies this paper considers IT concerns for data-theft in an industry wherein the potential for criminal intrusion is increasing every year.

Key Words

construction management; information technology; computer crime; project management; networks

INTRODUCTION

The building industry is one of the worlds most information intensive industries. The design, documentation and delivery of a building requires the application of a wide range of knowledge and information resources. Leslie (1992) makes the claim that; 'To assure the quality and value of its product and accountability of its decision makers, the industry must come to terms with this mass of information, and the problems associated with the communication and coordination of project decisions.' One such problem is security.

As an important aspect of global and national economic concerns the building and construction industry will increasingly become the object of computer intrusion. In any industry breaking the integrity of IT systems can be potentially disastrous, and the Building industry reliance on IT will place it in an area of high risk. Although in the near future there are large scale industry-wide problems of computer intrusion which must be overcome, the problems at the project level are already potentially serious.

The growing trend towards inter-organisational information systems has been noted by Cash and Konsynski (1985) and Betts (1992) has considered the strategic importance of such a move. This move also has great implications for

* *Faculty of Architecture, University of Newcastle, 2308 Australia.*

the security of project teams in the construction sector. Within a large project team there are many forms of information interchange, and this exchange is often undertaken between different professional firms. The network connections which join the engineers, architects, project mangers, and quantity surveyors, all would pass important information daily during the documentation of a large building. All of this information is potentially critical to the achievement of the project on time and on budget. Many conflicting interests are reconciled within the project team and the possibility of outside competition must be considered. For all of these reasons the consideration of security in the IT project network is important.

The prevalence of IT related crime is currently under scrutiny by researchers around the world (Chesterman and Lipman, 1988). However the exact extent of data theft and damage is unknown and estimates vary widely. Ball (1985) and Sieber (1986) both consider that the real value of money lost in data theft will never be known. They also however agree that the expression 'Computer crime' is often very inaccurate. Most data crimes combine traditional theft, masquerade, *etc*, as well as devices which intercept all forms of communications networks. The preoccupation with computer related security is a danger because it negates the understanding that computer intrusion normally occurs as a result of a more traditional, physical intrusion.

IT related crime is potentially the most costly form of crime in any industry today. This claim is well supported with the realisation that all industries, and the building industry in particular, are becoming dependent on IT. Ball (1985) quotes a University of Minnesota study which indicates that the average company when restricted from using company computers cannot function for more than 4.8 days. When engaged in fast-tracking a large building project, the loss of IT availability for half a day could be disastrous. Many project sites are totally dependent on phones and faxes, and all records, and in a few cases drawing files, are computerised. The potential for IT intrusion and misuse is increasing in the building industry, and in particular at the high risk communication system dependent stage level of the project development and implementation team.

This paper considers the ways in which computer crimes are perpetrated and general strategic counter-measures. The frame of reference of this report is the building industry and specifically the information network which exists within the project, inception development, documentation and monitoring stages. This paper draws primarily from case studies of IT crime from the United States of America, Europe, and Australia.

Information Theft?

Information is by definition, a commodity which is of value to somebody, although the value is not always clear or definite. The value of the information is dependent on the way in which the data is used, and the most valuable data is often sorted through standard items of IT. Data is communicated through word processors, on computer discs, and passed through all forms of telecommunications networks. When large amounts of money depend on the accurate, timely and secure transfer of information there must be a concern for the security of this data. Walraven (1992) notes that within a building project team; 'The Network concept puts an extra burden on the tools for archival/retrieval and data security.' This recognition leads to Walraven's ascertain that; 'Powerful data management tools are required to control user interaction and maintain data integrity.' As noted by Barton (1985), management of the construction process is an information intensive process. Many groups and interests come together to make decisions based around information transferred to them by way of non-sentient devices. Within a multi-disciplinary project team the efficient transfer in information is critical to the eventual assurance of quality on a project.

