IMPROVING SECURITY AWARENESS AND TRAINING THROUGH COMPUTER-BASED TRAINING

Steven M Furnell, Alastair G Warren, Paul S Dowland
info@network-research-group.org
Network Research Group,
University of Plymouth,
Drake Circus,
Plymouth,
PL4 8AA,
UK
Tel: +44 1752-233521 Fax: +44 1752-233520

Abstract: Security awareness is a critical issue for all organisations that depend upon information technology. However, significant survey evidence suggests that the issue is often given inadequate attention in modern organisations, leading to problems through security incidents. This paper considers various means that can be used to instil greater awareness, and argues that the most effective method is likely to be via training and awareness programmes. Unfortunately, organisational constraints often preclude the pursuit of such programmes (either in-house or externally) in a traditional manner, and a substitute is needed that can be accessed on-demand, in a self-paced manner. Thus the use of computer-based training is proposed, and the paper discusses the ongoing realisation of an appropriate training tool. The prototype provides an environment that permits the user to explore security problem scenarios, and then select appropriate countermeasures to address the issues identified. It is considered that such an approach would be suitable for promoting day-to-day security awareness for general users, and conducting more specific training for staff with greater security responsibilities.

Key words: Security awareness, Security training, Computer-based training.

1. INTRODUCTION

Although today's society and modern organisations have wholeheartedly adopted the personal computer and the Internet, readily accepting the benefits of such technological advances, the issue of information security has not been so widely adopted, considered, or understood. A major contributing factor here is that many IT users are simply unaware of security in any significant sense. Although they may use baseline technologies such as passwords and anti-virus software, this is often the extent of their awareness of the issue (and it does not even guarantee that these will be used properly). If systems and data are to be appropriately protected, then users at all levels need to be aware of the issues that they are likely to face, as well as what to do about them.

The need for awareness is recognised as one of the main principles of the recently revised Organization for Economic Cooperation and Development (OECD) security guidelines for information systems and networks, which are entitled 'Towards a Culture of Security'. The guidelines state that all participants "should be aware of the need for security of information systems and networks and what they can do to enhance security" (OECD 2002).

This paper examines the problem of security awareness, and presents details of a prototype software tool that is being developed as a means of providing an interactive security training environment for IT users. The next section presents some statistics to illustrate the current lack of security training and awareness in modern businesses. This is followed by a top-level consideration of the means by which security awareness can be promoted in an organisational setting. This leads into the specific issue of security awareness and training programmes, and the discussion of the computer-based tool that the authors' research group is developing.

2. THE PROBLEM OF SECURITY AWARENESS

Although security is often recognised at the business level, it is often found that organisations do not have a full understanding of what they should be doing or how to go about it. The availability and provision of comprehensive security guidelines is not the problem, as appropriate materials can be obtained from a number of sources. The problem is instead one of ensuring that security awareness occurs both in the first instance and as an ongoing factor of an organisation's operation. Indeed, survey results

from recent years have consistently conveyed the impression that security awareness and training programmes are distinctly lacking, as illustrated by the following notable examples:

- The KPMG Information Security Survey back in 1998 indicated that only 31% of respondent organisations had security education and training programmes for their staff (KPMG 1998).

- The results from the Department of Trade & Industry survey in 2002 indicated that only 20% of organisations utilised ongoing training (DTI 2002).

- The 2001 IT Abuse survey from the UK Audit Commission found that only about one third (34%) of organisations have any form of computer security awareness training for their staff (Audit Commission 2001).

- Ernst & Young's Global Information Security Survey 2002 found that less than half of the 459 companies questioned had security training and awareness programmes in place (Ernst & Young 2002).

Having said this, organisations have apparently realised that a lack of security training can usher in significant problems:

- Results published by the UK's National Computing Centre back in 2000 cited the problem of inadequate end user awareness as the most significant obstacle to information security, with over 55% of respondents identifying it as a reason (placing it ahead of issues such as budgetary constraints and technical complexity) (NCC 2000).

- The need for training is underlined by a further statistic from the UK Department of Trade & Industry's 2002 security breaches survey, in which 16% of the 1,000 organisations questioned claimed that a lack of training on security issues had been the reason for the most significant incident in the previous 12 months (DTI 2002).

