Assessing IT Security Culture: System Administrator and End-User Perspectives

John Finch, **Steven Furnell** and **Paul Dowland**

Network Research Group, University of Plymouth, Plymouth, United Kingdom
info@network-research-group.org

Abstract

Appropriate understanding and acceptance of IT security should now be regarded as an essential requirement within any modern business. Although a number of previous studies have been published that assess organizational attitudes, the respondents have typically been IT administrators or top-level managers, without any representation from the end-user community. As such, a genuine view of security attitudes and practices within the companies as a whole may not have been obtained. To this end, this paper presents the results of an investigation targeting both system administrators and a selection of end-users from a number of companies of varying sizes. Although the survey results did not reveal significant differences in the responses obtained from large companies versus small businesses, there was a marked contrast between some of the administrator perceptions and those of the end-users. These findings suggest a requirement for improved awareness and education within such organizations, in order to ensure that security is appropriately understood and accepted at all levels.

Keywords: *Security culture, Security awareness, Survey*

Introduction

In recent years, a number of notable national studies have been published that have assessed security practices and awareness in organizational contexts. For example, surveys from the Department of Trade & Industry in the UK, and the Computer Security Institute in the United States have presented highly publicized findings relating to organizational attitudes towards security, and the problems that they have faced (DTI 2002; Power 2002).

In many respects, the results from these surveys were hardly encouraging, indicating that organizations had suffered significant breaches and consequently needed to be doing more to protect themselves. However, it is quite possible that the reality of the situation, in terms of the true level of security awareness and compliance within our organizations, may be even worse than these survey findings suggested. The basis for this argument is that the respondents in the previous surveys were typically individuals such as IT managers and security officers (i.e. those persons with the day to day responsibility for dealing with security within their company). Although, in one sense, this would have enabled an accurate view to be obtained about how security was viewed from a corporate perspective, it would not necessarily have given a true picture of how seriously the issue was considered at ground level amongst end users. The fact that the previous respondents were largely those people responsible for setting up and running any technical security initiatives raises the question of whether their views were likely to be representative of the organization at large. For example, even though an IT administrator might indicate that there is a formal security policy for the system, this does not necessarily mean that the end-users take any notice of it.

This paper describes a small-scale investigation that was conducted by the authors in order to determine whether such discrepancies existed in practice. The investigation involved the distribution of security awareness questionnaires to administration staff and end users within a number of willing companies. The remainder of the paper describes the survey method that was employed, followed by a discussion of the results observed.

Survey Methodology

In order to enable separate opinions to be gathered from the two target groups, the survey exercise was conducted in two stages, addressing system administrators and end users respectively. The questionnaire given to system administrators was four pages long, and contained detailed questions about their organization's IT infrastructure and its associated security. There were a total of 44 main questions, structured in five main sections, the objectives of which are described below.

A. Infrastructure
This section concerned the IT infrastructure of the company being surveyed, in terms of operating systems, size of network, Internet connectivity and network services utilised.

B. Access to systems
A series of questions assessed how authentication had been addressed in company systems. Specific focus was given to this issue because it was one that end-users would also have a guaranteed ability to comment upon. The intention was to enable a comparison to be drawn between the administrator's perceptions of what happened and the practical reality amongst users.

C. Company security
This section identified the security measures the company employed, and was intended to enable an assessment of how aware the company was of security issues as a whole. Key issues considered were security policy, perceptions of employee awareness, and use of specific security countermeasures (such as firewalls and anti-virus software).

D. Personal opinions
Questions here attempted to assess the administrator's own awareness of security issues by asking them to indicate knowledge of specific security technologies, and to assess or rank a range of given threats.

E. Expenditure
The final questions attempted to ascertain how much value the company placed on IT security, by considering the amount spent on security measures, and the perceived obstacles to further investment.

The responses to the administrator survey were used to gauge their awareness and establish a baseline expectation for the individual user response for that company. For example if the user said they did not run a virus checker, when the administrator said that it was running, it shows a lack of awareness on the part of the user.