The neologisms Counter-intrusion and Information Technology combined imply the importance of strategies to reduce the impact of crimes relating to telecommunications, and computing technologies.

Throughout this paper computer criminals and the activity called 'hacking' will be discussed regularly. This paper will use an arguably erroneous assumption that a 'Hacker' is a computer criminal. The general activities of the hacker will, within this paper, be seen as aspects of computer intrusion and thus to some degree computer crime even if only in terms of invasion of privacy (Ross, 1991). The most widely accepted definition of what a hacker is, comes from Levy, who describes the hacker as a person whose aim is to make access to information, by way of the computer, as free and easy as possible (Levy, 1984). Telecommunication thieves ('Phreaks') are more easy to define as undertaking criminal activities as their motives invariably include the control of data (communication time) to engage in personal gain.

Within this paper the descriptions 'hacker', 'computer intruder,' 'data theft', etc, will be considered to be criminal activities, although this is a debateable point of view (Barlow, 1990).

Strategies for Intrusion

The methods of intrusion used by IT criminals may be split into two broad categories;

(a) Human engineering

(b) Virtual engineering.

The first is reliant on physical, real world interaction between people. In the 'Hacker' parlance these activities are known as 'Human engineering', a parody on aspects of the management theory. Human engineering feats usually involve physically stealing data, codes, or material with the intent of hacking, or 'conning' personnel. The usual purpose for such physical activities is to enable the computer intrusion. Almost all human engineering strategies are ploys to gain access privileges within the IT virtual network. Once within the network strategies change and the most common activities are; data theft ; data alteration (sabotage); systems control; and time theft.

The second component of computer crime is the actual contact by way of computer, phone, network, matrix or other virtual link. Virtual engineering techniques operate across networks, both phone and computer systems and their characteristic inter-connectivity provides potential breaks in security for criminal activities.

Within each of these two categories there are a number of separate activities which are common to IT related crimes. The following sections will analyse these in detail as well as discussing simple countermeasures and their direct application to the building and construction industry.

Human Engineering

Human Engineering aims usually involve acquiring access to virtual networks. Their goal is to appropriate either passwords, access codes, log-on codes, or phone numbers.

Physical Theft. Access Code Numbers and Trashing

At the most primitive level one of the first activities of the computer criminal is to cover their trail. The main forms of electronic trails left are through the phone network, specifically related to billing for calls. As most computer intrusions occur through the external network connections it is common for Hackers to attempt to acquire phone codes or access numbers.

Trashing is the action of sorting through a companies rubbish, and shredded documents in the hope that something valuable has been thrown out. Typical information which is valuable may include old faxes, each of which have built into the header the calling and receiving phone numbers. Also print-outs of changing computer access codes, lists of mobile numbers, and old credit card invoices, each of these provides a way to break through the barriers of privacy. Shredding does work to a degree but it is possible for a shredder to destroy a page but leave thin sections of text readable. Computer disks that have been thrown out are also potential sources of information. Sophisticated software programs may un-erase disks, and read multiple layers of files which have been supposedly erased. Such files often include information such as user number, time of access and date hidden in their data. All of this information may be the key to accessing the company computer without permission at some future date.

Phones and Faxes

Mobile phones are perhaps the weakest link in business information technology networks. For a nominal fee and with a limited technical experience a scanner may be acquired which may intercept calls made over cellular networks. Of particular relevance is the case of the construction site which might have many cellular phones in use by the project management team as well as sub-contractors, building inspectors and others. A considerable amount of important and potentially costly data is passed across mobile phone links, all of which is highly accessible to anyone with an interest in acquiring it. Mobile phones may not only be recorded but in some sections of the world may be intercepted and re-routed.

Until recently the fax machine was one of the safest instruments of data exchange in industry. However with the advent of fax/modems the fax is equally vulnerable to theft and compromise. A separate fax line will no longer protect documents, however a few fax/modems attempt to confirm the accepting number. This is not wholly foolproof as the phone network is equally accessible as the office network, but such strategies will reduce non-professional, or accidental interception of the data.