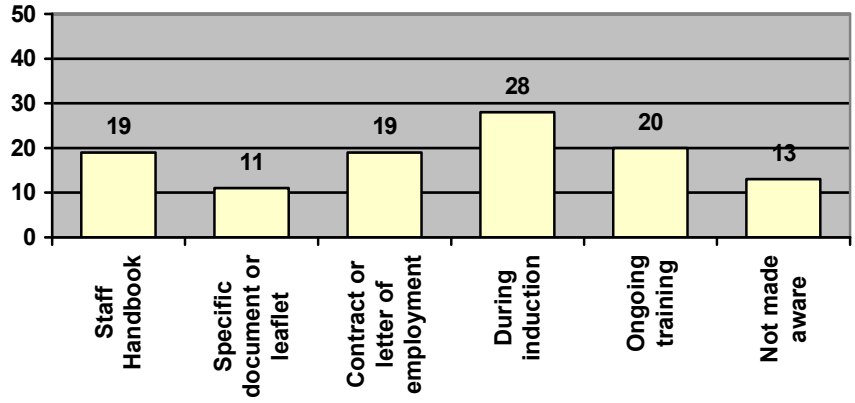
- The aforementioned Ernst & Young survey found that 66% of respondents cited employee awareness as a barrier to achieving effective security (Ernst & Young 2002).

These findings are supported by results from Information Security Magazine's 5th annual industry survey, published in 2002, which suggested that once an installation gets above 100 machines, user awareness becomes the issue with the most impact upon security (Briney and Prince 2002). The findings, which were based upon responses from 215 qualified respondents (filtered from a total of 2,196 responses returned in total), suggested that while the biggest concern in small organisations was preventing intrusions (cited by 44% of associated respondents), all of the other categories cited user awareness of security (scoring 31% in medium organisations, 29% in large, and 42% in very large installations). As such, even though the organisation would seem to have taken a positive step by having specific, named people to look after its security, the practical effect could even be counterproductive because the attention given to it in the environment as a whole is reduced.

With these points in mind, it is relevant to consider how organisations might set about instilling security awareness amongst their employees.

3. METHODS OF INSTILLING SECURITY AWARENESS

Organisations must do something to ensure that their employees are aware of their obligations. Without this, people will in all likelihood assume that they have not got any obligations, and presume that IT security is the exclusive preserve of the IT department. So what are they doing about it? The graph in Figure 1 depicts some further results from the Department of Trade & Industry's 2002 survey, and indicates how the respondent organisations claimed to make their employees aware of their obligations in terms of security.



(*Source: DTI*)

Figure 1 : How organisations make staff aware of security obligations

If one were to take a hard-line view of the issue, then the result ought to have been 100% positive response in the first five cases, and 0% in the last one. Certainly the methods listed are not mutually exclusive, and it cannot really be argued that doing one of them removes the need to do one of the others. It can consequently be seen that many of the DTI's respondents were doing far less than they could have been. The list below considers some of the things that an organisation could do in order to promote security and boost awareness, including the approaches indicated in Figure 1 and some additional ideas.

- *Corporate endorsement*
  All security guidelines and recommendations agree that the lead ought to come from the top, and that an organisation must be seen to consider security as a priority. This is essential in any case, but it will not necessarily get anyone to actually *do* anything. As such this should almost be regarded as a given, but organisations should not expect it to solve the problem.

- *Clauses in employment contracts*
  This again represents a starting point, but the downside is that it will often only raise awareness for a specific instant – after reading (and even signing) their contract, many employees will not remember what it actually said. Evidence for this point is provided by results from Finch et al (2003), who conducted a survey amongst 50 employees from a variety of organisations, and found that 20% of respondents could not remember that they had signed a security policy. Even if they do remember that they are meant to maintain security and have responsibilities in the area, most contracts will not give employees enough detail about *what* they are expected to do.

- *Threatening disciplinary action*
  This is basically the use of the stick rather than the carrot, in order to punish users who are found not to be following security appropriately. The approach is not appropriate to all cases (e.g. minor accidental oversights that are exploited), and will only work if the cause of the incident can actually be traced back to an individual. At the end of the day, the ability to invoke disciplinary procedures needs to be there (so that it can at least act as another incentive to staff to take things seriously), but if they need to be used then it still indicates that the employees involved have not taken security on board in the first place.

