The Insider Misuse Threat Survey: Investigating IT misuse from legitimate users

G.B.Magklaras and S.M.Furnell
Network Research Group, School of Computing, Communications and Electronics,
University of Plymouth, Plymouth, United Kingdom.
nrg@plymouth.ac.uk

Abstract

The majority of computer security methods tend to focus upon the detection and prevention of security incidents of external origin. However, a number of surveys and media reports indicate the dangers of legitimate user misuse of IT resources, a separate category of computer security incidents with serious consequences for the integrity, privacy and availability of computer systems and networks. After the discussion of some basic terminology, accompanied by relevant case studies, the paper explores the problem of insider IT misuse by analyzing the results of a survey that specifically examines the issue. The results revealed that insider misuse is a significant problem – both in terms of the volume of incidents and their consequent impacts upon the organizations concerned. The findings also suggested characteristics that may help to profile insider IT misuse, and hence develop more efficient tools for the mitigation of insider threat.

Keywords

Insider misuse, Insider threat, Misuse profiling, Survey.

INTRODUCTION

On 19 March 2000, the system administrators of Internet Trading Systems (ITS) Incorporation faced an unprecedented Denial of Service attack on their IT infrastructure (Radcliff 2000). The attack paralyzed the company's on-line trading system for almost three days resulting in serious revenue losses, until investigators found the attacker. Abdelkader Smires, their previous chief software engineer had employment differences with his managers. He thought that he was underpaid and requested a pay rise coupled with a range of additional benefits. When his requests were turned down, he decided to take revenge by using the computers of his previous employer (Queens College), after leaving Internet Trading Systems.

The 2001 CSI/FBI survey (CSI 2001) cited the case of Robert Hanssen, a 56 year-old FBI veteran. Hanssen abused his trusted access to the FBI Automated Case Support System that contained classified information about ongoing investigations and handed critical information to Russian agencies. In return, he was receiving large sums of money, inflicting a great deal of damage upon the prestigious image of the Federal Bureau of Investigation and the national security of his country. Nobody could imagine that a church-going and patriotic family man was betraying his country for money.

The previous scenarios were not derived by a Hollywood movie scenario writer, but they represent examples of real world events that have many things in common. Apart from their serious consequences (loss of business revenue, invaluable loss of national security information), the malicious acts were performed by people that had access rights to computer equipment, trust and more importantly excellent knowledge of the IT infrastructure.

Smires had legitimate accounts on Queens College computer systems. In addition, as an ex-member of staff and key designer of ITS's on-line trading system, he knew very well the weaknesses of the various system components prior launching the attack. Robert Hanssen also enjoyed unlimited access privileges to FBI's Automated Case Report System. In addition, he was an expert in the process of hiding the information he unlawfully acquired, by employing specially formatted floppy disks (Pluta 2001). At a first glance, the floppy disks appeared to be empty or containing legitimate information. However a closer examination by FBI Computer Forensics Specialists revealed they contained the illegitimate material that Hanssen had hidden in the very last track of 40-track formatted storage media. This track was not employed to store filesystem data by convention and hence the technique was a sophisticated way to hide information.

Both of the aforementioned case studies help one start shaping the picture of an insider as a person that has been *legitimately* given the capability of accessing one or many components of the IT infrastructure. The word 'legitimately' has been emphasized because it indicates the main difference between an insider and an external cracker. An insider should always be able to have at least a point of entry in one or more computer systems. The implication of this is that an insider does not usually need to consume as much time and effort to obtain additional privileges as an external cracker does. One can also infer that an insider is less likely to get caught by implemented security measures because of the level of trust that he enjoys. Lastly, it is not unusual for an insider to have intermediate to excellent knowledge of an organization's IT infrastructure. Thus a knowledgeable legitimate user might achieve a successful data security breach by means of consuming less effort than a traditional external cracker.

The other side of the 'insider IT misuse' problem relates to what can be considered as misuse activity. Although the great majority of the people are familiar with the generic meaning of the word 'misuse' (use something in a wrong way or for the wrong purpose), when we try to map it to an IT context, there is a need to clarify certain issues. Insider IT misuse can be a very subjective term. In fact, one of the most challenging tasks is to draw a clear line that separates an IT misuser from a person that uses the available resources in an acceptable way and for an approved purpose. The words 'acceptable' and 'approved' imply the presence of rules that qualify (or quantify) conditions of allowable usage for the resources concerned. These rules are often embodied within an IT usage policy. Part of this organisation-wide policy is the information security policy, defined as the 'set of laws, rules, practices, norms and fashions that regulate how an organisation manages, protects, and distributes the sensitive information and that regulates how an organisation protects system services' (Caelli et al. 1991).