The user questionnaire was significantly simpler than the administrator version, with only 18 core questions. The purpose here was to ascertain user awareness within the same companies as the administrators, and where possible make comparison between the perceptions of the two audiences.

A. Access to systems
This section deals with how they select and use their passwords, addressing in particular the issues of whether they compromise them in any way.

B. Company security
This section assesses user perceptions of issues such as security policy, training and threats within their organization. The core topics here are similar to those addressed in Section C of the administrator survey, and enable the attitudes of the two groups to be compared.

C. Personal opinions
Assessed individual views about security and the threats that might be faced within their company.

A detailed breakdown of the specific questions posed in each of the surveys, and the rationale for their inclusion, can be found in Finch (2002).

In terms of questionnaire distribution, a regional directory of businesses was used to enable appropriate companies to be identified. The rationale of restricting the exercise to companies in the region was to simplify the subsequent task of visiting them individually during later stages of the investigation. A number of further criteria were used to filter the potential candidates, including:

- avoiding industries that would not use a great deal of IT, such as builders or car mechanics;
- avoiding very small companies with only 1 or 2 employees.

This led to a selection of 58 companies of varying size, each of whom was contacted by letter to ask whether they would be willing to participate. Of these, only 13 offered a response of any kind (a 22% response rate), and nine of these were polite rejections for a variety of reasons (e.g. lack of time due to other commitments and unwillingness to discuss security with an outside body). Given that this left only four positive responses, it was considered necessary to cast the net to a wider geographic region in order to get a more credible number of respondents. This yielded a further five respondents, and a sufficient end-user population to facilitate a small-scale survey. Unfortunately, time constraints relating to the overall project within which the survey was being conducted did not permit further organizations to be approached.

Results

In each of the companies surveyed, the intention was to obtain the views from the main system administrator, followed by a sample of the associated end-user community. The exact sample available in each case depended upon the size of the organization, and the number of people that they were willing to permit to participate in the study. Ultimately, as well as one administrator from each company, a total of 50 users were surveyed, and the breakdown of

respondents across the organizations surveyed is presented in Table 1. Unfortunately, Organization I, which had the largest number of employees, did not supply any end-user surveys in time to be included in the final results.

Organization	Type of business	Total employees	End-user respondents
A	Surveyors	3	3
B	Retailer	5	2
C	IT Solutions	13	1
D	Education	24	4
E	Manufacturing	196	14
F	Utility	250	9
G	Finance	250	9
H	Utility	320	8
I	Accountants	500	0
Total			**50**

Table 1 : Respondent organizations (ordered by size)

Administrator survey findings

The majority of firms still use Windows 9x as their main workstation operating system, followed closely by the more secure Windows NT. Common factors amongst all respondents were the use of email for conducting business and allowing employees to access the Internet. In addition, eight of the companies maintained a web presence, with 50% of these allowing live access to corporate databases over the Internet. All of these aspects are indicative of the widespread use and dependence upon Internet access within modern organizations.

From a security perspective, positive common findings were that all respondents run anti-virus software on their systems as a continuous background task, and all maintain backups of their data. Another common factor was the use of passwords as the basis for front-line authentication. However, respondents varied in terms of how frequently these were changed (see Figure 1). Although none of the respondents indicated that passwords were not changed at all, one response did indicate quarterly changes were required (which security guidelines would generally agree is not frequent enough). The administrators who stated that passwords were changed at 'other' frequencies, typically changed them every fortnight.