– *Demonstration*
The idea here is to show employees some practical evidence of what can happen if they neglect security. The most likely way to get them to take notice and buy into the idea is to show them something that is directly to do with them (as it makes it more difficult for them to ignore). However, such overt demonstrations must be handled with care. A typical example of what can go wrong is provided by Cole (2001), who describes an approach that he and colleagues attempted in order to get the users in a large company to choose better passwords (some 95% of them were breakable). In spite of having circulated a password policy in the hope of yielding improvements, and emailing individual users whose passwords were still weak in order to reinforce the point, Cole discovered that more than three quarters of the passwords could still be cracked. He consequently opted for a more public illustration to the problem users – by writing their cracked passwords down on paper and sticking them to their monitors. However, the main effect of this was to make the users irate and abusive, as they felt that approach was too heavy-handed.

Another problem with demonstration is that some things are more difficult to show than others. For example, providing a realistic illustration of what can happen if someone's system gets infected by a virus can carry a significant risk. It could be faked by a system administrator, for example by identifying someone in the organisation who was not using anti-virus software properly, and then temporarily removing all their files and claiming that a virus destroyed them (the files could, of course, be reinstated later). However, although this would be very likely to get people's attention (especially that of the victim), it would be unlikely to endear the administrator to the user community once word got around that it was done deliberately just to prove a point.

– *Written materials, in handbooks and leaflets*
The combination of these approaches in the DTI results (accounting for 30% overall) illustrates that providing staff with material to read is a fairly common way of trying to promote the security message. Unfortunately, creating genuine awareness is not just about putting the information down on paper and assuming that people will read it. It is possible to waste a lot of money on glossy pamphlets that will simply get binned, or put in a drawer and forgotten about. In fact, even if it gets read, there is no guarantee that it will also be understood. Having said this, pamphlets, handbooks, or online

reference materials *can* have a valuable part to play in helping users who have experienced a security incident and then require guidance on what to do. The online approach is probably the best, in the sense that the materials will always be there for users to get hold of, plus of course the organisation can save on the associated production costs. All that needs to happen then is for users to actually remember that there are reference materials available when something goes wrong.

- *Awareness programmes*
  If people cannot be relied upon to read the things that they are given, then awareness programmes can be one of the best ways to draw their attention to the issues that are relevant to them, and ensure that the information has reached them. As the graph in Figure 1 suggests, this can be undertaken as part of an induction programme and as an ongoing activity. The DTI results show that the former is a somewhat more popular option, but it should not really be a choice – organisations ought to pursue both approaches. A one-off security awareness session is unlikely to be sufficient, because after a while many people will forget what they were told. Another factor, particularly in larger organisations, is that the content presented in a general staff induction programme is likely to have been generalised so that it is applicable to staff at all levels, rather than presenting information specific to individual roles. Employees also need to be aware of security issues that relate to their job, and the applications that they are likely to use. As such, if the business is big enough to warrant it, and budgets can be made to support them, initiatives such as the following ought to be given consideration:

  - the inclusion of security-related issues as an integral part of any ongoing organisational training strategy, as well as consideration of mechanisms to promote awareness during day-to-day activities.

  - the facility for staff with key responsibilities, such as IT administrators, to attend specialist security training courses. Established training companies, such as Learning Tree International and SANS, typically offer a range of such courses, targeting both general principles (e.g. Learning Tree offers a course entitled “Introduction to System and Network Security”, which covers fundamental theory aspects) and more specific technical topics (e.g. “Deploying Intrusion Detection

Systems: Hands-On" and "Implementing Web Security: Hands-On", both of which focus practical skills) (Learning Tree 2002).

In many cases, however, it may not be as easy as simply sending staff away on a course if they require training. If nothing else, the cost of doing so could be a significant obstacle – which could again be especially the case for small companies. For example, each of the Learning Tree International courses mentioned above had a standard registration fee of £1,545 per person (for a four day course) – to which participants would typically have to add the costs of travel to the Learning Tree training centre (in London or Edinburgh) and accommodation for the duration of their stay. In my case, for example, living hundreds of miles away from either location, this could easily add another £250 to the overall cost. In the context of the professional training market, these prices are not unusual and the intention here is not to suggest that they are unreasonably high, but such a cost might nonetheless represent a practical barrier to many small businesses (whose staff might of course derive just as much practical benefit as people from larger organisations).

