Organisational Security Culture: Embedding Security Awareness, Education and Training

Steven Furnell and Nathan Clarke

Network Research Group, School of Computing, Communications and Electronics,
University of Plymouth, Plymouth, United Kingdom
info@network-research-group.org

Abstract

Awareness and understanding of security is fundamental to establishing a successful security culture within an organisation. Published survey evidence reveals that although awareness, training and education are recognised as having a significant relationship to the achievable level of security, and are promoted in various security standards, many organisations do not make sufficient use of them. This discussion paper examines the general applicability of the techniques to employees at all levels, beginning with the end user community, and the principal approaches that may be suitable for them. The text then proceeds to consider the specific needs of individuals with key security responsibilities within an organisation, highlighting the fact that in many cases, these individuals do not have formal qualifications for the roles that they have been allocated. The various levels of qualification are then examined, and structured within an overall taxonomy to indicate the security expertise and capabilities that should be expected of individuals that hold them.

Keywords Security Culture, Staff Awareness, Security Training

Introduction

The underlying premise of establishing a security culture is that organisations have a much greater chance of protecting their assets if everyone plays an active part. To this end, all employees need to understand how security relates to them – reducing the potential for it to be dismissed as somebody else's problem. Achieving a successful security culture also implies that security issues are considered as part of organisational operations and decision making. A fundamental tenet of achieving this is consequently that security is understood – which in turn introduces demands for related education and training. Indeed, the lack of appropriate education is often cited as a main or contributing reason for the occurrence of security incidents and/or a significant barrier to be overcome.

- Twenty five percent of the 1,001 respondents to the UK Department of Trade & Industry's Information Security Breaches Survey 2004 indicated that, with hindsight, their worst security incident could have been prevented by staff training (DTI 2004)
- Five percent of respondents to KPMG's Global Information Security Survey 2002 cited education of users as the most important security issue facing their organisation. While this figure may initially seem low, it is worth noting that only viruses (22%), hackers (21%), remote access (17%) and Internet security (10%) were ahead of this rating (KPMG 2002)

- Lack of user awareness was cited as the most significant obstacle to achieving effective security in Ernst & Young's Global Information Security Survey 2004, placing the issue ahead of budgetary constraints and technology issues (Ernst & Young 2004).

With such points in mind, it is not surprising to find that the importance of security awareness and training are emphasized in the main standards and guidelines. For example, in 2002 the Organisation for Economic Cooperation & Development (OECD) issued a set of voluntary guidelines for information systems and networks, entitled 'Towards a Culture of Security'. The first principle of these guidelines relates to 'awareness', and states that "Participants should be aware of the need for security of information systems and networks and what they can do to enhance security" (OECD 2002). However, aside from recognising the importance, the guideline does not actually help readers to pursue the objective, and alternative sources need to be consulted in order to determine how such awareness might be cultivated.

Related issues are also clearly highlighted within ISO 17799, with 'security education requirements' being flagged as one of the key aspects that ought to be addressed by an organisation-wide information security policy document. This particular standard also makes some fairly clear points regarding the co-ordination of information security, and the allocation of key responsibilities. It is therefore not unreasonable to expect that those being allocated responsibilities will also be provided with relevant education and training to ensure that they can be fulfilled.

As with the other aspects of its recommendations, 17799 presents only general guidance regarding the specific issue of security training. The 'Personnel security' section of the standard includes a sub-section dedicated to 'user training', with the stated objective of ensuring that users are aware of security threats and "equipped to support organizational security policy in the course of their normal work". The (single) underlying guideline (entitled 'information security education and training') highlights the general requirement for users to be trained in security procedures, and the correct use of systems, with the specific wording as follows:

> *All employees of the organization and, where relevant, third party users, should receive appropriate training and regular updates in organizational policies and procedures. This includes security requirements, legal responsibilities and business controls, as well as training in the correct use of information processing facilities e.g. log-on procedure, use of software packages, before access to information or services is granted*.

As can clearly be seen, although some examples of what the users need to be trained about are mentioned, the recommendation is by no means exhaustive or detailed. Although the wide variety of possible implementation scenarios makes it impossible to be too prescriptive, it is perhaps surprising that this issue has not been explored in more detail. Certainly, when contrasted to other control areas within 17799 (such as equipment security or protection against malicious software), it is clear that security training does not receive as many specific recommendations. Having said this, there are a number of other points in the standard at which awareness-raising recommendations are highlighted. For example, the Personnel security section also refers to inclusion of security roles and responsibilities in employee job descriptions, as well as in the terms and conditions of

employment – which can certainly help to make security expectations explicit and raise awareness in the initial instance.

