Computers & Security Vol.18, No.8, pp.715-726, 1999

0167-4048/99$20.00

Computer Crime and Abuse: A Survey of Public Attitudes and Awareness

P. S. Dowland[1], S.M. Furnell[1], H.M. Illingworth[1] and P.L.Reynolds[2]

[1]*Network Research Group, School of Electronic, Communication and Electrical Engineering, University of Plymouth, Plymouth, UK.*

[2]*Orange Personal Communications Services Ltd, St James Court, Great Park Road, Bradley Stoke, Bristol, UK.*

In recent years, a number of surveys have indicated a significant escalation in reported incidents of computer crime and abuse. This rise is coupled with increasing attention to the issue in the mass media, which has the effect of heightening public perceptions of problems with IT and may represent a barrier to the adoption of technologies such as the Internet and World Wide Web.

This paper considers the effects of computer crime and draws upon the results of a survey conducted to assess public attitudes and awareness of the issue. With the mass media playing an important role in shaping individual opinions, this survey considered the effect that the reporting of incidents has upon public perceptions and understanding of computer crime and abuse.

The survey results show that individual awareness of computer crime and abuse is high and that the majority of respondents perceive it to be a problem. However, the views expressed regarding the seriousness of the different types of abuse (and the potential motivations for them) were more variable. In addition, awareness of abuse is more widespread than knowledge of the associated legislation that may be used to prevent and punish it. The results also revealed the significant potential for media reports to influence opinions in this area, highlighting the importance of a responsible attitude in order to foster the information society.

Keywords: Computer crime, computer abuse, hackers, viruses, awareness survey.

Introduction

The last two decades have witnessed the use of computer technologies in a wide range of business and domestic scenarios. As such, there are few people in Western society whose lives are not affected in some way by the use of Information Technology (IT). More recently, the explosive growth of both the Internet and World Wide Web (WWW) has meant that IT has had yet further impacts upon our everyday lives. However, with society's widespread use of and, in some cases, reliance upon technology, significant opportunities now exist for both mischievous and malicious abuse via IT systems. The meaning of terms such as hacker and virus are now widely understood in an IT context and related reports are common occurrences in the mass media.

A number of recent incidents have reaffirmed the susceptibility of IT systems to abuse. Examples here include the breach of security on Microsoft's Web-based Hotmail service [1] and the self-distributing 'Melissa' virus [2]. These incidents attracted significant media attention and it is considered that such publicity will unavoidably influence public opinions regarding the Internet and IT systems in general.

While a number of surveys have been conducted to assess the level of abuse, there has not been a corresponding investigation into the public perceptions that result. This issue may be equally, if not more, important in determining the effect that abuse has on

	Fraud	Viruses	Theft	Hacking	Other	Total
1984	60	-	17	-	-	77
1987	61	-	22	35	-	118
1990	73	54	27	26	-	180
1994	108	261	121	47	-	537
1998	67	247	88	56	52	510

Source: UK Audit Commission 1984-1998
Table 1 : Reported incidents of computer crime and abuse

the development of the information society. The paper begins by examining the results from previous surveys, which serve to indicate the level of computer abuse. The discussion then proceeds to present new results relating to the awareness and attitudes of the general public, based upon a survey conducted by the authors.

The Computer Crime and Abuse Problem

A number of national surveys can be cited which provide a good indication of the level of computer crime. One of the best examples comes from the UK Audit Commission, which has conducted a series of surveys over the last 15 years to assess the scale of the computer crime and abuse problem [3,4,5]. The results from these surveys, categorized by incident type, are presented in *Table 1*.

It is clear that over the last decade there has been a significant increase in the reported incidents. A clear factor influencing this increase is the explosion in virus incidents that can be observed in the 1990s. It is worth noting that, in the latest results, 'hacking' is the only category of abuse in which the reported incidents have risen (in both real terms and as a percentage of incidents reported) when compared to the previous 1994 survey.

Further Audit Commission figures (*Table 2*) show that the overall costs incurred by computer abuse incidents have also increased over the last 15 years. However, the average loss per incident is now less, which can be explained by the fact that viruses now account for a significant proportion of incidents and their financial impact is generally much less than other classes of abuse. It should also be noted that the figures only relate to *reported* incidents, from the respondents to one particular set of surveys. It is often conjectured that the true level of computer crime remains much higher than reported [7], as organizations do not wish to risk undesirable consequences such as bad publicity, legal liability or loss of custom.