Taking the issue of small businesses further, it is relevant to observe that they will typically face a number of operational constraints that limit their potential to address security. Such constraints will include:

- not having in-house staff with specific security expertise;
- lacking the financial resources to buy in specialist consultancy or provide training for their staff;
- lacking understanding of, or being dismissive of, the risks;
- inability or unwillingness to focus upon security due to other business priorities.

Although there are certainly numerous resources available to provide security advice and guidance without incurring significant expense (e.g. books, web sites, newsgroups and email lists), these offer little facility to test ones understanding in practice. It is desirable to be able to perform such testing before being faced with the task of applying security for real within an organisation. An environment is, therefore, required in which mistakes can be made and learnt from without incurring expense and leaving the system at risk. In response to this requirement, a security training tool is proposed that enables the investigation of available security countermeasures, combined with scenario-based testing and reinforcement. Such a tool represents an example of Computer Based Training (CBT) (Lee and Mamone, 1995).

CBT allows student centred, self-paced learning, enabling users to educate themselves in a time and place that suits them. For employers, CBT can offer benefits with regard to savings in staff being away from the office, reduced travelling costs and times, and saving on expensive accommodation costs that may be incurred for off site courses that require an overnight stay, as well as reduced costs for the training itself.

The use of CBT has certain advantages over conventional methods, especially in company training scenarios. Firstly, CBT is proven to be cost-effective. After the initial set-up costs, what remains is a full-time training facility, available at all times within the organisation. It is also highly appropriate for staff trainees, as they are able to have control of their training and adjust it to their own personal needs. In this way, it is possible for employees to acquire the desired training in specific skills, at their own pace, without having to take time off from work. As such, the training process can be tremendously flexible and personalised. It can also be used to train a large number of employees around the clock. It can run with minimal resource requirements, as there is much less need for a centralised training facility, and different companies or organisations can distribute the same CBT program among their employees.

4. A PROTOTYPE TOOL FOR SECURITY AWARENESS AND TRAINING

The authors have already produced one variant of a prototype training tool, which is described in Furnell et al (2002). The aim of the system is to provide an interactive and user-friendly approach to enhance security awareness and understanding. The training process is based upon a selection of interactive scenario descriptions, in which security countermeasures must be applied in order to solve one or more inherent security issues. The possible solutions must be selected from an accompanying database of security countermeasures, which users can reference in order to obtain explanations of the available security options and approaches. The information held about countermeasures encompasses the type of security issue that they aim to address, along with information about their strength of protection, and the associated impact that their selection might have upon the organisation and its staff (e.g. financial cost, ease of use, disruption to existing practices etc.). Part of the exercise with the tool, when applying the countermeasures to the problem scenarios, is for users to consider these

associated impacts (recognising that providing the highest possible level of security is rarely the only consideration).

The original prototype was an exploration-based system, with users selecting particular parts of an onscreen image (i.e. hotspot areas) in order to obtain a textual description that constituted of part of an overall scenario. From this description, the user would need to determine whether any security problem existed, and if so, recommend appropriate countermeasures. The system would then evaluate the overall security strategy that has been suggested, identifying any remaining weak areas or problems that might be introduced as a result. Further work has since been conducted to refine the concept and devise further problem scenarios that can be used as the basis for training activities. The ongoing work has sought to embrace a more multimedia-oriented approach, which will involve the playback of video segments in which problem scenarios will be depicted. This approach will reduce the requirement for users to read and absorb textual information, which many would consider tiresome after a while, increasing the likelihood of them losing interest in the training program. The presentation of information in an audio-visual format is also considered to be a closer approximation of what the task of identifying problems would be like in a real-life scenario (i.e. staff could not expect to be have the relevant information provided to them in a pre-written textual format – they would often be expected to derive it themselves from what they see and hear). Figure 2 shows the resulting remodelled version of the user interface, showing the different characters that participate in the scenario dialogues. In this revised context, selecting the hotspot areas of the image need no longer yield a simple textual description and can instead invoke the playback of a video clip in a Media Player window.