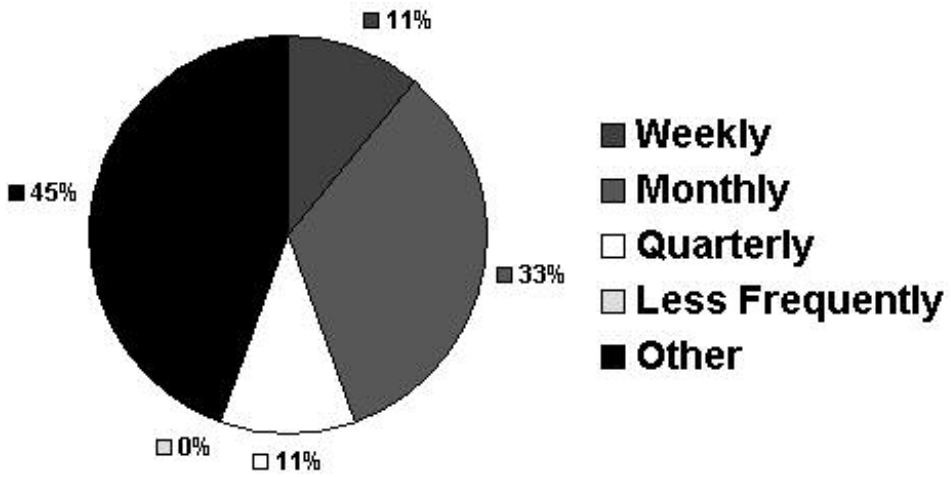

Figure 1 : How often the organizations expect users to change passwords

Two thirds of the companies did not have a format for passwords, leaving the user free to choose anything they like – the potential problem of which was later revealed in the end-user responses. Only two of the companies stored emergency copies of passwords in case they needed when users were unavailable (the copies were held in a safe in both cases). Aside from passwords, two thirds of administrators indicated that they had assessed other methods of entry, but all had found them unsatisfactory to be able to implement in practice.

In terms of security-related policies and procedures, only five out of the nine administrators (55%) claimed to have a formal security policy, while only 44% had a strategy for dealing with an external attack. Further undermining the likelihood of a general security culture, the education of staff in relation to security issues was a low priority, only being conducted by a third of the companies surveyed. None of the companies were BS7799 accredited, and only two had any intention of gaining the accreditation.

Significantly, there was no demonstrable difference between the attitudes of large and small companies in relation to these results. This is one aspect in which the results from this survey can be considered atypical, because in previous published surveys that have drawn a distinction between responses based upon organizational size, the results from small companies have typically indicated a weaker approach towards IT security (DTI 2002). However, the fact that the survey encompassed such a limited number of distinct organizations overall provides a likely explanation for this difference.

When it came to the implementation of security countermeasures, some of the results were more encouraging (see Figure 2). The majority of companies employed the baseline security measures that they were asked about (e.g. file backup), whereas more heavy-duty measures, such as Kerberos and telecommunication encryption, were each employed by only one company. In the case of user access hierarchies, which were only used by six companies, it was notably the three smaller companies in which they were not employed. In other cases, there was no clear distinction on the basis of organizational size.

