Software Piracy – Some Aspects for South African Managers to Keep in Mind

D de Kock and **W Kritzinger**
Department of Information Technology, Cape Technikon

S Lubbe
Department of Information Systems and Technology, University of Durban-Westville

ABSTRACT

Software piracy is a significant issue for managers of organisations, especially in developing countries. There are several factors which contribute to software piracy, and which are investigated in this study. This study consists of a literature review, and reports on empirical research, which was conducted using a survey instrument to determine if software piracy is prevalent in South Africa. The findings confirm the results of previous studies. The conclusion is made that software piracy will always exist and that stricter measures are needed to prevent its occurrence.

1 INTRODUCTION

Software piracy is known as the victimless crime, where, according to the software pirate, no one really gets hurt. What software pirates do not know is that their actions cause the software industry to lose revenue. Software piracy not only hurts the software industry but also legitimate users. This is because the software industry has to recover lost revenue by increasing software prices. Previous studies (Tan, 2002) have shown that certain demographic factors, such as the age of the consumer, may have an influence on ethical behaviour. The literature has shown that there are no significant differences in the incidence of software piracy according to the different age groups (Rahim *et al.*, 2000). In contrast, illegal software copying is common to all age groups, but younger age groups make more use of software piracy than older age groups.

This paper investigates software piracy in South Africa because any computer user has access to a CD-writer or the Internet and can copy software relatively easily. The study will concentrate on the factors that could cause people to become software pirates. The study also investigates the possibility that the problem of software piracy would be as big in South Africa as it is in the rest of the world. The study is important for managers who deal with software because it brings to their attention the problem of illegal copying and installing of software on organisational and personal computers. The study should create a new understanding of the issue in a South Africa context, because little research has been performed on the subject in this regard. The key factors that will be investigated include legal aspects and ethics. This study will look at some aspects, which have been covered previously in the literature, but will not attempt an in-depth study of other possible factors at the present stage, because of limited time and funding.

2 PARAMETERS OF THE STUDY

Software developers are protecting their software against piracy by developing copy protection techniques (Rahim *et al.*, 2000). Despite these copy protection services, software piracy still exists. The moral attitude of consumers, that it is their ‘right’ to copy software, will underline the message that this study would like to convey to managers – to stop software piracy. The dilemma of managers trying to stop software piracy needs to be investigated by looking at some of the factors that cause people to commit software piracy.

The study attempts to ascertain if factors such as consumers' ethical attitudes and morals, the perceived risks and moral judgement by others play a role in their decision to copy software illegally. The study further attempts to determine if demographics, computer experience and past purchase behaviour have an influence on the decision to use pirated software. The research objective is therefore to determine whether there is a relationship between participants' demographics and their attitude towards software piracy.

3 LITERATURE REVIEW

3.1 Definition of software piracy

Software piracy is the unauthorised copying and distribution of software (Lee, 1994). The different types of software piracy can be identified as industrial, corporate, reseller and home piracy as well as publisher patent and copyright infringements.

3.2 Software piracy

Industrial piracy takes place when individuals or groups of people make illegal copies of software with the intension of selling it for a profit. When someone installs a software application on a local area network (LAN) server, where employees can gain unlicensed access, that person makes him/herself guilty of committing corporate piracy. Reseller piracy, involves computer hardware, where companies sell computers with illegal copies of software preloaded onto their hard drives. Home piracy ranges from the distribution of illegal software, by trading disks with friends, family and colleagues, to running non-profit bulletin boards for distributing illegal software. Publisher patent and copyright infringement involve intellectual property theft, where one person copies material from another, without obtaining permission or acknowledging that they plan to profit from such action.

Other types of software piracy include direct infringement and indirect infringement. Direct infringement occurs when someone violates owner copyright by illegal reproduction, adaptation and distribution of software to the public. Indirect infringement can be divided into two categories, namely, contributory infringement and vicarious liability for infringement. The literature states that contributory infringement occurs when a person is aware of assisting, inducing or materially contributing to infringement of any of the exclusive rights, e.g. supplying serial numbers and cracker utilities. Vicarious liability for infringement occurs when someone has the authority to control the person who infringes any of the exclusive rights, and then gains financial benefit from his/her actions.