The idea is that users will view the clips and listen to the dialogues in an attempt to identify whether they contain any security-relevant issues. Some clips will contain information about one issue of relevance, whereas others will make reference to multiple security issues. Conversely, some clips may contain nothing of security-relevance at all (on the basis that if the user knows that everything they see will always contain at least one problem, then the exercise becomes somewhat artificial when compared to a real-world scenario in which they would have to use their own judgement in order to extract the relevant details from a lot of other information that is effectively redundant).

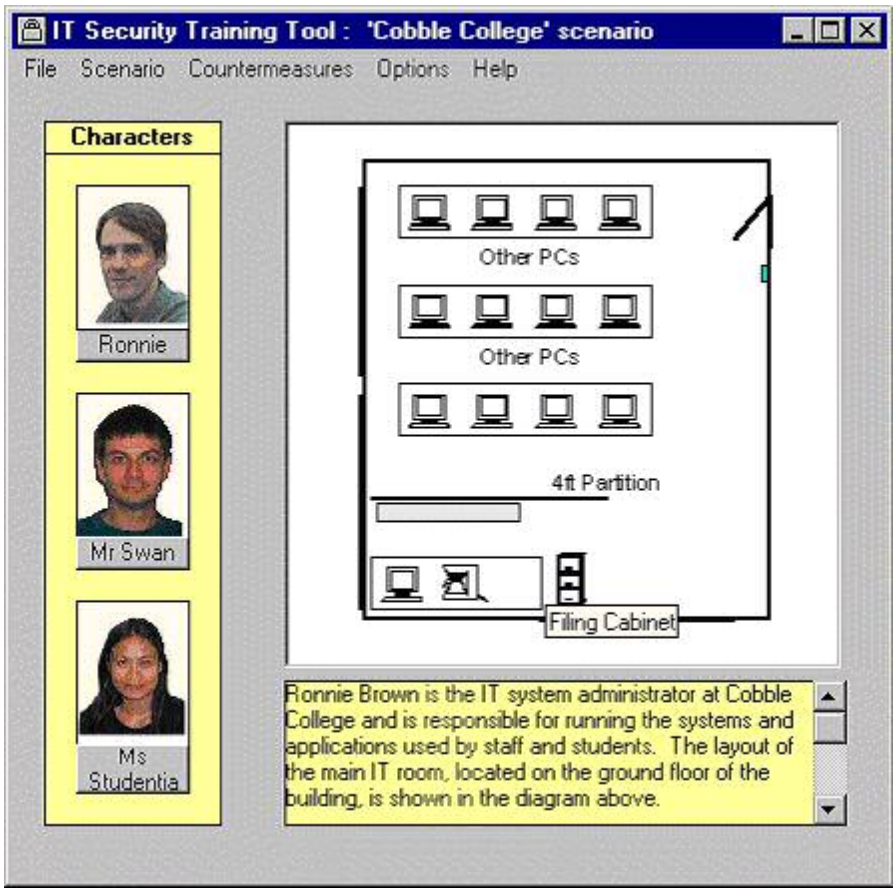


Figure 2 : Screenshot from the revised prototype

Selecting the individual characters yields background descriptions about each of them (which can again be in the form of video clips), enabling the user to determine the character's role in the problem scenario that is being explored. Another potential feature (that has not been realised in the problem scenarios currently specified) would be to allow the user to interview the characters, by asking them some preset questions. As with the dialogues from the hotspot areas, some of these questions would yield useful information in the context of the problem scenario, whereas others would simply provide irrelevant details that the user would have to use their judgement in order to filter out and disregard.

The other significant change in the ongoing work relates to the security controls and countermeasures from which the user would select their recommended solutions to any problems identified. The countermeasures in the original project were based upon those from the pan-European ISHTAR (Implementing Secure Healthcare Telematics Applications in Europe) project, which had developed a controls database as one of the deliverables of its research (Davey et al. 2001). Members of the project team had been involved in ISHTAR, and as such the database was a pre-existing resource to underpin an initial prototype of the training tool concept. However, for the ongoing work, it was considered that a more well-known, and widely applicable, foundation could be provided by basing the problem scenarios upon issues addressed by guidelines contained in the BS7799 (ISO/IEC 17799) standard (British Standards Institution 2000).