Whilst it is difficult to determine figures for computer crime affecting the domestic computer user, those

	Fraud	Viruses	Theft	Hacking	Other	Total
1984	£1,131,186	-	£2,301	-	-	£1,133,487
1987	£2,526,751	-	£34,500	£100	-	£2,561,351
1990	£1,102,642	£5,000	£1,000	£31,500	-	£1,140,142
1994	£3,042,318	£254,925	£394,725	£130,245	-	£3,822,213
1998	£2,360,646	£403,921	£62,480	£360,860	£100,740	£3,288,647

Source: UK Audit Commission 1984-1998
Table 2 : Costs of computer crime and abuse

available for the business sector show a high level of abuse. In the most recent Audit Commission survey [5], 46% of the 900 UK respondents reported some form of incident. These figures are similar to a more recent survey in the United States where the Computer Security Institute, in association with the Federal Bureau of Investigations (FBI), contacted large enterprises (with turnovers ranging from under $10 million to over $1 billion) to determine the levels and effects of computer crime and security [6]. In this survey, 319 out of the 521 respondents (61%) had experienced some form of computer abuse. This survey also showed that the levels of every form of computer crime in America increased over the previous year. Whilst computer crime is on the increase, organisations are starting to retaliate, with 32% of detected crime being reported to the police in the US — a marked increase over the 17% figure from previous years. Unfortunately, the UK is lagging behind, with only half of the surveyed organisations publicly acknowledging security incidents and only 25% reporting the crime to the police [8].

In the UK, the cost of computer abuse incidents reported to the Audit Commission survey totalled £3.9 million. However, this is dwarfed by the US with CSI figures showing a loss exceeding $123 million from the 521 companies participating in their 1999 survey. However, when considering these figures (and those from *Table 2*), it should be remembered that financial loss is merely one impact that may result. Other impacts, such as disruption to services, loss of data or damage to reputation, are more difficult to quantify.

While the above results indicate the scale of the problem and serve to give an indication of the commercial and/or financial implications, they do not address the wider issue of how computer abuse may be affecting public perceptions of information technology. This is likely to be a significant factor in realizing the full potential of IT, particularly in scenarios where public trust and confidence are required to ensure wide-scale acceptance. The Internet already has a general reputation for being insecure, which may ultimately limit its acceptance by the general public and lead them to less flexible solutions. For example, in the UK, the interactive digital television service 'Open' is citing the insecurity of the Internet as a key reason why its own home-shopping and online banking facilities are superior [9]. Highly publicized incidents of computer crime and abuse have significantly contributed to the Internet's reputation for insecurity. As such, it is useful to determine more specifically how such incidents are perceived and the possible effects that this may have.

A Survey of Attitudes and Awareness

In order to determine the potential wider impacts of computer crime and abuse, a survey has been conducted to assess the attitudes and awareness of the general public. The survey aimed to address the following issues:

- public awareness of, and attitudes towards, computer crime and abuse;
- the influence the media has over individual views and perceptions of computer crime and abuse.

The survey consisted of 53 main questions, the majority of which were multiple choice, with the remainder requiring short written responses. Many of the questions contained multiple sections, resulting in a maximum of 130 possible answers per respondent. The survey was split into a number of categories, each focussing on a specific area of interest to the authors. Questions 1-7 gathered general details, to determine the gender, age, education, and level of computer use; these provided demographic information on the survey response base. Questions 8-14 considered the use of computers within the respondent's work environment, whilst questions 15-19 considered the use of computers at home. These helped to provide information on the spread of IT into the home and work contexts, as well as the likely IT awareness of the respondents. Questions 20-34 were intended to determine individual opinions and knowledge in the area of computer crime and abuse. In particular, this section looked at the respondents' perception of hackers and the perceived representation of them by the mass media. The final section (encompassing questions 35-53) looked at the respondent's views on user

authentication and supervision, which was considered to be an interesting progression from their views on computer abuse. This paper targets the issues of computer crime and abuse, whilst the findings relating to authentication and supervision will be the focus of a future publication.

The study was conducted over a six-month period, commencing in October 1998. The survey was distributed to a wide range of individuals and organizations with the intention of gaining a diverse variety of opinions. The questionnaire was made available in two forms, a printed copy and an online version published on the authors' WWW site. Approximately 300 printed surveys were distributed with 148 completed responses being received, representing a response rate of 49%. A further 27 surveys were submitted via the Web-site resulting in a total of 175 responses. It should be noted that, whilst questionnaires were sent to companies, the focus required respondents to reply from an individual rather than organizational perspective. As such, these responses were still representative of a public rather than business viewpoint on the issues.

Analysis of Results

General

The survey demographics showed a male dominance in all age groups, with 80% of the total respondents being male. In terms of age, 74% of the respondents were below 35, indicating that the vast majority of the responses were likely to be from people who had 'grown up' with IT to some extent. The overall breakdown of respondents by age group is given in *Figure 1*.