Many people violate software copyright law, without even being aware of it. Examples of such violations are giving away old versions of software after receiving upgrades, using shareware without paying for it, leaving software copies on a hard disk when selling a computer and borrowing software, to name a few.

3.3 Factors influencing software piracy

The proliferation of computers, networks and electronic mail, combined with the World Wide Web (WWW), make access to information easier than in the past. This creates favourable conditions for people to commit computer crimes (Armstrong & Lubbe, 1995).

The key factor that influences software piracy is the consumer’s ethical attitude. The ethical decision process of the consumer is influenced by three factors, namely moral intensity, perceived risk, and moral judgement. Moral intensity has to do with the extent of issue-related moral imperative in a situation. Perceived risk is negatively related to self-esteem, rigidity and risk taking and positively related to anxiety. Risk perception is argued to have cross-cultural variation. People in socially-collectivist cultures tend to choose riskier options, e.g. use pirated software, than those in individualist. Moral judgement has to do with believing that it is right is to avoid breaking rules, obeying for obedience's sake, and avoiding doing physical damage to people and property.

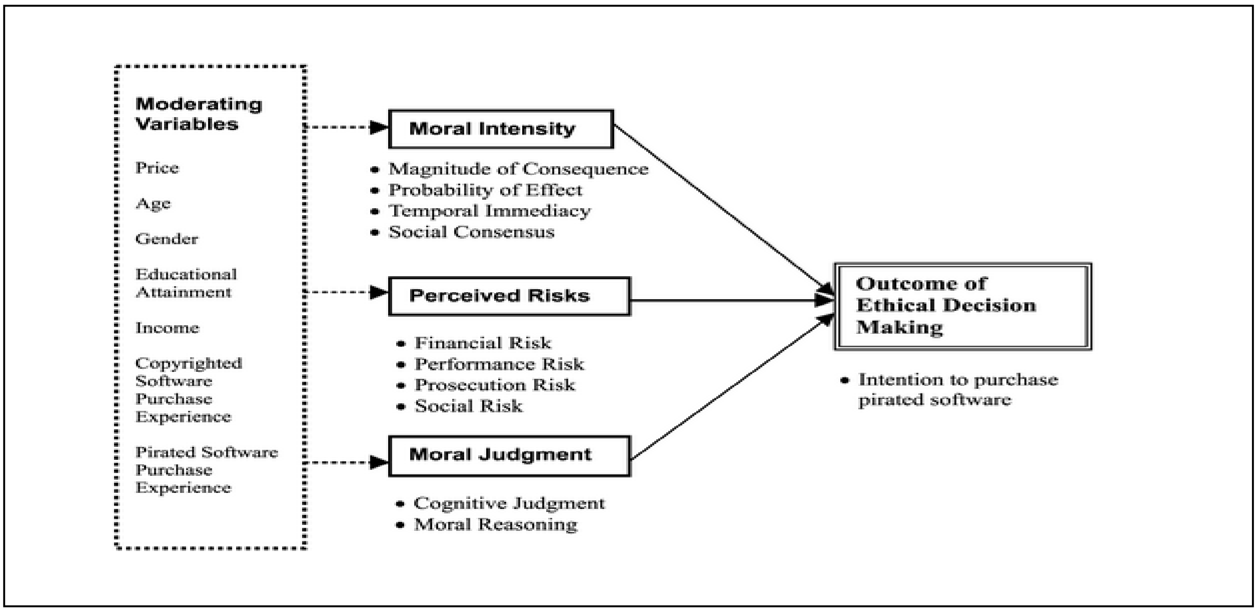
Tan (2002) has developed a four-component model that describes the process of a consumer's ethical decision making. According to the model, the consumer must recognize the moral issue, make a judgement, establish intent and implement actions.