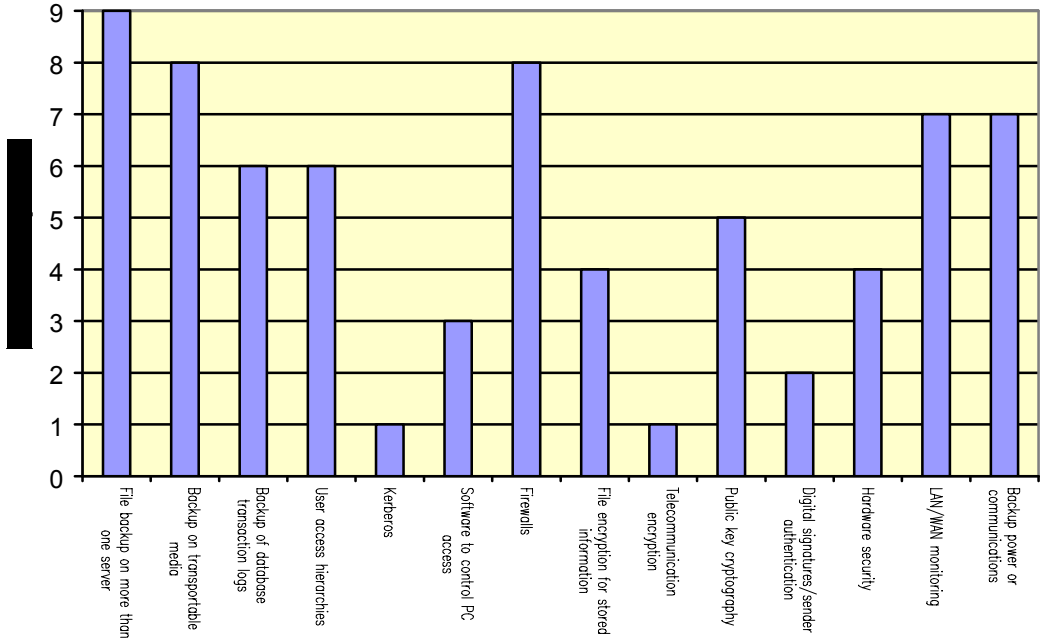

Figure 2 : Security measures employed

In order to enable a rough assessment of their own security awareness, administrators were asked to indicate whether they were aware of six different security-related technologies, as listed in Figure 3. The majority of administrators were aware of all of the genuine options here, with only the SET standard causing difficulties. Two fake acronyms, AKT and CFQ, had been included in the questionnaires in order to assess whether respondents were responding positively simply to appear well informed. Reassuringly, none of the administrators claimed to have heard of these.

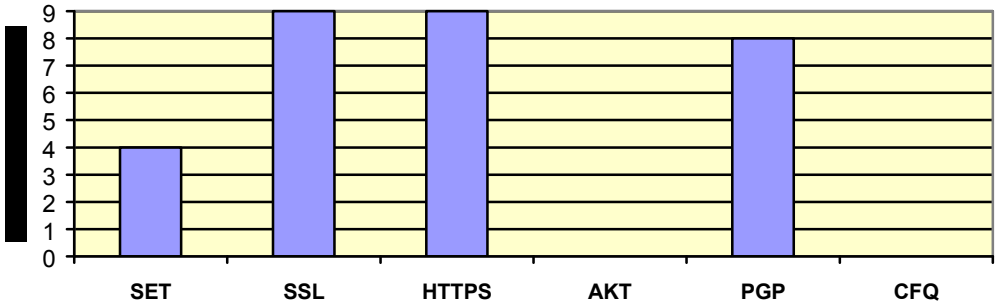

Figure 3 : Awareness of security technologies

Administrators were then asked to rank the significance of a number of security threats, and were presented with a list of options. The results are shown in Table 2, and clearly suggest that employee-related actions are generally considered more problematic than technical security issues. The same question was later posed to end-user respondents, and the contrast between the results can be seen later in Table 3.

Threat	Rank
Employee errors in computer software/hardware use	1
Employee actions that are intentionally harmful	=2
Viruses	=2
Physical theft (e.g. notebook theft)	4
Internet and Intranet connection	5
Harmful intrusion from outside	6

Table 2 : The largest perceived security problems

In terms of the priority afforded to security from a budgetary perspective, all responses suggested that very little is spent on security when compared to the overall budget for IT. As can be seen from Figure 4, two thirds of the respondents claimed that less than 1% of their annual budget was for security, and no-one indicated anything greater than 5%.