In terms of employment background, a high number of responses were received from the technology fields (with 103 out of the 175 responses claiming to be from the computing, communications or engineering domains). Academically over 70% of the respondents claimed to hold A-Levels or above, with 44% having a degree level education. This represents a generally high level of academic achievement and reflects the

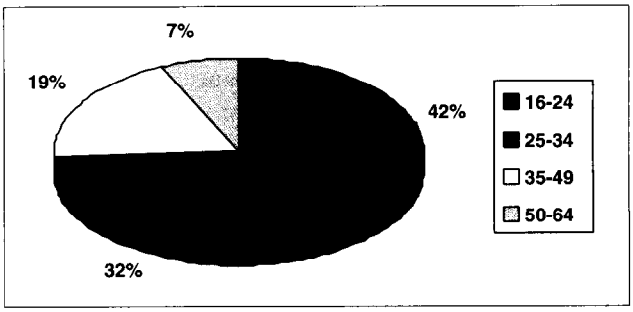

Figure 1: Survey respondents by age.

fact that the distribution of a large proportion of surveys occurred via academic channels.

The vast majority of respondents had considerable familiarity with IT, with over 98% having used a computer for over 1 year, 88% using a computer at work and 84% using one at home. In terms of the level of use, the results indicated that, in both home and work environments, over half of the respondents used their systems for four hours per week or more. The respondents were also asked about the availability of Internet access. 129 respondents (88%) claimed to have access at work, while 69 respondents (48%) claimed to have access at home. The latter statistic indicates that the respondent group is clearly ahead of the UK average in terms of Internet adoption, as current penetration into UK homes is considered to be around 14% [10].

The general information above shows that the respondents had considerable experience using computers in both home and work environments. As later sections of the survey looked at views on computer crime and abuse, it was felt that the respondents were suitably qualified to comment on these issues. However, this did tend to preclude an assessment of how the views of non-IT aware members of the public might have been affected by media presentation of crime and abuse issues.

Personal Misuse Practices

Before asking the respondents about a variety of computer abuse issues, the survey attempted to gauge their own morals. This was achieved by obtaining their

views regarding three types of dubious practice, namely the use of unlicensed software, unauthorized use of IT facilities and the sharing of passwords.

In recent years, the Business Software Alliance (BSA) has taken a firmer stance on the use of unlicensed software in the workplace with their 'BSA Crackdown 99' [11]. Despite this work, the use of unlicensed software is still rife, at 30%. In addition, 35 respondents (20%) claimed they did not know the status of the software they were using and 21 respondents (12%) declined to answer. However, this is overshadowed by 61% of domestic users with unlicensed software, although again 32 respondents (18%) declined to answer.

The results indicated that 75% of those using computers at work used their equipment for non-work related activities. Although this type of activity is classed as abuse according to the Audit Commission categorizations [5], it may well depend upon the policy of individual organizations as to what extent it is permissible. However, the level to which such illegitimate activities occur may well be of interest to employers.

In terms of passwords, 31 (21%) of the 151 respondents who used computers at work claimed to have used another person's password or account without their consent or knowledge. This is especially of concern as, in a later question, 114 (65%) of the respondents considered the act of viewing someone else's data to be a serious act of computer abuse (although how they can reconcile their views and their own actions is questionable). Finally, despite the obvious risks, 29% of respondents claimed that other people knew their password(s), which serves to reiterate some of the known weaknesses of this approach to user authentication [12].

Opinions on Computer Crime and Abuse

In general terms, over 80% of respondents felt that computer crime and abuse was a problem. While this represents the vast majority of respondents, it is surprising that the figure is not higher still. The fact that a fifth of respondents do not perceive computer abuse as a problem indicates that they either have an extremely lenient view of the activities or do not recognize the significance of IT in modern society.

A more detailed evaluation of respondents' views about computer crime and abuse began by asking them to assess the seriousness of a range of potential abuse scenarios. As can be seen from the results in *Table 3*, most acts of computer crime were rightly considered to be of serious concern. However, a number of interesting observations can also be made. Firstly, it can be noted that only theft of computer equipment was considered to be entirely criminal, with no respondents considering it to be acceptable. Secondly, the incidents that were most readily identified as being 'very serious' were those with a clear analogy in the real world (i.e. theft, sabotage and, to