Deception

Once information has been gathered concerning personnel within a company, and the management structure, and regular business partners, often through trashing and scanning, then the next stage of intrusion is deception. The intruder, armed with the right information is often able to simply call the switchboard of the business, and while masquerading as an associate of the firm is able to gain access to project documents and even the internal network. This activity commonly called 'fast talking' can be overcome though educating the project members regarding consultant firms, product representatives, and liaisons with authorities and regulatory bodies.

Virtual Engineering

Virtual engineering techniques often follow as a consequence of the more traditional 'human engineering' activities. Once either access codes, or phone numbers have been gained, and the office staff have been deceived into allowing temporary access to the company files them the real intrusion will commence.

Accessing the System

Access codes allow external terminals to interface with a central data storage/retrieval unit. The access should be limited and these days often is, but mostly the protection is limited to a form of password. Accessing a mainframe from an outside terminal was fairly easily accomplished in the mid

1980s as simple software programs could break into them by randomly attempting to enter the password. Such software programs could attempt to input as many as one thousand passwords a minute in an attempt to randomly choose the right access code. The software could be run for hours or even days looking for passwords, and when they were found it would record these and keep searching for more. As the intrusion software was usually connected via a phone line, and being re-routed through some public company charged to another company such devices could run for very long periods without incurring any cost to the hacker, and with no likelihood of being traced. Criminals with an understanding of the phone network could even re-route tracer calls so that their location was never known.

Network Infiltration

When the 'Chaos Computer club' in Berlin worked with the KGB to steal American military data the vehicle for intrusion was a connection between the Berkeley on-campus system with ARPANET and then throughout INTERNET (Stoll, 1990). In particular INTERNET was connect to MILNET, the military data NET. Although MILNET was not classified it did contain potentially damaging data. There were two weak points that allowed the Chaos Chess club to infiltrate the MILNET. The first was a propensity of users of small, public systems to use obvious passwords. The German IT criminals used a strategy whereby they would first scan a Bulletin Board Service (BBS) for the names of its users, and then randomly reinsert these peoples first names, last names, and initials. This technique was invariably successful on small university and company networks. Once connected to a user account they used the time and space allocation to set up their own account and act as a remote System operator.

The weakness of networks is that they are like a chain or literally a 'NET'. Every point in the chain is connected to other points. A bulletin board in Hamburg, CERN, provided a link between academics in Berkeley and those in Germany. Berkeley was linked to INTERNET and ARPANET, and from there to MILNET. Although MILNET was not classified it was well security protected but available to the right user from Berkeley, with the right protocols and passwords. The weakest link was in Germany but it provided the key to enter almost anywhere.

In the history of computer crime this one factor is a regularly recurring element of incursion. Networks are designed to links with other networks. In order to carry out their working functions efficiently there is a need for outside links. If the computer network was totally isolated then the danger of intrusion is dramatically limited. Those few corporations which have isolated internal NETs and have experienced computer crime have generally occurred through staff infiltration, or an inside agent. Once within the virtual boundaries of a system it is a relatively easy action to gain control of the system (Quarterman, 1990).

During the project development process a number of firms might be involved in a complex interplay of data transfer. Each of these firms may also be connected to a BBS, research NET, and other business associates. The number of security weak-points grows geometrically with the number of connections. When data is transferred daily to many linked networks there is a need to understand the extent of the network connections. The most simple solution is to have each firm that is involved in a project monitor their own connections and severely limit them. Also there is the possibility of having a project system operator. When a project reaches a certain complexity and scale, for example a high rise building under fast track construction, critical information is processed every hour. Too often the management structure is based around the professional roles of engineer, project manger, and architect, with the computer links between these groups left unwatched. In a large project there is a need for a system operator who monitors data transference from one group to another. Such a person may never directly interact with every team member but rather their charter is to ensure that information is passed quickly, efficiently and securely. A vigilant and well trained system operator is capable of monitoring all that occurs through computers, faxes, word processing, and even incoming and outgoing calls. It is highly unlikely though that they would discover any impropriety if it occurred instantly, because the process of data monitoring usually revolves around patterns. A system operator should be capable of seeing breaks in a pattern of data flow and these may often lead to discovery of a security breach (Hafner and Markoff, 1991).