Although somewhat more detailed guidance can be found in other sources - a good example being the NIST handbook on computer security (NIST 1996) - it is still ultimately down to each organisation to be aware of the need for attention to these issues, and determine the methods are likely to work most effectively within their environment.

Security promotion in practice

The lack of detailed guidance is likely to explain why, although the principle is accepted, the practice of security education appears somewhat harder to achieve. Indeed, surveys consistently portray a less than encouraging picture in terms of the proportion of respondents that appear to be giving the issue serious attention. As an example, Figure 1 presents the results from the two most recent surveys from the Department of Trade and Industry in the UK (from 2002 and 2004) and globally from Ernst & Young (in 2003 and 2004), and shows the proportion of respondents claiming that their organisations provided some form ongoing security training. Although the more recent versions of each survey suggest some level of increased attention, all show less than half of the organisations providing such support – which is particularly interesting given the earlier results cited from these surveys, in which lack of training was perceived to be an obstacle and the cause of significant security incidents.

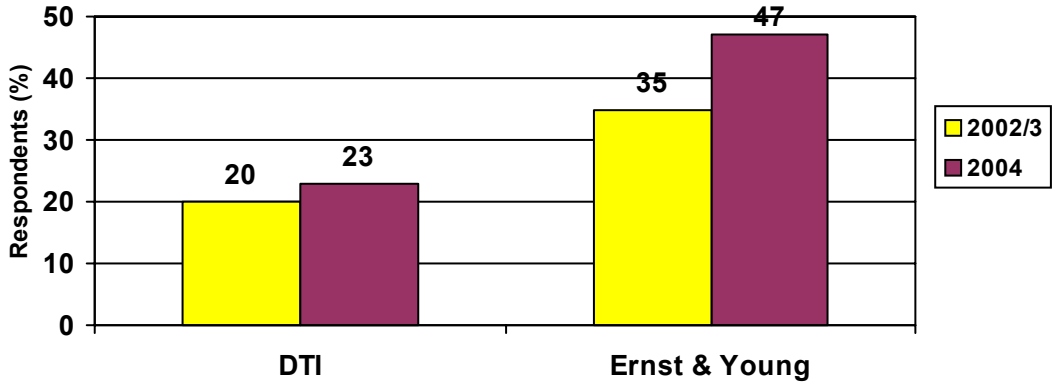


Figure 1: Provision of ongoing security training

The paucity of security promotion is also evidenced by the views of respondents to the Computer Security Institute's 2004 Computer Crime& Security Survey. These results show the average opinion emerging from 488 respondents across all sectors surveyed (including government, medical, manufacturing, retail and educational domains) was that their organisation did not invest an appropriate amount on security awareness (Gordon et al. 2004).

It is important to realise that security culture will only be achievable if the concept is seen to be supported by the top level of the organisation, and the provision of security education can clearly be a crucial contribution in this respect. Drivers for establishing such a culture are increasingly being felt from a legal perspective. For example, it is becoming established that system usage and security policies that explicitly define employee's responsibilities are not only required to protect computing assets from misuse

and abuse, but also to protect organisations from possible litigation from employees, customers and third parties that may result from security breaches (Bennett, 2003). By addressing and promoting these aspects effectively, organisations can provide themselves with a safeguard that enables them to demonstrate that they have taken an considered and responsible approach to security. In addition, legislation itself may specify expectations in terms of security. For example, the UK Data Protection Act (1998) specifies that personal information must be stored and accessed securely, with negligence potentially resulting in severe penalties for the organisation and those responsible for it. For these reasons, organisations again need to do their best to protect themselves, by ensuring that employees are in a sufficiently informed and capable position to uphold the requirements upon them.

Having established the need to promote security, it is necessary to recognise that simply providing a generic programme for everyone will not be the answer, and employers need to determine what level of understanding their employees actually need in order for the desired security culture to be fulfilled. As the aforementioned NIST publication clearly expresses, the issues of awareness, training and education aim to address needs at different levels:

- Awareness – Enables of recognition of what needs to be protected.
- Training – Provides skill in how the protection can be achieved.
- Education – Provides deeper understanding of why protection is required.

It is very unlikely that all employees will need the same provision. Indeed, from the organisational perspective, it can be argued that awareness is desirable for everyone, and training will certainly be appropriate to some degree (depending upon the employee role, responsibilities and system access), but the requirement for education is possibly limited to dedicated security personnel.