In order to mitigate the insider threat in IT systems, security surveys have verified the presence of the problem and computer security researchers have produced a number of insider threat mitigation frameworks.

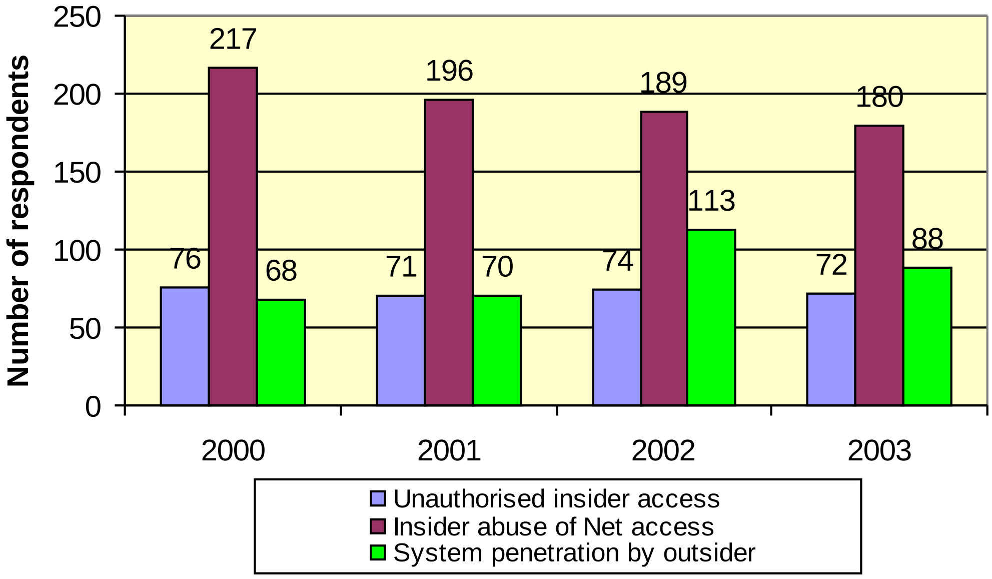

Figure 1: Respondents reporting internal and external incidents (Richardson 2003)

One of the most commonly cited recent surveys, the CSI/FBI 2003 Computer Crime and Security Survey (Richardson 2003) provides a concise picture about the impact of insider misuse in IT infrastructures (Figure 1). Amongst many types of security breaches, the survey quantified the frequency of reporting for three generic types of incidents. The category of 'Insider abuse of Net access' included improper usage of the Internet connection by legitimate users (downloading of inappropriate material, use of the World Wide Web for non-work related purposes to name a few), whereas 'Unauthorised insider access' focused on improper access to sensitive data by insiders. It is clear from the graph that the volume of reported insider incidents considerably outweighs the number of external-sourced penetrations ('System penetration by outsider').