Risk is also a critical factor that has an influence on ethical decision-making (Tan, 2002). Tan *cites* Rettig and Rawson, who note that risk might drive people to unethical behaviour and that radical individuals are more vulnerable to risk-taking decisions than conservative individuals. Fraedrich and Ferrell are *cited* by Tan as researchers who have measured the impact of perceived risks and moral philosophy on ethical decision-making. These risks, amongst others, include financial-, performance- and social risks of software piracy. Financial risk involves the probability of losing money by making a decision. Performance risk is related to the probability that a product or service may not work. The user has no guarantee that pirated software will function correctly. In addition to the performance risk, there is the probability that the failed pirated software will subject the individual to financial risk in terms of expenses due to lost time, data recovery and reinstatement of the computer system.

The probability that use of the pirated product or service may affect what others think of the individual is a social risk. A prosecution risk also effects the moral decision, because being linked to software piracy is an infringement of copyright law and a user runs the risk of civil action (Tan, 2002). Tan implies that there is a link between moral judgment concerning an action and the intention to perform that action. Moral judgement is the reason why certain actions are perceived as morally just or preferred.

Tan (2002) notes that moral intensity, perceived risks and moral judgement influence the outcome of the ethical decision. He depicts this by using an issue-risk-judgement model (Figure 1) (Tan, 2002). Due to the fact that studies have shown that ethnical behaviour is influenced by consumer demographics, situational variables such as age, gender and educational attainment have been taken into account, because they can affect the outcome of a decision. Past buying behaviour of consumers may also have a contingent effect on their ethical decisions. The probability is higher that an individual will acquire pirated software again, if that person has bought illegal software in the past (Tan, 2002). The greater the price difference between original software and pirated software, the larger the economic incentive is to act unethically and buy illegal software.

Figure 1 Issue-risk-judgement model (Tan, 2002)



3.4 Effects of software piracy

Software vendors estimate that billions of dollars in revenue (BSA estimates about $2 billion in 2002, (see Naraine, 2003) are lost annually due to worldwide software piracy. Software piracy is also a channel for spreading computer viruses. Furthermore software piracy leads to higher prices for legitimate users, because software vendors have to recover lost revenue due to illegal software distribution. Another effect of software piracy is that software publishers are more reluctant to do business in regions where it occurs more frequently. This can cause a slow-down in development of technologies in these regions, making the regional organisations less competitive.

3.5 Legal aspects

Software piracy falls into the field of intellectual property law (Lee, 1994). All information found on items such as diskettes, CD-ROMs or the Internet, is covered by copyright laws and licenses (Saunders, Forcht & Counts, 1998). There are also certain other issues which have not yet been defined by laws in court decisions, as explained below.

Commercial software is directly or indirectly licensed by software publishers by means of contracts called “end-user license agreements” (EULAs). A EULA is a legal contract between the Software Company that owns the copyright to the software, and the organization or individual that uses it. A EULA grants permission to use the software along with additional rights, since the EULA also poses certain restrictions on the use of the software. The “Grant of License” section in the EULA describes how the software should be used and includes restrictions against reverse engineering, leasing, or renting of the software. The EULA also describes the terms under which the user may make a backup or archival copy of the software. All software should be accompanied by a EULA; otherwise it may have been purchased illegally.

Legal issues of computer crimes are often a grey area (Armstrong & Lubbe, 1995). Software piracy is one of the computer crimes that more easily dealt with. There are, however, still certain problem areas such as software downloaded from the Internet. An example would be people-to-people (P2P) networks, where there is no central organization responsible for copyright infringement (Cheng, Ang, Lim, & Tambyah, 2002). P2P networking is direct Internet-based communication between two or more agents, e.g. computers that can bypass a centralised computer server.