Electronic Voice Mail Access

Some of the most basic items used in the building industry are prone to tampering and misuse. Electronic voice mail is often accessed through the telephone keypad. Usually a section of data storage has been left accessible for recording phone messages. Almost any illegal access to a phone and computer network in a large business also allows access to the voice mail facility. Such an intruder could quite easily replay all of the voice mail sifting through it for valuable pieces of data. In particular hackers have been known to take detailed notes regarding company hierarchy and personal friends through these actions. This allows the hacker to call during normal office hours and by using the right names, terms, and even personal details to eventually convince people to accept the caller as a legitimate business partner. The eventual outcome of this exercise is to be given, quite openly, legitimate access to computer networks, even personnel access codes and access privileges. All electronic voice mail is subject to outside perusal, and should be used sparingly. Simple messages regarding the quantity of finishes, or selling rates for property, may be easily intercepted if left on voice mail and this knowledge is used by outsiders for profit.

Destruction of Data

The computer virus is a well known software device which seeks to alter, or destroy data. Analogous situations to data destruction have been known to effect digital fax transmissions and other forms of information technology but most are not as potentially dangerous as the computer virus. The implication of the term virus is something that multiplies and consumes. Most virus programs do one or other action, fewer are involved in both. On November 2 1988 Morris released a software program into INTERNET which crashed more than six thousand INTERNET computers (Spafford, 1989). Similar 'logic bombs' and virus programs have been used as weapons of retaliation and sabotage in well known cases. The fear of such retaliations kept AT&T from prosecuting computer criminals for many years. Operation Sundevil, the USA's nationwide crackdown on computer crime, was once beset with hackers breaking into police computers and cancelling search warrants and all points bulletins concerning their own criminal activities. Virus programs were left to destroy records and leave false leads (Sterling, 1992). The fact that the police promptly stopped looking for the Hackers after the warrants and APBs were cancelled says something about the power and perceived defacto authority of IT.

Bugs within major business operating system may provide loopholes for both internal theft, or sabotage, as well as weak-spots for infiltration. Several major computer operating systems possess software bugs. As the source codes for such software are often available to those with an understanding of computer programming, IT criminals are often able to hide small programs within operating systems to monitor and record access codes, data transfer, and phone numbers. This information might then be down loaded once a week to the clandestine controller which greatly reduces the possibility of being caught. An experienced system operator could, if vigilant for such an intrusion strategy, closely monitor memory usage and note small variations. However the chance of such an intruder being found are very small. Once within the system software and having achieved access privileges the only way to shut out such a person is to dismantle the entire system. It is better to keep the IT criminal outside the system as once within the network they are hard to remove.

IT Time

One contentious area of data theft relates not to the alteration or acquisition of data, but rather to the effect of stealing time on data NETs.

Computer time and telecommunications time is not just a factor of the relative usefulness of an item during the working hours of the day. The cost of some networks means that they must be operated for long hours each day and night to gain maximum benefit from the memory capacity. In large architectural and engineering practices the computers often undertake lengthy plotting exercises during the night hours. However during this period a certain amount of unused potential exists in the IT network. It has been known for computer crimes to be based around the theft of computing potential from one company, being used as a weapon against another. Not only is there a danger of what the computer time is being used to do, but also computer time is expensive and the cost of connecting NETs across the world may run into thousands of dollars.