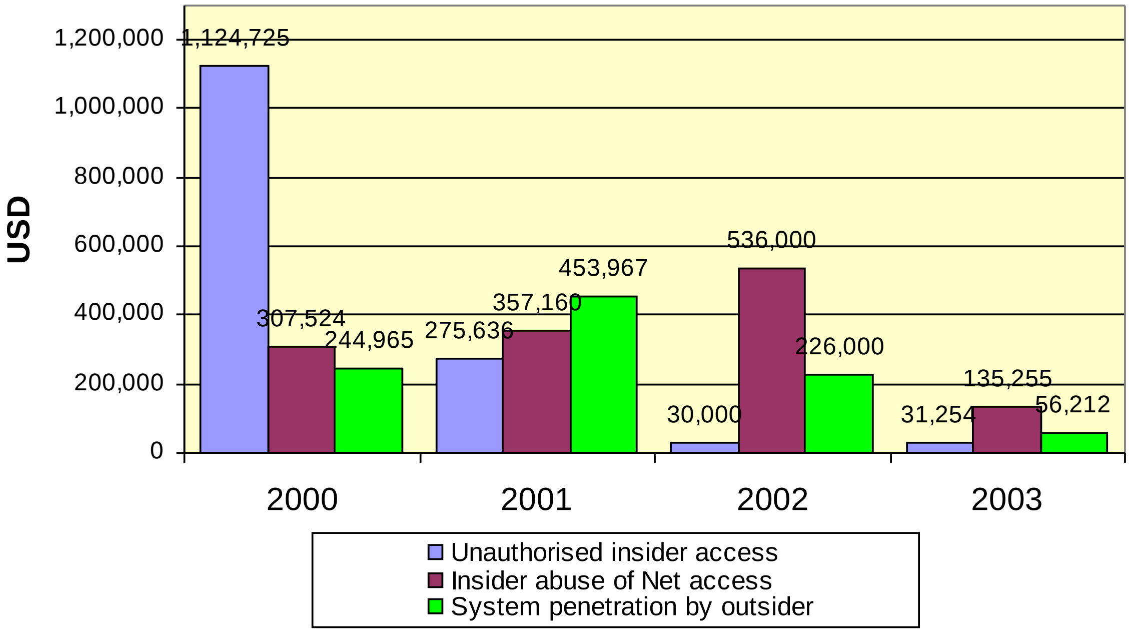

Figure 2: Average annual losses of insider and external incidents (Richardson 2003)

Continuing this comparison, the CSI/FBI results also present a breakdown of the associated costs arising from the incidents (Figure 2), which clearly indicate that losses resulting from misuse by legitimate users are often substantially more than those related to external incidents. This gives a clear indication that insider attacks are important threats that need to be addressed to safeguard the health of IT infrastructures.

More recently, the British Department of Trade and Industry (DTI), in association with PriceWaterhouseCoopers (PWC), published survey results suggesting that insider misuse has doubled since 2002, mainly driven by the increased adoption of World Wide Web and Internet related technologies (DTI 2004). Approximately a third of the DTI/PWC 2004 respondents claimed that their worst security incident was internal. This is clearly another verification of the existence of internal security threats.

However, the generic focus of the previously mentioned surveys does not answer crucial questions about the insider IT misuse problem:

- Are legitimate user incidents more frequent than external hacking attacks? Is the first type of incident more serious than the latter one?
- What really constitutes an insider IT misuse problem? What are the most frequent ways for a legitimate user to abuse an IT infrastructure?
- What are the most likely places in computer systems to collect information about legitimate user misuse?
- Is there any indicative information about what kind of user is likely to initiate an insider IT misuse incident?

These questions can be addressed by a survey that focuses more specifically upon legitimate user misuse incidents. The results of such a survey are the main focus of this paper.

THE INSIDER MISUSE SURVEY

The 'Insider IT misuse' survey ran for approximately nine months (August 2001 – April 2002), and the respondents completed the survey via the World Wide Web. The survey targeted various IT professionals (system administrators, IT security specialists, technical managers/CEOs) across Europe, and ultimately collected data from 50 respondents. Although a greater number of participants were originally expected, this sample is still valid as the results display certain clear trends.

The bulk of the participants (70%) came from the UK, with between one and four respondents from a variety of other European countries (i.e. Belgium, France, Germany, Greece, Italy, Netherlands, Norway and Sweden). Figure 3 shows the breakdown of respondents by industry sector. Software and hardware vendors came top of the list (26%), whereas a smaller number of participants originated from 'utilities' and defence companies.