Awareness and training for end users

In spite of high profile incidents, and the significant attention that has been devoted to them in recent years, users still do things that demonstrate their lack of understanding of basic safeguards. For example, all of the following are familiar end-user failings that ought to be avoidable with effective security training and awareness programmes:

- Poor choice of passwords
- Opening malware-infected email attachments
- Getting tricked into providing sensitive data to phishing scams (Furnell 2004).

The fact that such incidents remain all too frequent occurrences is indicative of the users not having understood their part in the security culture. However, resolving such problems is not just a case of telling the users about the threats and then expecting them to act appropriately. Security expectations must be promoted effectively, and then suitably reinforced. The latter is an important aspect, in the sense that even if steps have been taken to emphasize security in the first instance, the employees should not be assumed to have retained the information. Some good evidence of this is provided by Finch et al (2003), who conducted a survey amongst employees from a variety of organisations, including a question about whether they had been required to sign up to a security policy. As shown in Figure 2, the results were revealing in the sense that 20% of respondents could not remember that they had signed a security policy, while a further 12% claimed to have signed one, when in actual fact they had not been required to do so.

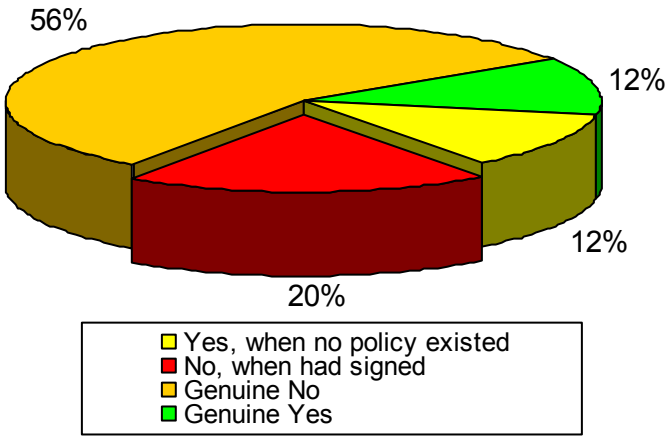
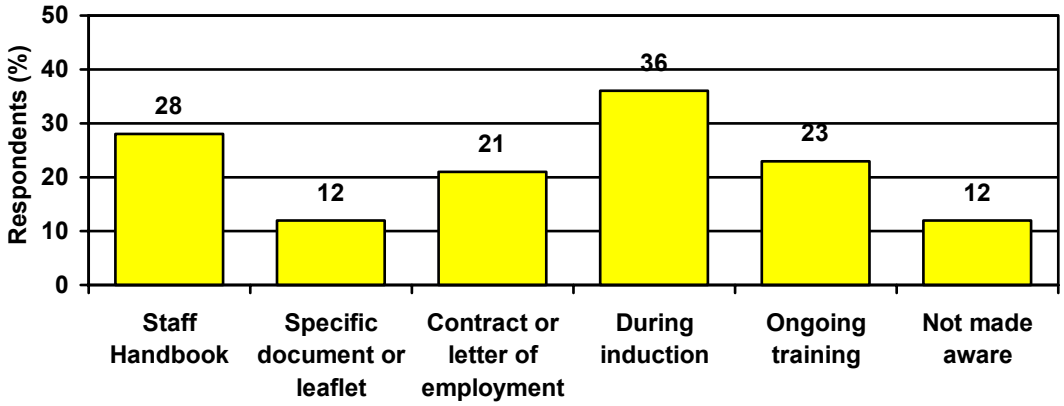


Figure 2: Employee recollections of signing up to a security policy

With such realisations in mind, it is clear that approaches need to be considered for keeping security issues in the forefront of employees' minds. Some examples of possible approaches are shown in Figure 3, which additionally illustrates the extent to which they are followed by the respondents to the aforementioned DTI security breaches survey. In addition to these ideas, organisations could also make use of posters, screen-savers and other electronic reminder systems – all of which represent a good solution for promoting short messages. Indeed, many products have been developed to fill these gaps (see, for example, www.easyi.com/infosec), and a variety of related materials can also be located online.