	Very serious	←	Indifferent	→	No crime
Viruses	71%	17%	9%	1%	2%
Viewing someone else's data	29%	37%	25%	4%	5%
Altering someone else's data	80%	15%	3%	0%	2%
Theft of computer equipment	82%	15%	3%	0%	0%
Unauthorised copying of software	18%	22%	36%	13%	11%
Unauthorised copying of data	24%	35%	26%	6%	9%
Computer fraud	70%	20%	9%	0%	1%
Sabotage	90%	6%	3%	0%	1%

Table 3 :Views on computer crime and abuse

a lesser extent, fraud). By contrast, a surprisingly high proportion of respondents expressed indifference or no concern about issues such as unauthorized copying of data or software, or viewing someone else's data. This indicates that many people may have little appreciation of issues such as privacy in an IT context and draws into question whether they would be able to make informed decisions about their own use of technology. The responses regarding unauthorized copying of software tie in with the earlier results observed in relation to personal misuse practices.

Respondents were asked a number of questions in relation to computer hackers, which represent one of the most 'hyped' forms of abuse in the mass media. When asked to describe their image of a hacker, the strongest single view that emerged (from 30% of respondents) was solitary, young, male and lacking social skills — which is the stereotypical image of a hacker presented by the media. No other strong view was apparent from the other 70% of responses, with many respondents giving their opinions of what hackers *do* rather than the type of people they are. With regard to the popularity of the stereotypical image, it should be noted while this is often still the case, the use of hacking skills is no longer the sole province of the lone teenager in his bedroom to whom this image is normally applied. For example, there is evidence to suggest that hacking skills are being applied in organized activities such as information warfare and cyber terrorism [13]. Such activities are beyond the scope of the loner portrayed by the stereotype and suggest that some people need to reappraise their views what hacking may mean in modern society.

The respondents were also asked whether they considered hacking to be acceptable (71% claiming it is not), an invasion of privacy (80% claiming it is) and theft (52% claiming it is). It can be noted from these figures that there are surprisingly large proportions of respondents who did not appear to be taking a negative view of hacker activity. To further determine perceptions of hacking and attitudes towards the hackers, the survey asked for opinions of why people hack, the results of which are shown in *Table 4*.

	Yes	No	Don't Know
Out of curiosity	82%	11%	7%
To make money	62%	21%	17%
For the thrill of it	93%	1%	6%
To 'beat the system'	94%	1%	5%
For malicious reasons	68%	16%	16%

Table 4 : Perceived motivations for hacking

It is interesting to consider in more detail the views of the 29% of respondents who felt that hacking *is* acceptable. Of this group, the views expressed regarding the motivations for hacking were generally benign (i.e. for the thrill of it, out of curiosity and to beat the system). However, more than half of them still considered hacking to represent an invasion of privacy — which seems contradictory to it being acceptable.

The respondents were asked whether they considered that acting via a computer was likely to make the hackers feel less responsible for their actions. The basis for this is that it is often conjectured that many hackers would not contemplate undertaking analogous activities in the real world to those that they undertake online. The general opinion of the respondents was that this is the case, with 61% giving a positive response (23% did not agree, whilst the remaining 16% were unsure). In reality, however, it can be noted that hardcore hackers have no qualms about committing physical theft or breaking and entering in order to assist them in their hacking endeavours [14,15].

While the respondent's views on hacking showed that such activities are considered unacceptable, their attitudes towards suitable punishment were not so clear. When asked if confessed or convicted hackers should be allowed to work in the computing field, 59% said they should, with only 25% suggesting they should not. This reaction is generally supported in the IT industry, with security companies employing hackers as consultants to provide an alternative viewpoint when evaluating and implementing security systems. This approach has been taken by a number of large organizations employing Tiger Teams [16] to test security of both IT systems and physical locations. A

similar response was found when the respondents were asked if hackers should be allowed to have a computer at home — again 59% had no problem with this. However, when compared to the responses regarding use of computers in work, a slightly lower proportion (23%) was firmly against the idea of allowing access at home. This viewpoint appears to be counter-intuitive, in that computer access at home would be more likely to be unsupervised and, as such, there is more chance for the hacker to revert to undesirable behaviour.

The generally lenient views of the respondents are in stark contrast to decisions made in publicized hacking cases, where the convicted hackers' access to computing equipment has been severely restricted in both employment and domestic contexts [14,17]. An example of this is the most recent sentence bestowed upon US hacker Kevin Mitnick, which bans him from access to computer hardware and software, and stipulates that the only technology he should be permitted to own to for the three years after his release is a landline telephone. Furthermore, Mitnick will not be permitted to be employed by any company with computers or computer access on its premises [18]. Whilst it can be strongly argued that these restrictions are intended to keep Mitnick out of further trouble, a counter-argument is that they will severely restrict his options for employment (particularly in areas where his IT skills could be applied).