Only the designer/owner of the software can give permission to use copyrighted material (Saunders *et al.*, 1998). Permission is given for the copyrighted material to be distributed in electronic form as long as it is not commercially used or sold. In some countries, protection does not exist, due to the lack of proper legislation or policy (Ilkka *et al.*, 2001). Low availability of software and high prices provide justification for both violators and governments to tolerate the practice of piracy.

3.6 Techniques for limiting software piracy

People see software updates as a nuisance, but they can be turned into a technique for limiting software piracy (Jacobson & Reiter, 2001). Updating is linked to “software aging”, which forces users to update their software, otherwise it becomes less useful over time. This method of protection relies on the regular update of software. Software piracy and software updates are addressed at the same time, improving the system as a result. Software updating discourages software piracy, because legitimate users are getting the benefits, while inflicting damage on the illegal users of software. This creates a situation where illegal software versions become incompatible and are therefore forced to rely on more piracy for updates. This increases operating costs for pirates, since they are forced to keep in touch with their clients. Software aging mainly focuses on industrial piracy, and stops people from making a profit from selling pirated software.

Another technique for limiting piracy is making counterfeit software easier to recognize by embedding hologram images on the original surface of disks (e.g. MicroSoft Office 2000). If there is an indication that software has been pirated, individual might not want to purchase it. Meterware, on the other hand, is a technique where users are billed for using software. Once a month the user dials a "billing number". The billing office will then determine how many times the software was used and bill the company for use.

3.7 A normative model of software piracy

The normative model (Figure 1) is used as a tool for understanding issues, such as demographics, computer exposure and past purchase behaviour and their relation to people's ethical attitudes towards software piracy. A normative model is a one-stage model that relates independent and dependent variables, without any intermediate variables (Rahim *et al.*, 2000). The use of pirated software is the dependent variable, and the normative model ties this variable to eight independent variables, grouped into three categories, these being demographics, computer exposure and past purchase behaviour.

The normative model in Figure 1 shows that moderating variables such as gender, age and income can be used to test against variables such as: computer ownership, any education in IT, and whether a user can identify the difference between original and pirated software. Computer exposure includes the user's opinion on the probability of failure of pirated software. Past purchase behaviour includes issues such as whether the person has ever purchased pirated software before.

3.8 Research questions

Based on the issues that have been identified and the contribution of the literature, the following research questions have been identified:

1. What are the demographics of software pirates in the Western Cape and how do demographic factors affect software piracy?
2. What factors show agreement with international trends?
3. What should managers look out for in order to prevent software piracy?
4. What type of tasks are performed using pirated software?

4 RESEARCH METHODOLOGY

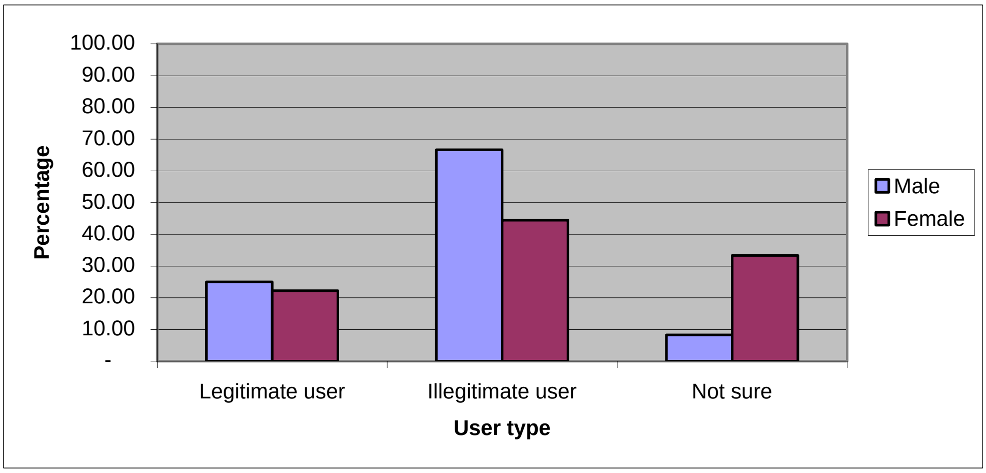
The survey approach was used to investigate trends in software piracy. A questionnaire was developed, based on Figure 1, that consisted of two parts and can be supplied upon request.