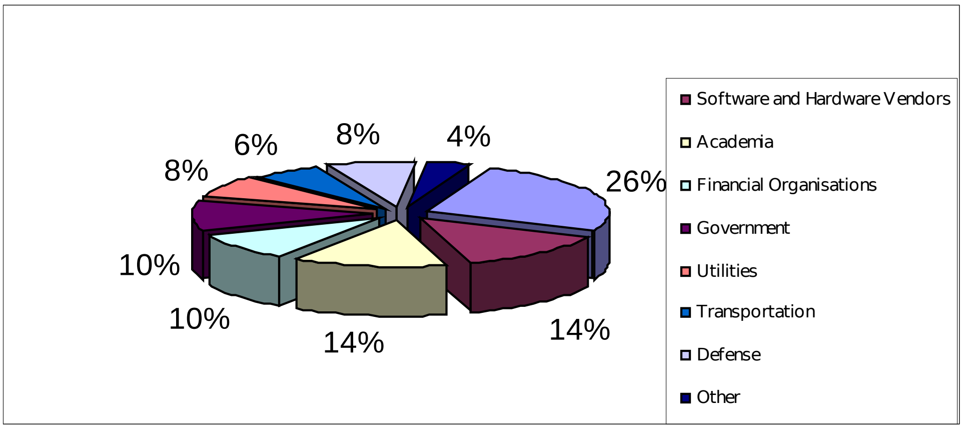

Figure 3: Respondents by industry sector

As shown in Figure 4, the great majority of the questioned IT professionals had a technical background, leaving a margin for non-technical opinions originating from management (Human Resources, Executive Boards). This does not necessarily provide a balance of opinions amongst technical and non-technical respondents. Nevertheless, in an IT infrastructure there is always a direct relationship between what is enforced by technical personnel and the desired information security policy derived by management. Thus, an opinion from management would still be of great value for the respondent sample, especially for information security policy issues.

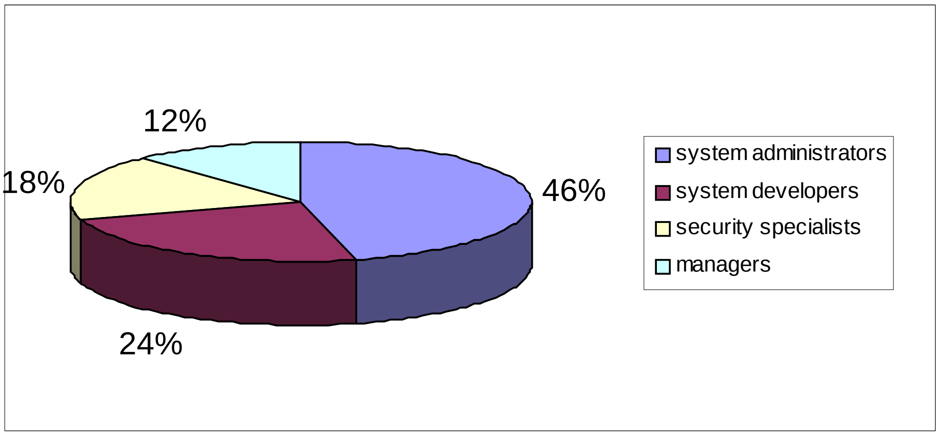

Figure 4: Respondents by profession

One of the main goals of the survey was to reveal the true magnitude of Insider misuse incident occurrence and compare it to that of external misuse activities. The majority of reported incidents appear to have internal origin. Seventy percent of respondents have traced the majority of security incidents back to legitimate users, whereas less than a quarter reported attacks that were mostly related to external activities (Figure 5).