A Hypothetical Intrusion

In order to consider counter-intrusion strategies a typical project team may be assembled and then a hypothetical strategy for infiltrating this network is proposed. Figure 1 shows a simplified algorithm for infiltrating a network team. The first step is to determine the associates, or consultants employed within a project team. One of the secondary consultants might then be approached, usually over the phone with the intent of finding out if the company was attached to any other network. This scheme might take the form of a questionnaire asking about the companies network connections, blatantly seeking to find out if the company uses any security systems, and how many hours a day are they connected. Once the greater ring of networks has been established then the intruder would approach the distant connections and attempt to gain access to these networks. Such large, public networks are notoriously less secure than private company NETs. Typical distant networks could be suppliers catalogues, specifiers indexes, on-line standards associations and authorities. A few of these distance networks may be accessed by paying a small legitimate fee, others would usually be engineered to gain access to the network.

Once within the network software scanning may allow access codes or passwords to be broken and a link to the consultant NET established. From within the consultant network the entire project team is now vulnerable and the intrusion is complete. Figure 2 shows diagrammatically the Virtual and Human aspects of the intrusion.

Counter strategies to overcome the problems of intrusion and to avoid the typical profile of intrusion presented above are;

(a) Research the extent and form of consultant links to outside networks.

(b) Examine consultant security strategies and determine weak points.

(c) Monitor suppliers and outside networks and note any unusual activities.

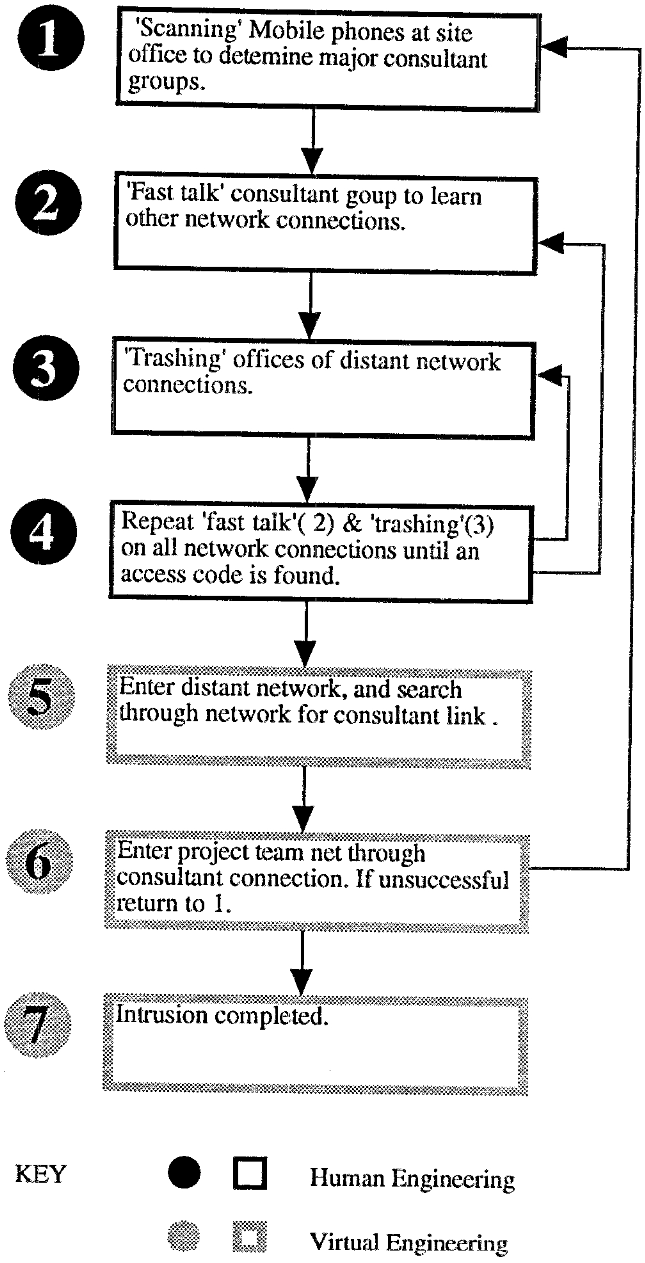
1
'Scanning' Mobile phones at site office to detemine major consultant groups.
2
'Fast talk' consultant goup to learn other network connections.
3
'Trashing' offices of distant network connections.
4
Repeat 'fast talk'(2) & 'trashing'(3) on all network connections until an access code is found.
5
Enter distant network, and search through network for consultant link .
6
Enter project team net through consultant connection. If unsuccessful return to 1.
7
Intrusion completed.
KEY
Human Engineering
Virtual Engineering