The first part of the questionnaire captured the demographics of the participants who participated in the survey. The demographics section collected details about individuals' age, gender, income, education and whether they own computers. The second part of the questionnaire focused on the reasons for using pirated software, the tasks performed using pirated software and participants' consumer behaviour. It also focused on their knowledge of software piracy, e.g. whether they could spot the difference between original software and illegal software, whether they were aware that their computers might have illegal software loaded onto them and also focussing on the easiest ways to obtain illegal software. A letter was included with the questionnaire explaining to participants what the questionnaire is about. The letter mentioned that the results would only be used for research purposes and that they would be treated confidentially. This ensured that participants would not shy away from participation.

The questionnaire was piloted on a group of students to ensure that the questions were clear and understandable. In August 2002, the revised questionnaires were handed out and posted to 40 people in an apartment building where one of the researchers lives. This building was selected for convenience sake because of easy access and time and cost limitations. Only 21 questionnaires were returned, which might be an indication that people are still not keen to distribute data about their illegal activities. The data obtained from the sample group were entered on a spreadsheet and analysed using Excel. The figures from the questionnaires were rounded, to simplify the outcome.

5 DISCUSSION OF THE RESULTS

Figure 2 Use of pirated software based on gender



Ninety five per cent (Table 1) of the population sample falls into the age group of between 18 and 35 years. Of this specified group, 55 per cent are illegal software users, 25 per cent are legitimate users and 20 per cent are unsure if they have illegal software on their computers (Figure 2). The rest of the sample falls in the age group over 35, and are all illegal users.

Table 1 Background profile

Background profile of participants	%
Gender	
Male	57.14
Female	42.86
Age	
18 years and younger	0.00
Between 18 and 35 years	95.24
35 years and older	4.76
Income	
R2000 or less	61.90
Between R2000-R5000	23.81
Between R5000-R10000	9.52
More than R10000	4.76
Education	
Education of any type in IT	61.90
No education of any type in IT	33.33

Table 1 continued

Background profile of participants	%
Computer ownership	
Own a computer	95.24
Does not own a computer	4.76
Pirated software	
Bought pirated software	19.05
Has not bought pirated software	80.95
Probability pirated software can fail	48%
Difference between illegal and original software	
Can spot difference	42.86
Can not spot difference	57.14

It was decided to remove the age group, “35 years and older”, from the analysis, since 5 per cent of the population sample represents only one person and inclusion of this 5 per cent might give a misleading view that people over 35 years are all illegal users (Table 2). It can be argued that there are differences in ethical beliefs between younger and older people. Although 95 per cent of the population sample falls into the age group between 18 and 35 years, 55 per cent of this group are illegal users. Therefore the conclusion is drawn that people younger that 35 find it easier to use pirated software without worrying about the consequences.

5.1 Gender

The results show that 57 per cent of the population sample is male and 43 per cent is female (Table 1). Of the 57 per cent that represent males, 25 per cent are legal users, 67 per cent are illegal and 8 per cent are not aware of any illegal software on their computers (Table 2). In contrast, of the females, 22 per cent are legitimate users, 44 per cent illegitimate users and 33 per cent are not sure whether they are using illegal software (Table 2). There is a strong positive correlation of 0.65 between male and female users, meaning that if the one increases, the other will also do so. This correlation is also statistically significant. The p-value was calculated by Excel as being more than 70 per cent which indicates that the true effect is positive and that there is a strong possibility that an illegal user of pirated software would be male.