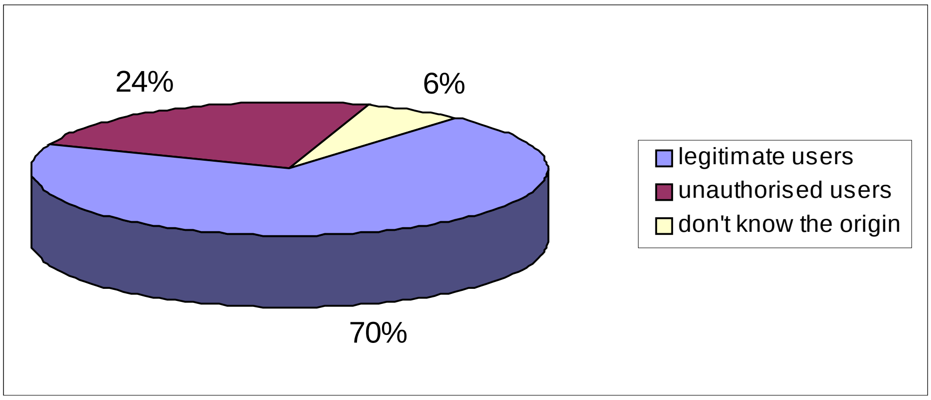

Figure 5: Origin of reported incidents

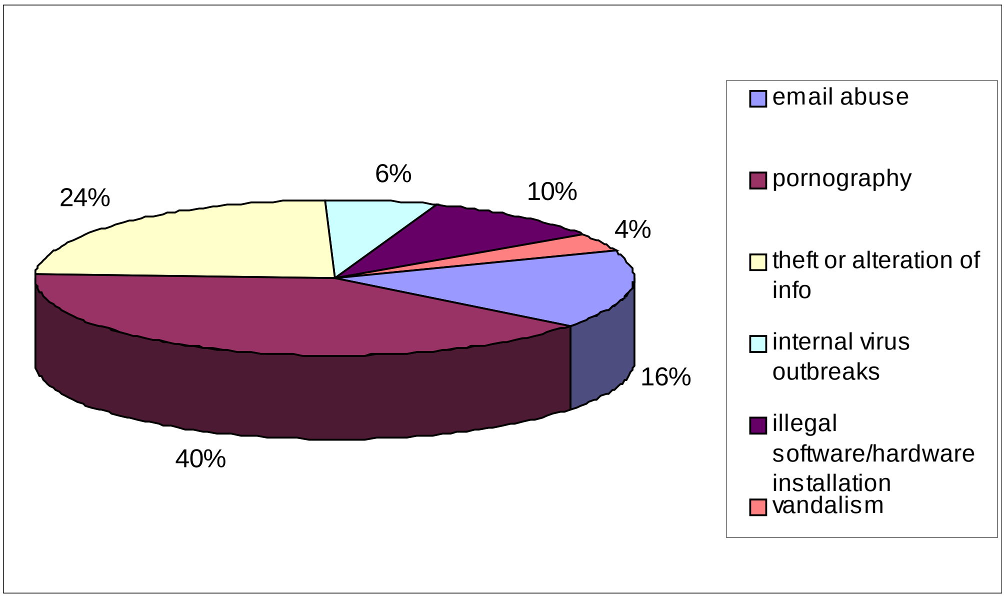

Figure 6: Most frequent types of insider IT misuse

Forty percent of the respondents considered the storage and dissemination of pornographic material on computer equipment as the most frequent type of legitimate user misuse. This was followed by 12 reported cases of theft or fraudulent alteration of proprietary and commercially sensitive information (24%), whereas e-mail abuse was the third most common type, accounting for 16% of the reported cases. Internal virus outbreaks (two incidents were recorded of which one of them was classified as an intentional one), physical destruction of computer equipment (vandalism) and installation of illegal (unauthorised or pirate software packages) were encountered less often, and accounted for the remaining 20% of the insider incidents.

Although the previous statistics give an impression of the range of organizations affected by insider incidents, it does not necessarily reveal their true consequences for the respondents. In addition to the frequency of occurrence, one has to consider the financial consequences resulting from these types of cases. Figures 7 and 8 illustrate the reported substantial revenue loss for incidents of internal and external origin respectively. It should be noted that what is represented here does not constitute information based on stated sums of money. The figures represent the statistics of how many respondents admitted substantial revenue loss. A total of 34% (12 out of 35) of the respondents that have faced mostly internal security incidents reported serious revenue loss. The percentage is marginally equal to the respective figures for substantial revenue loss for a majority of external misuse incidents (33%, or 4 out of 12), although the reported number of external cases was smaller than the internal ones.

More useful conclusions could be deducted if the reported lost revenue was quantified in relation to the annual turnover of the organizations. Someone could then compare properly the financial impact of external versus internal incidents. Unfortunately, although the survey asked the respondents to (optionally) disclose an estimate of their lost revenue, only four out of the fifty respondents chose to do so, and thus there is insufficient data for discovering trends and publishing useful information from this aspect.