The survey also attempted to assess awareness of relevant legislation. Given that the majority of respondents were expected to be from the UK, the survey targeted two specific acts of parliament; namely the Data Protection Act 1984 [19] and the Computer Misuse Act 1990 [20]. The Data Protection Act is relevant from the perspective of requiring organizations to implement appropriate security to protect the data that they hold, whereas the Computer Misuse Act provides a means for them to deal with people who have breached that security. However, the survey results revealed that awareness of them is variable. While 76% of respondents had heard of the Data Protection Act, an act that has received much publicity, awareness of the Computer Misuse Act was much lower, with only 46% of respondents having heard of it. This raises the question (particularly amongst such an apparently IT literate response base) of how many people realize that computer abuse is actually illegal, as opposed to just being morally or ethically wrong. In the absence of this knowledge, some individuals may more easily enter into abusive activities, whilst victims may not realize that they have a legal recourse.

Incident	Description
Chaos Computer Club	A German hacking group that has been responsible for breaking into (supposedly) secure systems on a worldwide basis.
Kevin Mitnick	A notorious US hacker who has been involved in a range of hacking incidents. At the time of the survey, Mitnick was awaiting trial in relation to his most recent arrest for hacking into more than a dozen organizations, including Fujitsu, Motorola, Air Touch, MCI, Pacific Bell and Sun Microsystems [17].
WarGames	A 1983 Hollywood film in which a teenage hacker almost triggers a nuclear war. Passing reference to the film is frequently made in mass media reports of hackers.
Michelangelo virus	One of the early viruses to gain attention in the mass media (in 1992). The payload of the virus was programmed to activate on Michelangelo's birthday (6th March), affecting both floppy and hard disks.
Friday the 13th virus	Another early virus, which affects .COM files on the target PC and was activated, as the name suggests, if the day was Friday 13th. The virus is now very rare, but it again received media attention when originally introduced, making it potentially memorable to respondents.

Table 5: Publicized computer abuse incidents

Media Influence

In order to gauge the extent of media influence, the respondents were firstly asked to indicate whether they could recall reading or hearing about *any* computer crime incidents in the news. The vast majority (81%) responded positively to this point. To determine the media's role in more detail, the respondents were presented with a list of computer abuse related headings (encompassing people, groups and viruses) and asked to indicate which they had heard of. The majority of the entries referred to issues that would have received media attention several years before the survey. This was considered to represent a good test of the extent to which media reporting left a lasting impression. The five entries listed, and the rationales behind them, are given in *Table 5*.

The results indicating the respondents' awareness are presented in *Figure 2*, which gives a clear indication that the majority of the general public can recall the occurrence or reporting of specific incidents. This, of course, does not given an indication of how accurately the respondents recalled the incidents or the extent to which they understood any technical issues involved. However, it can consequently be surmised that the media does have some success informing the populous on computer abuse issues.

It is clear from the results that virus incidents are the most easily recalled. This is particularly significant in the context of the two virus examples that were mentioned in the question. At the time of the survey, both viruses were already several years old and were no longer active 'in the wild'. In addition, even at the time of their original release, neither had actually caused much damage. As such, the fact that they were still remembered several years later is a testament to the long-term effects of media reporting and, possibly, the extent to which both viruses were originally over-hyped.

The fact that viruses are the most easily remembered class of incident may be attributable to the effects that they can have upon the public at large. Whereas the activities of hackers can be often be dismissed as being 'someone else's problem', the indiscriminate nature of viruses and their potential for direct impact upon an individual causes more people to take notice. Another possible contributor to the high positive response in the survey may be the inclusion of the word 'virus' as part of the incident description. This may have assisted some respondents in classifying and, thereby, recalling the Michelangelo and Friday 13th incidents or it may have prompted them to respond positively simply because they recognized the term virus (even in the latter case, the figures still serve to give a general indication of virus awareness).

With regard to the specific hacking-related incidents listed (i.e. Chaos and Mitnick), the awareness was significantly less than other categories. However, the