The findings are supported by Rahim *et al.* (2000) who also used gender as one of the independent variables for software piracy. They noted that other authors discovered that gender had no effect on software piracy. The findings of this paper confirm Rahim *et al.’s* findings by noting that males are more likely to use pirated software than the females. Computer use is also seen as a masculine activity and therefore males use computers more often than females. It is also known that in general, males have less ethical sensitivity than females (Rahim *et al.,* 2000).

Table 2 Normative model layout

	Percentage		
Age	**Legal**	**Illegal**	**Not sure**
18 years and younger	-	-	-
Between 18 and 35 years	25.00	55.00	20.00
35 years and older	-	100.00	-
Gender			
Male	25.00	66.67	8.33
Female	22.22	44.44	33.34
Income			
R2000 or less	23.08	53.85	23.07
Between R2000 and R5000	40.00	40.00	20.00
Between R5000 and R10000	-	100.00	-
More than R10000	-	100.00	-
Spot difference			
Can recognize difference	33.33	55.56	11.11
Cannot recognize difference	16.67	58.33	25.00
Believe that pirated software can fail	52.00	39.00	53.00
Past purchase behaviour			
Bought pirated software before	-	75.00	25.00
Haven't bought pirated software	29.41	52.94	17.65
No education in IT	50.00	50.00	-
Computer ownership			
Own a computer	23.81	57.14	19.05
Do not own a computer	-	-	-
Education			
Education in IT	7.69	61.54	30.77
No education in IT	50.00	50.00	-

5.2 Income

According to the original results, 62 per cent of the population sample have a monthly income of R2000 or less, 24 per cent have an income between R2000-R5000, 10 per cent between R5000-R10000 and 5 per cent earn more than R10000 (Table 1). It was decided to normalise income groups by removing the income group, "Between R5000-R10000" and "More than R10000" from the analysis for statistical purposes, because only two persons and one person, respectively, made up each category. This created two categories for the purposes of analysis. Of the normalised income group that earns R2000 or less, 23 per cent are legitimate users, 54 per cent are illegitimate and 23 per cent are not sure whether they have pirated software on their computers. Of the income group that earns more than R2000, 40 per cent are legitimate users, 40 per cent illegitimate users and 20 per cent are not sure whether they have illegal software on their computers. There appears to be a weak relationship between an individual's income and his/her use of pirated software (the correlation was measured as 50 per cent). There was a probability of 90 per cent that a person earning a low salary will use pirated software.

This finding is supported by a statement in the literature that people with higher incomes can afford original software and are less likely to resort to software piracy (Rahim *et al.*, 2000). On the other hand, someone with a lower income will place priority on basic needs before allocating money for luxuries. As software is often expensive, the probability is higher that the person will engage in software piracy before considering buying original software. It can therefore be stated that there is a relationship between an individual's income and his/her use of pirated software.

5.3 Computer ownership

The results showed that just one person in the sample did not own a personal computer. According to the sample group, of those that own a computer, 24 per cent are legal users, 57 per cent are illegal users and 19 per cent are not sure whether they have illegal software on their computer (Table 2). It can be stated that there is a relationship between computer ownership and the use of pirated software. The probability that computer owners will use illegal software is nearly 70 per cent (at 5 per cent significance).

A person who owns a computer is likely to spend more time on a computer (Rahim *et al.*, 2000). Such a person will perform a wider variety of tasks than someone that does not own a computer. To obtain a wider variety of software, the person is likely to obtain software from various sources, some of which could be illegal software. It can be argued that there is also little or no supervision on the use of software when people are working in their own privacy. This could in turn encourage the use of pirated software. The theory is thus supported by the findings.

5.4 Education

The results show that 62 per cent of the population sample had some form of IT education and 33 per cent no IT education (Table 1). Of the 62 per cent of computer literates in the sample, about 7 per cent are legal users of software, 62 per cent are illegal users of software, while 31 per cent of them are not sure whether they make use of pirated software (Table 2). In contrast, the sample representing people who have no education in IT, 50 per cent are legal users and 50 per cent are illegal users (Table 2). The probability that there is a link between education and illegal software is not that high in this sample (only 50 per cent). The results show that IT educated people make greater use of illegal software.