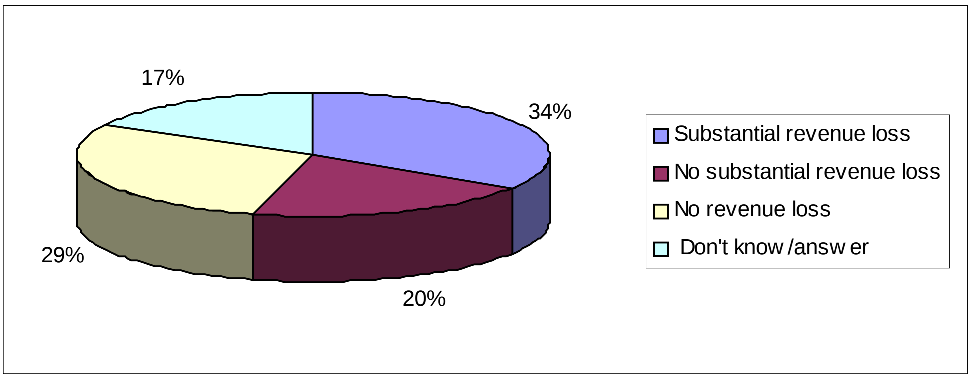

Figure 7: Revenue loss from insider misuse

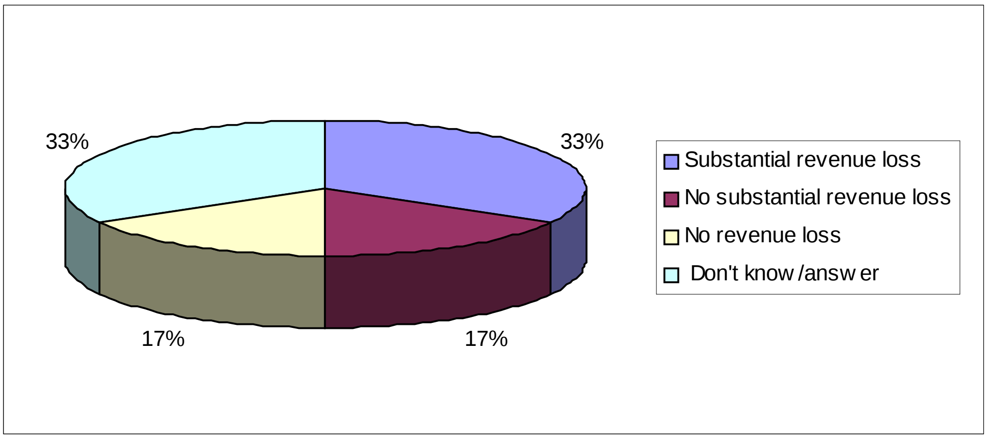

Figure 8: Revenue loss from external incidents

The survey also focused upon another important aspect of tackling the insider misuse problem: that of discovering the generic characteristics of a legitimate user that misuses a system. The introductory section of the paper discussed the subjective nature of the insider misuse problem in relation to the various different IT security policies. An important characteristic of the problem is to show which things could be considered as misuse acts amongst the various IT sectors.

Lost productivity from unauthorized use of computing resources during office hours (e.g. general Internet browsing, computer game playing), has been a well-documented concern for many organizations (Pruitt 2001). The survey results clearly reflected this problem, with 46% of respondents considering the extensive unauthorized usage of computer resources for non-job related purposes to be a misuse act under their IT usage policy. Those respondents came mainly from commercial organizations, where efficient revenue generation is a primary concern.

Another popular category of classified internal misuse acts is the load that they impose on IT infrastructures. Employees tend to sometimes overuse these resources (even when they employ them for work-related purposes) causing a variety of administrative issues that could potentially result in service degradation or failure. Excessive usage of hard disk space and network bandwidth are two great examples that have forced system administrators to use mechanisms such as disk quotas (Indiana University 1997) and network bandwidth shaping techniques (Stolarz 2001). The earlier is a result of the ever increasing storage needs of users, whereas the latter a consequence of the usage of many Peer-to-Peer (P2P) applications. Forty four percent of respondents have identified excessive resource utilization as a misuse act against their IT infrastructure. The available data showed no distinct pattern that could relate this classification to a particular type of organization. However, most of the respondents that considered excessive resource usage as a misuse act had an IT infrastructure consisting of at least 500 hosts. Therefore, it is safe to conclude that insiders are more likely to get penalized in large IT environments, where the impact of resource over-utilization becomes more apparent.

Finally, the majority of the respondents (76%) claimed that an attempt to install one or more unauthorized applications is also classified as a misuse act for their organizations. This could be used as a strong criterion for the purposes of gauging insider threats in an IT environment.

Although previous paragraphs have shown the variability of what normally constitutes an IT misuse act amongst the various IT organizations, there are also notable generic traits for the profile of an insider. In particular, 86% of the respondents believe that sophisticated (in terms of IT system knowledge) users are more likely to misuse an IT infrastructure than less knowledgeable users.

In response to the question "*If you were designing a security pre-employment screening procedure for candidate employees, what would you think is the most important piece of information that should be included in the screening policy?*", 40% of the respondents chose the verification of the reasons for leaving previous employment as the most important parameter. The verification of the knowledge of IT security skills, previous credit difficulties as well as the existence of previous criminal conviction records, were also chosen as most important parameters at a smaller scale, as shown in Figure 9.