Figure 1. Intrusion Algorithm

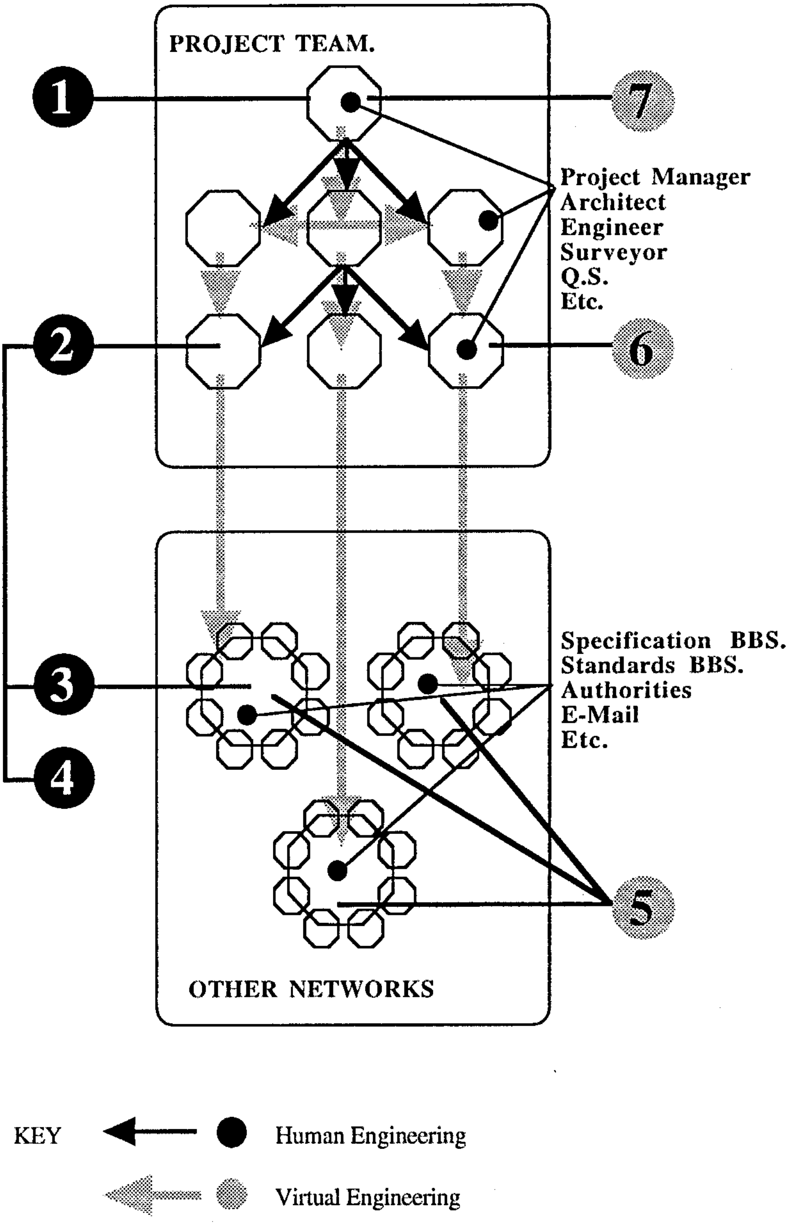

Figure 2. Intrusion Diagram

(d) Change passwords weekly, and destroy the lists.
(e) Clean-out the network weekly, and reanalyse external network functions.
(f) Consider security hierarchies, such that the Project management team may only receive data electronically from consultants, but must deliver data physically in reply.