Tan (2002) *cites* Solomon and O'Brien, who note that educational background, amongst other demographics of consumers, is significantly correlated with their attitude towards software piracy (Tan, 2002). People who have limited experience with computers are likely to perform routine tasks only and are unlikely to try a wider variety of software programmes (Rahim *et al.*, 2000). People who have more experience with computers have greater knowledge of software use. The frequency and duration of software use of these people will increase and therefore they will be more likely to use a wider variety of software. Computer-experienced people are more likely to use pirated software. The results in this study therefore support the theory, but not that significantly.

5.5 Difference between original and pirated software

In this study, 43 per cent of the population sample can spot the difference between original software and pirated software (Table 1). Of the 43 per cent, 33 per cent are legitimate users, 56 per cent are illegitimate users and 11 per cent are not sure whether they have pirated software on their computers (Table 2). The rest of the sample does not know the difference between original and pirated software, and of these 17 per cent are legitimate users, 58 per cent are illegitimate users and 25 per cent do not know if they own pirated software (Table 2). There is a relationship between people who can recognize the difference between the software types and the use of pirated software. The probability is more than 80 per cent that people will own pirated software, because many cannot distinguish between legal and illegal software or are indifferent to pirated software.

If there is a clear indication that software might be pirated, there is a chance that people will not purchase it. This technique appeals to a person's integrity, because the consumer faces a social risk (Tan, 2002). The situation in South Africa is slightly different, because people are more inclined to use illegal software due to the fact that they would like to have the latest software but often cannot afford it.

5.6 Probability of pirated software failing

According to the results, legitimate users believe that there is a 52 per cent chance that pirated software will fail to function, illegal users believe there is a 39 per cent chance and those who are not sure if they have pirated software, believe that there is a 53 per cent chance the pirated software could fail to function (Table 2). There is no guarantee that pirated software will function as well as original software (Tan, 2002) and for this reason consumers face a performance risk. Pirated software may also contain viruses or could even damage computer systems. This poses a financial risk for the consumer, since the afore-mentioned risks inflict costs in terms of loss of time due to reinstatement of systems and data recovery. The higher the risks perceived by consumers, the lower the probability that they will purchase the pirated software (Tan, 2002). This agrees with the findings of this study.

5.7 Past purchase behaviour

The percentages in Table 1 indicate that 81 per cent of the sample has never bought pirated software before, while only 19 per cent has done so. There is also an indication that most of the pirated software was obtained free of charge. Of the proportion that have bought pirated software before, 75 per cent are illegal users and 25 per cent are not sure if they have illegal software on their computers. The rest of the sample that has never bought pirated software before, contains 29 per cent legal users, 53 per cent illegitimate users and 18 per cent who are not sure if they are using illegal software. A conclusion is made that there is a relationship between past purchase experience and the use of pirated software. This is supported by the theory.

Tan (2002) argues that individuals who have bought copyrighted or pirated software before are likely to repeat their actions when acquiring new software. If consumers have bought pirated software in the past, the probability is higher that they will acquire pirated software again. The larger the gap is between the price of original and pirated software, the greater the economic incentive to act unethically. There is no deception when people are willing to buy counterfeits, and they are therefore not the victims of a scam (Cheng *et al.*, 2001). Another study is required in order to understand the reasons behind people's favourable attitude towards software piracy.

5.8 Additional results that could help managers

According to the results, 57 per cent of the population sample makes use of pirated software, 24 per cent are legitimate users and 19 per cent are not sure whether they own or use illegal software of any kind on their computers (Table 1). This result indicates that there is a huge market for illegal software with more than 50 per cent of software users participating in illegal activities.

According to all the people that participated in this survey, the high cost of software is one of the biggest reasons why people resort to software piracy. The second most common reason for people making use of pirated software is because they think that there is no threat of being prosecuted. The third reason is delayed release dates in the area representing 10 per cent of the population. The fourth reason why people use software piracy is lack of the availability of appropriate software on the market.