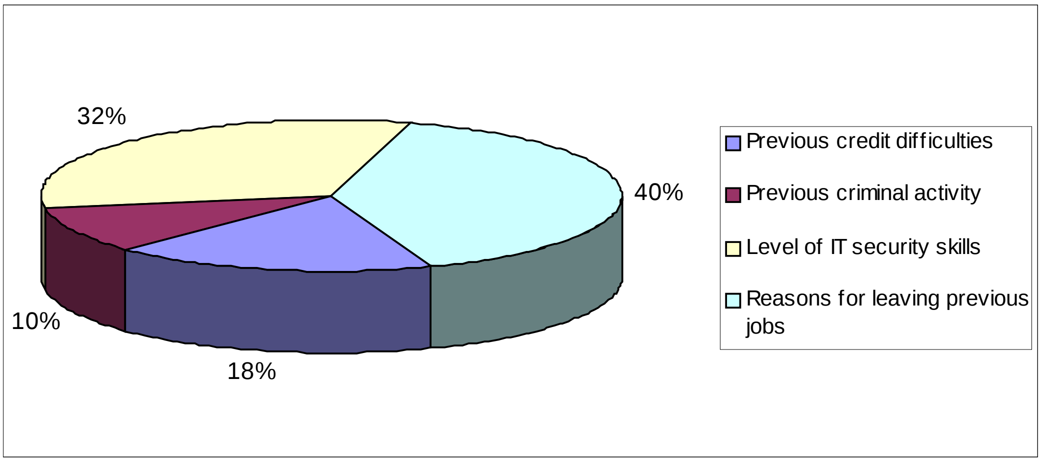

Figure 9: Important security pre-employment procedure parameters (the insider's past)

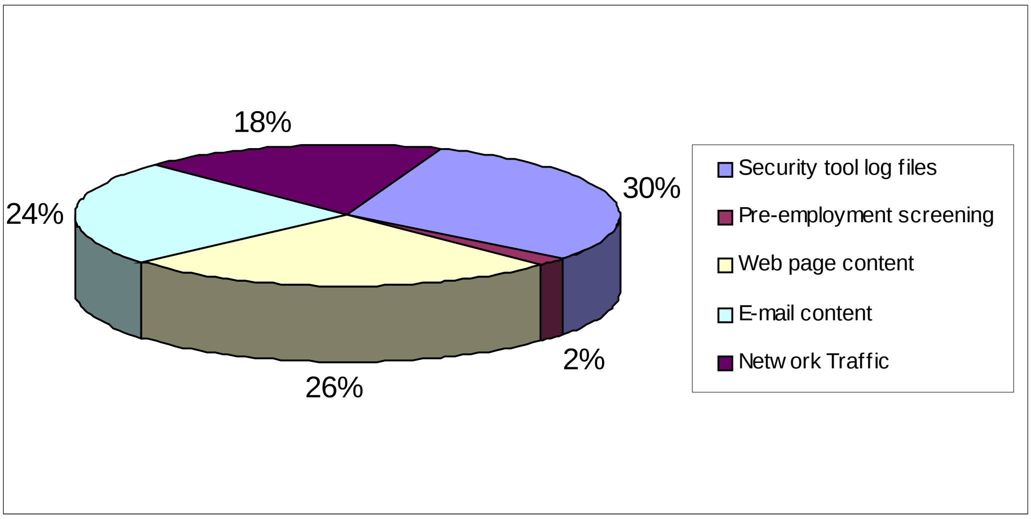

Figure 10: Most indicative source for tracing insider misuse incidents

A final point provides a useful technical insight on how the insider misuse acts could be traced accurately and conveniently (in terms of technical feasibility) in an IT infrastructure. As shown in Figure 10, most respondents flag the examination of bespoke security tool log files as the most reliable way of tracing back the origins of an internal misuse act. However, as the chart shows, several other methods are also considered to offer strong potential. Notably, the questionnaire had also offered OS log files as an option. However, all of the respondents turned down that option, and that was expected. If external entities have the ability to cover their trails by using special audit log modification software, this would certainly be achievable by an insider whose access to the OS log files might be given by default or might be easier to obtain.

CONCLUSION

Despite the small number of respondents, the statistics of the insider misuse survey have clearly shown notable trends, in order to establish a profile of the legitimate employee that misuses certain elements of the IT infrastructure. The results were derived by examining the opinions of mostly technical personnel.

The fact that 70% of respondents traced the majority of their security incidents back to internal origins reveals that the insider IT misuse problem is certainly a well-established threat factor for the health of computing environments. However, due to the relatively small number of respondents, and the fact that the thematic area of the survey was biased towards insider misuse, it is not safe to assume that the survey's majority of insider incidents can be considered a statistically safe result.