As a result, twelve sets of problem scenario dialogues have been developed, based around different sections from BS7799 (Warren 2002). Some of these are single problem scenarios, in which the dialogue is focused around a single issue raised in BS7799, and for which the user would consequently be expected to home in on a particular control area in order to recommend the appropriate solution. Other dialogues present multiple problem scenarios, in which the characters mention several security issues, potentially spanning a number of different areas from BS7799. These scenarios would consequently be aimed at more experienced users, wishing to test their wider knowledge of security.

Figure 3 presents an example of some of the dialogue from one of the single problem scenarios, which in this case is set in the context of a doctor's surgery and involves two characters, Dr Grays and her receptionist Judith (remembering, of course, that in the tool itself this would be acted out in a video clip rather than presented textually). In this example, the point that users would be expected to identify is that measures should be taken when disposing of equipment and media to ensure that information is not compromised. Smaller and less technically proficient companies may dispose of their PCs and media without realising the need to ensure that all data has been securely removed. The point relates to section 7.2.6 of BS7799 (Secure disposal or re-use of equipment), which states that machines that contain sensitive information should be physically destroyed or securely overwritten instead of standard delete functions.

DR. GRAYS	"Morning Judith, how are you finding the new PCs?"
JUDITH	"Great, I really like these thin screens, rather than the bulky old monitors."
DR. GRAYS	"Any problems with the software? Are they working OK with the patient records system?"
JUDITH	"I have not noticed any problems."
DR. GRAYS	"Where are the old PCs?"
JUDITH	"I have stored them in the cupboard until they are collected."
DR. GRAYS	"What about any old data that may be on them?"
JUDITH	"All gone, I went to the DOS prompt and ran delete star dot star, should be OK."
DR. GRAYS	"Good, good. Lets open the doors and see some patients."

Figure 3 : Extract from a single problem scenario dialogue

Multiple problem scenarios may incorporate a number of dialogues, each of which may convey a number of problem issues. An example of a dialogue from one such scenario is presented in Figure 4, and is set within ToolEng Limited, a small (and fictitious) engineering and tool making company. The dialogue takes place during a tea break, and various staff members have congregated in an office that had previously been used by an IT contractor called Brian, who has left the company unexpectedly. A replacement contractor, John, has just started to work for the company. The characters Joe and Jason are fitters who work for ToolEng, while Dennis is the design manager and Janine is an accountant.

JOE	"John, as Brian's office used to be the rest room, we use it for our breaks, and Brian used to let us surf the web if we wanted during our breaks, is that OK?"
JOHN	"I guess so."
JOE	"Hey Jason, I know that you are keen to have a look at the web – you know my login and password, don't you. Here is an old floppy you can copy that stuff onto . . . And Jason, do not forget to put your timesheet in the tray outside before lunchtime."
JOHN	"So what happens to the timesheets?"
JASON	"Oh, Janine collects them, and works them out at home, which is quite good, as once you are logged on you can see every machine on the network, I think"
DENNIS	"Joe have you got a minute? I want to check a design with you."
JOE	"Yes, no problem, I 'll be there in a minute."

Figure 4 : Extract from a multiple problem scenario dialogue

In contrast to the single problem scenario in Figure 3, there is quite a lot going on here, and it is unlikely that a novice would pick up all of the issues. For the record, the problems, and the related BS7799 controls, are as follows:

- It seems that there is no control of network access within ToolEng. Control 9.4 (Network access control) states that internal and external networked services should be controlled.

- It would appear, from Jason's use of a floppy disk on Brian's PC, that there are no controls against malicious software. This is contrary to the recommendation of control 8.3.1 (Controls against malicious software).

- Should staff be eating their food in Brian's office near to his PC? Control 7.2.1 (Equipment siting and protection) states that organisations should consider their policy towards eating, drinking and smoking within close proximity to information processing facilities.

- It is not good practice for Joe to allow Jason to login using his name, or divulge his password to Jason. This contravenes control 9.3.1 (Password use).

- It would seem that each user has access to every other machine once logged on. Control 9.4.2 (Enforced Path) suggests that this should not be the case.