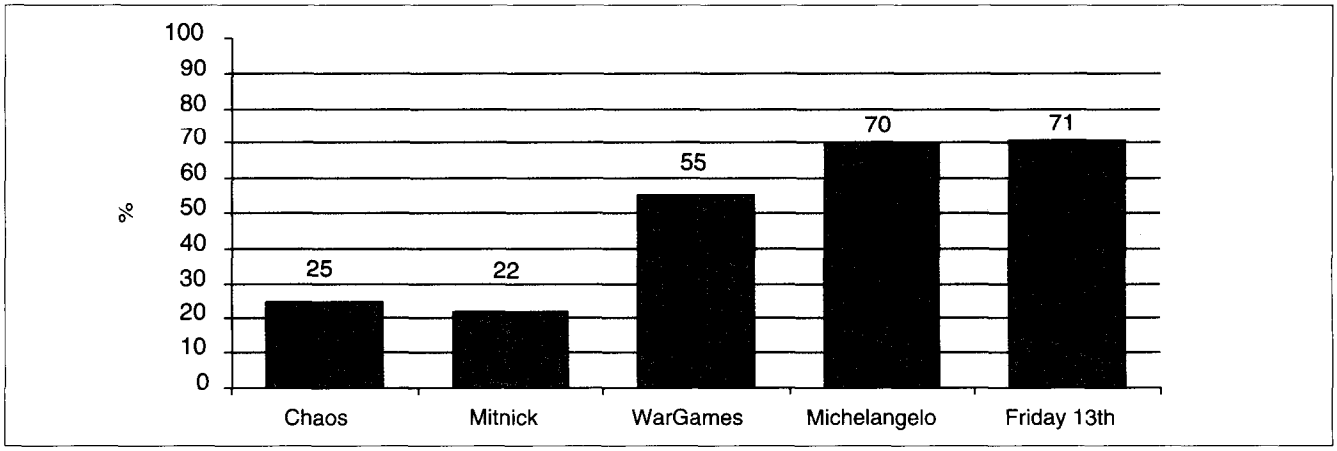

Figure 2: Respondent awareness of specific incidents.

proportions are still considered significant for a number of reasons. Firstly, unlike the virus items, the list presented in the questionnaire did not give any indication to the respondents about who or what the entries might be (i.e. they simply said 'Kevin Mitnick' and 'Chaos Computer Club' and asked for an indication of awareness). Secondly, neither of the cases are directly related to the UK (where most of the survey respondents came from) and, as such, have received little coverage outside the technical press.

When asked to describe their view of the way that the media treats IT crime issues, the respondents' answers were generally critical, with the comment that the media glamorized such cases appearing many times. Many of the respondents also considered that the media trivialized the reporting of computer crime issues, reflecting a perceived distinction between the reporting of 'common' crimes and those that are IT-related.

In the context of the information society (with IT forming a core feature of communication, commerce, leisure and many other activities), the attitude of the mass media towards reporting IT related issues will become more important. If the media continues to glamorize computer crime cases (as some respondents perceived), then public opinion may turn to favour the offenders who could in turn be elevated to celebrity status. In America, Kevin Mitnick has become a household name with rallies held in many cities supporting him [21]. It is possible that the public may be influenced into accepting computer crime as a part of modern life. This could result in a tolerance of computer crime in much the same way that individuals accept that in certain areas, the more common forms of crime occur frequently. Similarly, if those reporting computer crime treat such cases as being regular occurrences, public perception could be adversely affected and the uptake of promising technologies, such as electronic commerce, may suffer.

A Wider View of Media Influence

Public awareness of computer crime and abuse is a double-edged sword. On one side, some level of awareness of issues such as viruses is essential (even amongst domestic users) in order to ensure that appropriate precautions may be taken. On the other side, the focus should not be such that people are scared away altogether (which could easily be the effect upon those who are already uncomfortable with IT).

It is clear from the results that awareness of computer crime amongst the respondents is high and it can be suggested that the media has played a significant role in this. Therefore, in order to better gauge the potential for media influence, a brief investigation was conducted to determine the level to which computer crime and abuse issues are mentioned in the media and the manner in which they are presented. In order to achieve this, the authors performed an electronic search of articles that have appeared in two of the main UK broadsheet newspapers (and their associated Sunday editions) over the last two and a half years. The newspapers in question were *The Times/Sunday Times* and *The Guardian/Observer* and the following search string was applied to the full text of articles:
comput* AND (virus* OR hacker* OR hacking)

This was intended to locate any articles containing the word 'computer' (or a variation), as well as references to either hacking or viruses. The articles retrieved were then manually filtered to remove those that still did not relate to the subjects under investigation. This yielded the results shown in *Figure 3* and it can be seen that, on average, computer crime and abuse issues are mentioned twice a week in each of the newspapers sampled.

It should be noted that these results did not all relate to reports in which hacking or viruses were the headline news, but rather where mention of one or both issues was made in a news-reporting context (which included both main stories and side references to the issues). However, the results are still considered to provide a valid indication of the extent to which computer crime and abuse issues pervade our current society. It is also worth noting that the search would only have trapped reports in which hacking or viruses were mentioned alongside the word 'computer' (which was considered the most likely context and was used to avoid, for example,

the inclusion of stories about medical viruses in the results). As such, other stories relevant to computer crime and abuse (e.g. computer-based frauds) may have gone unnoticed.