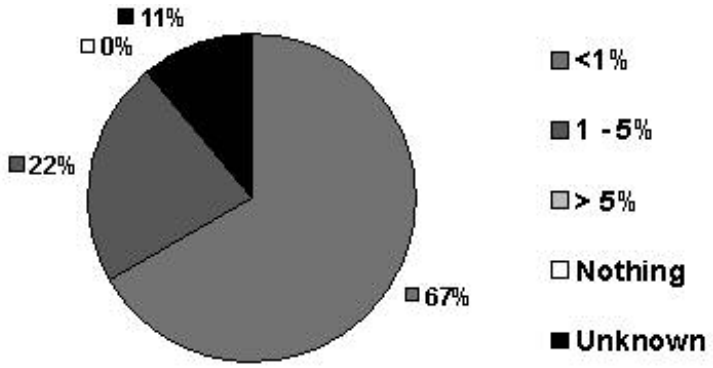

Figure 4 : Security spending as a percentage of total IT budget

The limitations of budget were subsequently cited as a significant factor in hindering the implementation of the IT security policy, with 33% of respondents highlighting this reason. However, a more significant limitation appeared to be senior managers not placing enough importance on the issue. Meanwhile, other obstacles that were offered on the survey as possible options (namely lack of staff and inability to locate appropriate solutions) were not cited by any of the respondents.

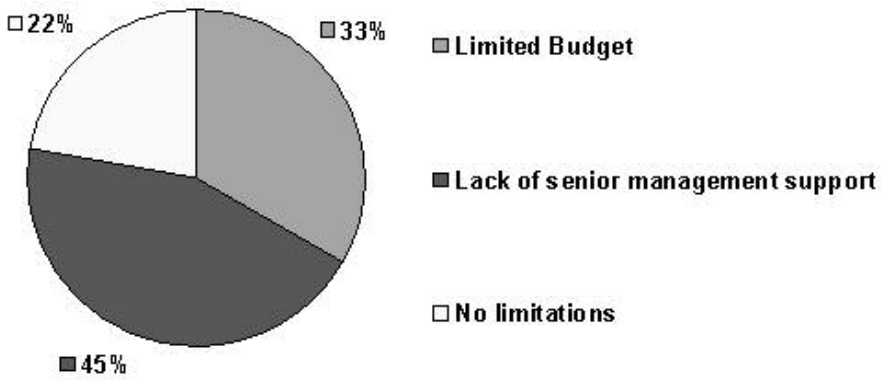

Figure 5 : Obstacles to implementation of security policy

End-user survey findings

After the administrator responses had been collected, the end-user questionnaire was distributed to potential respondents within each of the organizations. As previously indicated in Table 1, a total of 50 responses were received, from all of the companies except Organization I (which was unable to return any results in time due to business pressures).

The first significant issue addressed in the user questionnaire was that of password authentication. Of the 50 end-users surveyed, 21 (42%) admitted using personal information as the basis for their password. Of these, only four people admitted, or realized, that someone else could potentially guess their password as a result – the remainder felt that their password could not be guessed.

After passwords, the next aspect of security that one would instinctively expect users to be aware of is anti-virus software. The administrator responses had established that all of the respondent organizations employed AV software on their systems. However, 12% of end-users were unaware of this. Furthermore, it was questionable whether the message regarding the danger of viruses had really got through to users, as 22% of them admitted that they would open an email attachment even if they were unsure of the source – suggesting that they did not appreciate the potential impact that an infected attachment could have.

The responses in relation to security policy were even more interesting, from the perspective of the contrast that they indicated between user and administrator understanding of the issue. End-users were asked whether they had been required to sign a security policy (see Figure 6). Before presenting the results here, it is relevant to consider that the earlier administrator responses had revealed that four of the companies did not have a formal security policy. What this meant in terms of the end user population was that 34 of the respondents (68%) could not possibly have been asked to sign one, because none existed in their company. However, the actual end-user survey results revealed that, of these 34, six people actually stated that they had signed one. Out of the remaining 16 users (working for companies who did have a policy), 10 of them (62.5%) claimed not to have signed up to a security policy. So, out of 50 users surveyed, only six people had actually had to sign a policy and remembered the fact. Of these six users, only three referred to the policy on a regular basis (equating to 19% of those that had actually signed a security policy, and 6% of the total surveyed). This clearly indicates that merely having a policy and getting users to sign up to it is an inadequate means of ensuring that it will actually mean anything to them. Organizations need to take more proactive steps, such as security education and training (which the earlier administrator results acknowledged was lacking) in order to improve understanding.