The survey did not intend to prove (or disprove) the conventional wisdom of some information security surveys, which dictates that most security incidents occur from legitimate users. The CSI/FBI 2001 survey (CSI 2001) contains some notable comments about the value of these opinions by Eugene Schultz: "I would like to add that any statistics concerning security related incidents should not be taken at face value…". Moreover, the DTI/PWC survey report (DTI 2004) mentions that: "… They [surveys] also tend to be biased towards larger and more security-aware organizations…". Both of these statements indicate that the goal of an information security survey is to reveal broad incident trends, not make warranties about absolute numbers validated by accurate statistics. Nevertheless, some parallels can be drawn between the insider misuse survey and the aforementioned generic studies. These parallels can be used to verify the validity of some trends that could be used to form the portrait of an insider.

The insider misuse survey concluded that the three most serious types of misuse were the downloading of pornographic material, the abuse of email resources, and the theft or malicious alteration of data (Figure 6). In direct comparison, the DTI/PWC 2004 survey highlights the incidents of web browsing misuse, misuse of email, and unauthorized access to systems or data as the major system misuse categories.

It is really difficult to compare classes of incidents amongst different surveys, due to the different scope of the incident categories. The 'Web browsing misuse' category of the DTI/PWC 2004 survey can include the downloading of pornographic material and other unauthorized use of the web facility, mainly for non work related purposes, as highlighted by the insider misuse survey. The same can be said about the DTI/PWC 'email abuse category'. Although the insider sisuse survey considered activities such as spamming, or the use of email for abuse or defamatory purposes, the scope of the DTI/PWC email abuse definition was broader including email utilization for personal purposes, resulting in lost productivity. Nevertheless, the two surveys highlighted three of the most common problem areas in slightly different order.

Another notable similarity between the authors' survey and the DTI/PWC findings is the emphasis upon staff security checks during the recruiting process. Figure 9 indicated that all of the surveyed professionals indicated some preference towards the existence of certain pre-employment security checks for prospective employees. The DTI/PWC indicated that the majority (66%) of the respondents usually perform some sort of security check during the recruiting stage. The DTI/PWC survey comments that the absence of these security checks from company procedures is clearly a serious omission.

Finally, the profile of an insider threat was also refined by indicating that sophisticated users are more likely to misuse an IT infrastructure than less IT-literate user. Specialized data security tool logs, as well as web and email content were the most useful sources of Insider IT Misuse according to the perception of the respondents. This provides an overview of where technical specialists are likely to focus their efforts, in order to mitigate the problem of IT misuse.

REFERENCES

Caelli W., Longley D., Shain M. (1991) *Information Security Handbook*, Stockton Press.

CSI. (2001) "2001 CSI/FBI Computer Crime and Security Survey", Computer Security Issues & Trends, Vol. VII, No1.

DTI. 2004. Information Security Breaches Survey 2004. Department of Trade & Industry, April 2004. URN 04/617.

Indiana University. (1997) "Unix Workstation System Administration Education Certification Course", Indiana University Unix System Support Group, URL http://www.ussg.iu.edu/edcert/session2/disk/diskspace.html, Accessed 31 July 2004.

Pruitt, S. (2001) "Are employees wasting time on-line?", PC World Internet portal, 2 August 2001, URL http://www.pcworld.com/news/article/0,aid,56947,00.asp, Accessed 31 July 2004.

Radcliff, D. (2000) "The Cyber-Mod Squad Sets Out After Crackers", Computerworld, 19 June 2000, URL: http://www.computerworld.com/news/2000/story/0,11280,45927,00.html, Accessed 31 July 2004.

Richardson, R. (2003) *2003 CSI/FBI Computer Crime and Security Survey*. Computer Security Institute. Spring 2003.

Stolarz, D. (2001) "System-and Network-wide bandwidth shaping for P2P apps", , O'Reilly Developer Weblogs, 6 August 2001, URL http://www.oreillynet.com/pub/wlg/549, Accessed 31 July 2004.

Pluta, S.A. (2001) *United States of America v. Robert Philip Hanssen - Affidavit in Support of Criminal Complaint, Arrest Warrant and Search Warrants*, United States District Court for the Eastern District of Virginia – Alexandria Division, February 2001, URL http://news.findlaw.com/cnn/docs/hanssen/hanssenaff022001.pdf, Accessed 31 July 2004.

COPYRIGHT