Having established the extent of reporting, the other consideration of interest was the manner in which crime and abuse cases were presented. An effective way of assessing this was considered to be via the headline banners of the reports (which are specifically intended to draw reader's attention and are likely to be amongst the best remembered elements of the story). With this in mind, the following list presents examples of some of the headlines identified:

- "Red faces at the Pentagon as hackers drop in on the military" (*The Times*, 4 March 1998)
- "Hackers can cripple Internet in 30 minutes" (*The Times*, 21 May 1998)
- "Virus terrorists plot to upstage millennium bug" (*The Times*, 27 January 1999)
- "E-mail virus sparks world alert" (*The Times*, 31 March 1999)
- "Sabotage by computer hackers costs big business billions" (*The Sunday Times*, 4 April 1999)
- "Hackers from hell cast a wide net to take their revenge on the FBI" (*The Guardian*, 29 May 1999)

It is clear that several of these have a rather sensationalist tone and, indeed, reading the full articles often reveals the headlines to be somewhat misleading. The wisdom of this approach is debatable. On one hand, recalling such strong headlines may help to convince people that they ought to do something about their own security. However, from another perspective, it is likely that they serve to increase people's fear or mistrust of technology. Furthermore, over-glamorized reports may actually serve to encourage other computer abusers, eager to attract themselves a similar level of publicity.

A final observation is that the sample headlines were all taken from broadsheet newspapers. In general terms, these are considered to house more responsible journalism than tabloid publications and it can be assumed that the coverage in the latter (which influence a larger proportion of the population) would have been more sensationalist.

One of the concerns about media treatment of computer crime is that it may influence the public's willingness to adopt new technology such as the Internet. Whilst the survey did not address this issue directly, some related observations can be made. Of the 69 respondents who claimed to have Internet access at home, 63 (i.e. 91%) still expressed very serious concerns about three or more of the issues highlighted in *Table 3*. This suggests that their awareness of computer crime was not a barrier to their use of the Internet and that the benefits were perceived to outweigh the potential risks. However, it can also be noted that people without domestic Internet access expressed a

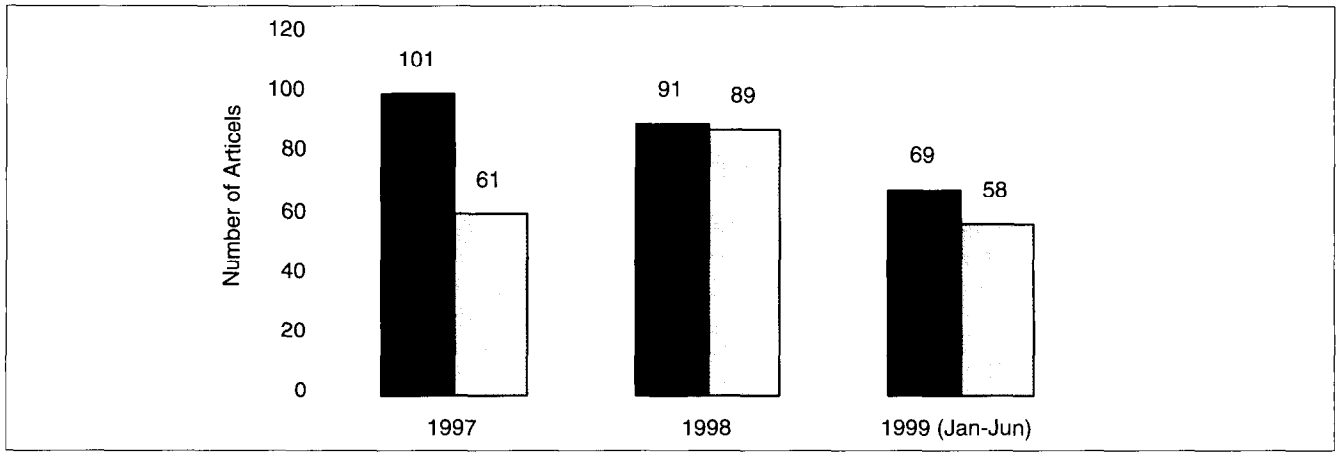

Figure 3: Articles mentioning computer crime and abuse.

similar level of concern over the security issues and it may be conjectured that this may be one of the factors preventing their uptake. However the current survey results do not provide conclusive evidence to support this theory.