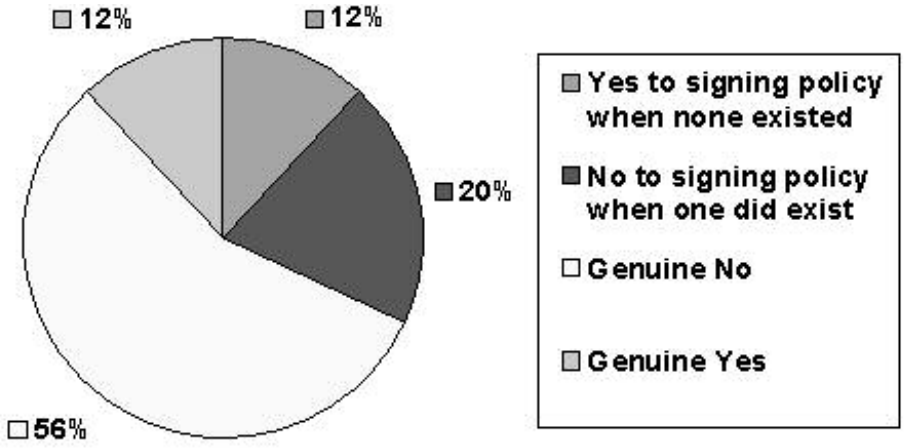

Figure 6 : Users claiming to have signed a security policy

The final significant results from the end-user survey related to their perception of security threats. The participants were presented with the same core list of threats that had been given to administrators, and were similarly asked to rank them according to the perceived danger. Table 3 presents the results of this, with the user rankings set alongside the earlier results observed from administrators, and shows that their perceptions varied dramatically.

Threat	Admin Rank	User Rank
Employee errors in computer software/hardware use	1	4
Viruses	=2	1
Employee actions that are intentionally harmful	=2	2
Physical theft (e.g. notebook theft)	4	6
Internet and Intranet connection	5	5
Harmful intrusion from outside	6	3

Table 3 : Comparison of administrator and user views on threats

It would appear, for example, that end-users are much less aware of the risks that their own accidental errors can pose to system security than they ought to be. The fact that this was the highest ranked problem from the administrator perspective again suggests the need for users to be better educated so that they understand how their actions can unwittingly compromise security. The problems of viruses and intentionally harmful employee actions are given similar recognition by both audiences. The other significant inconsistency related to intrusions from outside (e.g. hackers), which users seemed to presume was a reasonably significant problem, whereas administrator experience clearly suggested otherwise.

Conclusions

This paper has considered the problem of achieving security within modern organizations. Although the survey presented here was clearly limited in terms of the number of respondent organizations, the results provide some interesting indicators, which are worthy of further

consideration and investigation. The most significant point is that a company cannot simply rely on the security message to spread itself. Even where the system administrators felt that appropriate measures had been put in place, there were clear indications from the users that security was not fully understood. This has implications when considering the results of other published surveys, in the sense that their results ought to be regarded as being the likely 'best case' from the respondent companies, rather than being assumed to be generally representative of what the users are actually doing.

Regardless of the disparity between administrators and end-users, the results from the survey suggested that there was clear scope for improvement of security, and associated awareness, within all of the respondent companies. It was, however, notable that awareness was higher in the companies working in more highly regulated domains, which suggests that the issue can be tackled more effectively where there is the legal incentive to do so.

In conclusion, companies have to be more proactive in tackling both security measures and related awareness. The issue of promoting security amongst end-users goes beyond simply having a security policy (although this is a necessary starting point). Ongoing reinforcement of the issue needs to be given more attention.

References

DTI. (2002). Information Security Breaches Survey 2002. Department of Trade & Industry, April 2002. URN 02/318.

Finch, J.W. (2002). Approaches to establishing IT security culture. MSc Thesis. University of Plymouth, Plymouth, United Kingdom.

Power, R. (2002). "2002 CSI/FBI Computer Crime and Security Survey", Computer Security Issues & Trends, vol. VIII, no. 1. Computer Security Institute. Spring 2002.