Following the selection of the chosen countermeasures, the user is able to have their solution rated by the system against the optimum solution originally conceived by the author of the problem scenario. Through this they will be able to determine the appropriateness of their recommendations. If an incorrect assessment is made (e.g. the user believes there to be no problem when in fact there is one, or vice versa), then their overall score is affected accordingly, before the system automatically guides them in the correct direction. If desired, the system could present additional information, such as a narrative description, to support the countermeasure solutions and ensure that the user understands the rationale behind the scenario author's approach. In some cases, there may be more than one valid solution, via different combinations of countermeasures that achieve the same objectives. The system would be able to assess this by comparing the attributes of the countermeasures chosen (e.g. protection category, disruption level, financial cost, user friendliness) with the attributes of those selected by the scenario author. These attributes are maintained in the countermeasure database along with the basic title and description details.

When it is fully developed, it is considered that the tool will have a number of potential applications. For example, it may be used:

- as an educational awareness mechanism for general staff, which can be accessed on a day-to-day basis. They can attempt to solve

the problem scenarios, and then use the database materials to explain points that they did not understand.
- as a training tool for staff with specific security responsibilities within the organisation. They can use the database materials to acquire the background knowledge, and then test their understanding using the problem scenarios.
- as a means for more established security personnel to refresh their knowledge and test alternative solutions to the problems.

Development work is continuing at the time of writing, in the guise of masters and PhD level research projects at the authors' institution.

5. CONCLUSIONS

Security awareness is an essential requirement for any organisation utilising IT systems. However, as the evidence presented in this paper has illustrated, the issue is often given insufficient attention, and is consequently considered to be a significant factor in the ongoing occurrence of security incidents. However, achieving an appropriate level of awareness can be difficult, particularly in smaller organisations with limited funds and in-house expertise that can be drawn upon.

Computer-based training can be used to help inform and educate employees at all levels, exposing them to different security threats, and allowing them to experiment with different countermeasure solutions, within the confines of a simulated environment. It also allows awareness to be cultivated in a more active and engaging manner than simply requiring staff to read pamphlets and other reference material. The principal advantage of the proposed tool will thus be that it enables staff to become familiar with the types of security issue that they may encounter, as well as the countermeasures available, the situations in which they are appropriate, and any constraints that they may impose.

The development of the prototype system, and associated methods, will continue within the authors' research group. Once the software itself has been more fully developed, the intention is to use it as the basis for practical trials, and ultimately determine whether it has a measurable effect upon security awareness within a reference environment.

REFERENCES

Audit Commission. 2001. *yourbusiness@risk - An update on IT Abuse 2001*. Audit Commission Publications. September 2001.

British Standards Institution. 2000. *Information technology. Code of practice for information security management*. BS ISO/IEC 17799:2000. 15 February 2001. ISBN 0 580 36958 7.

Cole, E. 2001. *Hackers Beware*. New Riders. ISBN 0735710090. pp290-291.

Davey, J, Furnell, S. and Gaunt, N. 2001. "The ISHTAR Security Guidelines", in *Implementing Secure Healthcare Telematics Applications in Europe*. The ISHTAR Consortium (Eds). Technology and Informatics 66, IOS Press: pp167-180.

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

Ernst & Young. 2002. *Global Information Security Survey 2002*. Technology and Security Risk Services, Ernst & Young LLP.

Finch, J.W, Furnell, S.M, and Dowland, P.S. 2003. "Assessing IT Security Culture: System Administrator and End-User Perspectives", to appear in *Proceedings of ISOneWorld 2003 conference and convention*, Las Vegas, Nevada, USA, April 23-25, 2003.

Furnell, S.M., Gennatou, M. and Dowland, P.S. 2002. "A prototype tool for information security awareness and training", *Logistics Information Management*, vol. 15, no. 5/6: 352-357.

KPMG. 1998. *Information Security Survey 1998*. KPMG Information Risk Management, London, UK.

Learning Tree. 2002. *Hands-On Training for IT Professionals and Managers*, Learning Tree International catalogue, September 2002 – February 2003.

Lee, W.W. and Mamone, R.A. 1995. *The Computer Based Training Handbook: Assessment, Design, Development, Evaluation*. Englewood Cliffs, NJ: Educational Technology Publications.

NCC. 2000. *The Business Information Security Survey 2000 (BISS 2000)*. National Computing Centre, Manchester, UK.

OECD. 2002. *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*. Organisation for Economic Co-operation and Development.

Warren, A. 2002. *An Educational Tool for Information Security*. MSc Thesis. University of Plymouth, Plymouth, UK.