The most common use for pirated software is personal use, chosen by 71 per cent of the population that participated in the questionnaire (Figure 4). The second most common use of pirated software is for playing computer games (38 per cent of the population). Office work is one of the least likely reasons for use of pirated software.

The four research questions have all been addressed in the discussion above. The answers to the questions can be summarised as follows:

1. The general demographics of illegal users are:
   - mostly younger that 35 years old and in the lower income group;
   - mostly males; and
   - IT-educated users.
2. All of the factors cited in international studies are supported by this study. The probability that IT-educated users will use illegal software is not as high as in the overseas studies.
3. Managers should:
   - audit the contents of personal computer hardware regularly;
   - keep tighter control over their original software and backup copies;
   - keep the ethical side in mind for themselves and for their employees; and
   - ensure that their organisations keep track of where their software has been installed.
4. The software the pirates acquire and sell or give away, is usually every-day software that people cannot afford (e.g. MicroSoft Office). There is also a big market for games and Internet design software.

6 CONCLUSION

According to Tan's (2002) issue-risk-judgement, some people are more ethical than others. If a person considers software piracy morally unacceptable, this has a major influence over the person's decision regarding piracy. It is too great a challenge to influence the general attitude to ethics regarding software piracy, and for this reason it always pose a problem.

The software industry and public authorities face the challenge of increasing moral intensity and thus changing the decision to buy or use pirated software. One way to achieve this is to make originals easier to recognise by using holograms, which appeals to a person's integrity. By making a clear indication that software is illegal, there is a higher probability that people will not buy the pirated software.

The study also identified that computer ownership and computer education are related to software piracy. This is due to the fact that there is little or no monitoring of software on private computer. Little or nothing has been done to trace and take action against users of pirated software (Tan, 2002). By taking legal action, consumer's ethical decision making is affected, since risk of prosecution affects moral decisions.

As a final thought, it is important to confront the problem of software piracy by looking at possible ways to put a stop to it, rather than by analysing the current state of affairs, since high rates of growth in technological infrastructure throughout the world will mean that software piracy will always pose a significant threat.

REFERENCES

1 ARMSTRONG, G. & LUBBE, S. (1995) "Computer crime and the measures of detection and prevention of such crime," *VITAL*, 10(1): 19-31.

2 CHENG P.S., ANG, S.H., LIM, E. & TAMBYAH, S.K. (2001) "Spot the difference: Consumer responses towards counterfeits," *Journal of Consumer Marketing*, 18 (Spring): 219-235.

3 ILKKA A., GUERRERO-CUSUMANO, R. & JOSE-LUIS, (2001) "Correlates of intellectual property violation", *Multinational Business Review* 9(1): 59-65.

4 JACOBSON, M. & REITER, M. (2001) "Discouraging software piracy using software aging", http://www.star-lab.com/sander/spdrm/papers.html, Downloaded: June 2002.

5 LEE, M. (1994) “Legal aspects of computer crimes and information systems security in Hong Kong”, http://www.is.cityu.edu.hk/Research/Publication/paper/9404.pdf., Downloaded June 2002.

6 RAHIM, M.M., RAHMAN, M.N.A. & SEYAL, A.H. (2000) “Software piracy among academics: an empirical study in Brunei Darussalam” *Information Management & Computer Security*: 8/1/2000 14-26.

7 NARAINE, R. (2003) “Tackling software piracy an uphill battle”, http://www.internetnews.com/entnews/article.php/1856611, Downloaded March 2003.

8 SAUNDERS, D., FORCHT K.A. & COUNTS, P. (1998) “Legal considerations of internet use - issues to be addressed”, *Internet Research*, 1(8): 70-74.

9 TAN, B. (2002) “Understanding consumer ethical decision making with respect to purchase of pirated software”, *Journal of Consumer Marketing*: 19(2): 96-111.