These strategies are only effective in combination and there are weaknesses in the totality as well, but the combined use of these ideas may reduce the impact of Data theft. The following section looks at a few of these strategies in detail.

Strategies to Promote IT Security in the Building Industry

In the early seventies and eighties computer security in the construction industry was largely nonexistent and this situation has not greatly changed. At this time most computer intrusion was based around virtual engineering, the systems in themselves were so simple to access that physical constraints were not real barriers. As the problems of security become more widely known throughout the 80s, and as the spread of virus programs continued, an increased awareness of computer crime in business was recognised, although an understanding of the methods of intrusion were less well known. As recognised above IT intrusion techniques almost always rely on conventional, although not very complex, criminal techniques.

The majority of the intrusion strategies recorded in this paper possess potential hardware, or software solutions, although these are often short term barriers which provide only the semblance of security. More lasting solutions to increase IT security at the project level must rely on 'human' solutions, as no machine solution will be perfectly foolproof without the user becoming aware of the need for security. In the words of Ball (1985) : "It's time to recognise that computer security is a management problem, and that only coordinated effort will make computer crime more difficult."

Just as Quality Assurance schemes promote checking procedures and clarity of communication systems, they could also provide the catalyst for security. Raising management understanding of the issue and training of workers in simple procedures will reduce the number of ways in which security may be breached.

When setting up a multi-disciplinary project team care should be taken with the structure and maintenance of the IT network. There must be an understanding of the way in which systems operate, other connections outside the site and how associated firms connect with the project office. All passwords and access codes should be renewed upon forming a new working team, all outside modem and fax connections should be reviewed, and a manual of data transference protocols produced and used. By monitoring log-on times, the flow of data and the people who regularly access data, patterns of communication will appear. Any variation in these patterns will often not be obvious to those involved in the communication process, but should be visible to a person monitoring the IT network. Most of these strategies are not unusual as the efficient transfer of data has been a preoccupation with the building industry almost since its inception. However the benefits of IT have often blinded users to their potential weaknesses. With the increased number of portable terminals, notebook computers and briefcase fax modems the number of possible infiltration points has been dramatically expanded.

The final strategy is awareness. The activity of 'trashing' is well known as the first step in breaking into a system. Careful shredding of documents and common sense destruction of sensitive materials will reduce this risk. Access accounts must be monitored, particularly distant connections. A professional virus or logic bomb will not be easily detected but a comprehensive backup system may reduce data loss. Once an intruder is found within a system the damage can be potentially great. Ideally security and procedures should restrict entry to the internal data NET. Problems with fax, phone and other telecommunications interception are rampant and not so easily overcome. The raising profile of the mobile phone scanning industry should assist in gradually training users to limit their discussions to non-classified data.

One solution offered by Ball (1985), and the A.C.M Special Security Interest Group is that of increased encryption. Not just within passwords and access codes but also within procedure and protocols. Passwords may be broken, the IBM generated DES encryption standard is no more a barrier to a determined criminal than is a lock on a door. However a company which has strong procedures and a specialised language, for example the technicalese of the building industry, requires more than just a password scanner to break the outer rim of protection. The proposed 'Keyless' encryption service, based around repetition to ensure understanding is achieved, is likely to cause greater workloads and an increase in potential intrusion times. Automatic software encryption and decryption devices which are transparent to the user are effective providing the encryption 'blue boxes' are not compromised by intrusion. A security system is only as strong as its own developmental security. Although this is the case there is much to be said for line-couple encrypters. This allows only correctly encoded data to be transmitted. The loss in time is minimal and the security gain potentially high. Within the project team if the links between offices, or sites are minimised and secured through encryption devices, and line encoders, then the internal system might be strengthened. Despite this, the weakest links for interception are outside the office network. Temporary lines to site sheds provide weak points as they may be tapped using commercially available electronics components with ease in less than three minutes.