Conclusions

Computer crime and abuse represents one of the undesirable, but ultimately inevitable, consequences of the IT and communications revolution. Many sources, this paper included, refer to the new environment that has been ushered in by IT as the Information Society. From the perspective of this discussion, the term 'society' is key — with it should come the realization that, within any sufficiently mature community, a dishonest or disruptive element is highly likely to emerge. Hence, the perceived inevitability of computer-related abuse. Over time it is considered equally inevitable that IT will become even more pervasive and will represent the de facto environment in which many of our activities are conducted, irrespective of the continuing threat of abuse. The continuing adoption and public use of the Internet will be a catalyst for this. However, at the present time, we are still in a transitionary period, where alternatives to IT may still be utilized by those who are technophobic or lack confidence in the security of the medium (note: in reality, of course, IT may still underlie many of these activities, but its role is not apparent at the public interface). In this environment, the public awareness of and attitudes towards computer crime and abuse are important issues, as they will affect the ease with which the transition can occur.

While our results suggest that the media has been successful in terms of informing people that computer crime exists and instilling an awareness of the different types of incident, it seems to have done a relatively poor job of raising awareness of the possible corrective actions. This is illustrated by the relatively low awareness of the Computer Misuse Act when compared to general awareness of computer misuse. In this sense, it can be considered that media reports are not performing such a useful service as might otherwise be the case and they are likely to have a scaremongering effect upon those who are less familiar with the area. The need for a responsible and informed approach by the media is, therefore, evident.

References

[1] McCullagh, D. and Glave, J. 1999. "Hotmail Accounts Exposed to All", Wired News, 30 August 1999. http://www.wired.com/news/news/business/story/21490.html

[2] Garber, L. 1999. "Melissa virus creates a new type of threat", *Computer*, vol. 32, No. 6. 16-19.

[3] Audit Commission. 1990. *Survey of Computer Fraud & Abuse*, Audit Commission Publications, UK.

[4] Audit Commission. 1994. *Opportunity Makes a Thief*, Audit Commission Publications, UK. ISBN 0-11-886137-9.

[5] Audit Commission. 1998. *Ghost in the Machine – An Analysis of IT Fraud and Abuse*, Audit Commission Publications, UK, ISBN 1-86240-056-3.

[6] CSI. 1999. "Issues and Trends: 1999 CSI/FBI Computer Crime and Security Survey", CSI, USA, March 1999.

[7] Nycum, S.H. and Parker, D.B. 1990. "Prosecutorial experience with state computer crime laws in the United States", in *Security and Protection in Information Systems*, A.Grissonnanche (Ed.), Elsevier Science Publishers B.V., North-Holland: 307-319.

[8] KPMG. 1998. "Information Security Survey 1998", KPMG Information Risk Management, UK. http://www.kpmg.co.uk

[9] Rushe, D. 1999. "Digital television steals march on home shopping rivals", *The Sunday Times*, Business Supplement, 5 September 1999: 4.

[10] ICM. 1999. "ICM Poll – The Internet – January 1999", ICM Research. http://www.icmresearch.co.uk/reviews/1999/internet-99-jan.htm

[11] *Secure Computing*. 1999. "BSA Warns of Crackdown", Secure Computing, UK, January 1999.

[12] Jobusch, D.L. and Oldehoeft, A.E. 1989. "A Survey of Password Mechanisms: Part 1", *Computers & Security*, Vol. 8, No. 7: 587-604.

[13] Furnell, S. and Warren, M. 1999. "Computer Hacking and Cyber Terrorism: The real threats in the new millenium?", *Computers & Security*, vol. 18, issue 1: 28-34.

[14] Littman J. 1997. *The Watchman — The Twisted Life and Crimes of Serial Hacker Kevin Poulsen*, Little, Brown & Company Limited. ISBN 0-316-52857-9.

[15] Hafner, K and Markoff, J. 1991. *Cyberpunk: Outlaws and Hackers on the Computer Frontier.* Fourth Estate Limited.

[16] O'Neill, B. 1998. "Computing and the Net: Hackers for hire", *The Guardian*, 26 February 1998: 5.

[17] Littman J. 1996. *The Fugitive Game — online with Kevin Mitnick*, Little, Brown & Company Limited. ISBN 0-316-52858-7.

[18] Thomas, D. 1999. "Mitnick Could Go Free in January", Wired News, 10 August 1999. http://www.wired.com/news/news/politics/story/21197.html

[19] HMSO. 1984. *Data Protection Act 1984*, Her majesty's Stationary Office, UK.

[20] HMSO. 1990. *Computer Misuse Act 1990*, Her majesty's Stationary Office, UK.

[21] Sprenger P. 1999. "Pro-Mitnick Demos in US, Russia", Wired News, 5 June 1999. http://www.wired.com/news/news/politics/story/20053.html