CONCLUSION

"Information theft is destined to grow more troublesome as word processors replace typewriters in many offices. ...Typewriters do not store information when a report is finished - but with word processors, data stays in the system for future recall." (Ball, 1985) Almost all forms of IT leave not only a trace record of the data being communicated but also an electronic trail linking all components of the communication network. An intruder into the IT network may follow such a trail directly to the core where the data is kept.

Data must be used to be of benefit, and the twin processes of storage and retrieval are well studied. However both the storage and the retrieval methods must now be considered for security reasons. In any industry security should be a concern and arguably no other industry relies on IT as much as the building industry. Security strategies are still reliant on the human component, and the side effects of slowed data transmission due to security constraints are not desirable in the building industry. Within a project team, a thorough understanding of the forms of intrusion common in practice may provide the team with enough knowledge to fulfil the short term need, while the long term problem may only be solved through widespread education in the building industry.

References

Ball, L D Computer crime. in Forester, T. ed. (1985), *The information technology revolution.* T.J. press. Cornwall. p535

Barlow, J P (1990), Crime and Puzzlement, *Whole Earth Review*, Fall. Quoted in Hafner, K. Markoff, J. (1991).

Barton, P ed. (1985), *Information systems in construction management.* Batsford Academic press. London.

Becker, H B (1973), *Functional analysis of information networks, A structured approach to the data communications Environment.* John Wiley & sons. New York.

Betts, M (1992), How strategic is our use of information technology in the construction sector? *The international Journal of Construction Information technology.* Vol 1. No 1. Dec. pp79 - 97.

Cash, J I and Konsynski, B R (1985), IS redraws competitive boundaries. *Harvard Business review*, March /April. pp134-143.

Chesterman, J and Lipman, A (1988), *The electronic Pirates.* Routledge. London.

Hafner, K and Markoff, J (1991), *Cyberpunk, Outlaws and Hackers on the computer frontier.* Simon & Schuster. New York.

Laver, M (1989), *Information Technology: Agent for change.* Cambridge University Press. Cambridge.

Leslie, H G (1992), *An information and decision support system for the Australian Building Industry.* National Committee on Rationalised building. CSIRO division of building. pvii

Levy, S (1984), *Hackers: Heroes of the Computer Revolution* .Anchor Press/ Doubleday.

Möttönen, V J and Niskala, M (1992), Hyperdocuments in maintenance management of buildings. Vol. 9. section 12.1.3. *Proceedings, Management Maintenace and Modernisation of Buildings Conference.* Rotterdam October.

Quarterman, J S (1990), *The Matrix: Computer Networks and Conferencing Systems Worldwide.* Digital Press. New York.

Ross, A (1991), *Strange Weather. Culture, science and technology in the age of limits.* Verso. New York.

Sieber, U (1986), *The International Handbook on Computer Crime.* John Wiley & Sons. New York.

Spafford, E H (1989), The Internet Worm: Crisis and Aftermath, *Communications of the ACM*, June.

Sterling, B (1992), *The Hacker crackdown.* Bantam books. New York.

Stoll, C. (1990) *The Cuckoo's Egg.* Doubleday, New York.

Walraven, C (1992), Integrated CAD solutions for building management, maintenace and modernisation of buildings. Vol. 9. section 12.2.4. *Proceedings, Management Maintenace and Modernisation of Buildings Conference.* Rotterdam October.

Webster, F and Robins, K (1986), *Information technology, A luddite analysis.* Ablex publishers. New Jersey.

c. 1993, Management of Information Technology for Construction, K. Mathur et al (Eds), World Scientific Publishing Co., Singapore.