(*Source: DTI 2004*)

Figure 3: How organizations make staff aware of security obligations

However, raising awareness is only part of the process. It is also necessary to ensure that people have the knowledge and capabilities to do what is expected of them. Without this, they may not be able to take proper advantage of the security facilities available to them. As such, security training must also be considered. In doing so, a key point to realize, particularly in larger organisations, is that a single training programme is not

going to be sufficient. If the business is big enough to warrant it, and budgets can be made to support them, then a range of initiatives ought to be given serious consideration:

- *Job training*
  Staff should receive instructions on how to perform their day-to-day duties as well as any specific security issues relating to their role. This should convey a clear statement of what is expected in terms of security, with well-defined bounds so that they are not concerned when performing legitimate duties. It must be ensured that personnel have sufficient training to comply with any security requirements specified in their contract of employment.
- *Use of systems & applications*
  Staff should receive adequate training for any systems and applications that they are likely to use, covering both general operation and use of any security features provided. In addition, documentation should be available for general reference to supplement and re-enforce the training provided.
- *Internal training programmes*
  Internal company-wide training and awareness programmes should be operated as part of the induction of new staff, and as refresher courses for existing personnel. These initiatives should be based upon the organizational security policy and concentrate upon providing basic security awareness for all personnel. Coverage should include the basic security procedures that should be followed by staff using information systems (e.g. correct use of passwords, backing up of data, awareness of viruses etc.). More specific in-house training may be provided at departmental levels, with programmes tailored to the needs of the staff within them. In addition, organisations could usefully consider the use of computer-based training tools, which employees may then utilise in an on-demand, self-paced manner (Furnell at al. 2003).
- *Specialist training courses.*
  Some staff with key responsibilities, such as IT administrators, will require training beyond the level of that described above and thus may benefit from attending specialist security training courses (e.g. addressing the security features of operating system and server platforms, and the correct configuration and usage of specific security tools, such as firewalls and intrusion detection systems). This point is explored further in the next section.

As previously indicated, these activities should not be considered as one-off tasks. In addition to reminders and refresher courses, there should also be recognition that security issues may need to be revisited as things change in the organisation. For example, the introduction of new systems and technologies, changes in the business focus and structure, or staff promotion, may all be triggers for new points to be highlighted or for skills to be kept up to date.

Supporting key roles and responsibilities

The recognition of individuals with key responsibilities for security merits further discussion, as a lack of appropriate knowledge or skills on the part of these individuals can pose major problems. For example, a system administrator who is not sufficiently security-aware may neglect or fall short in essential tasks such as such as setting security parameters and applying critical updates and patches. For example, looking at the zone-

h.org site, approximately a third of website defacements are considered to happen as a result of mis-configured systems (Zone-H. 2004) – suggesting a possible lack of skill on the part of the administrators responsible for the servers.

One of the key reasons for such problems is often that security responsibility in many organizations is entrusted to an IT generalist. Supporting evidence can again be provided by drawing upon survey evidence. For example, the DTI Information Security Breaches Survey 2004, which found that 89% of the teams responsible for information security lacked anyone with formal security qualifications. Similarly, the respondents to Ernst and Young's Global Information Security Survey 2004 ranked 'availability of skilled staff' as the third most significant obstacle to achieving effective information security.

Such concerns raise the question of what options are available to organisations who wish to employ suitably skilled personnel:

- *Academic qualifications*
  Educational courses, offered by academic institutions, leading to diploma and degree qualifications. An increasing number of universities are offering specialist security programmes at both undergraduate and master's levels.
- *Professional certifications*
  These may be broadly based, or more specifically focused around individual technologies and security roles. The best known example of the broadly based approach is the Certified Information Systems Security Professional (CISSP) certification from the International Information Systems Security Certifications Consortium (ISC)2. This addresses the principles, safeguards and practices of security based upon a Common Body of Knowledge (CBK) covering ten topic domains, from security management and continuity planning, through to network security and cryptography ((ISC)2 2004). An example of the more focused certification is the Global Information Assurance Certifications (GIAC) program, which offers a range of certificates suited to different aspects of security, and hence the different roles and responsibilities that individuals might assume (e.g. GIAC Certified Intrusion Analyst, GIAC Certified Windows Security Administrator, and GIAC Certified ISO-17799 Specialist) (GIAC 2004).
- *Vendor-specific certification*
  These are commercial and market-driven offerings that relate to an individual's proficiency with a specific manufacturer's range of products. An example here is the Cisco Security Specialist (CSS) credential.

With such a range of possibilities available, organisations seeking to recruit or contract appropriate expertise could conceivably be faced with a confusing situation. For example, what skills should they look for? Do they truly want someone who has been educated or someone who has been trained? Is someone who comes to the organisation with an MSc-level qualification in IT security likely to be as useful in day-to-day practice as a CISSP? With such concerns in mind, it is useful to structure the various qualifications into some kind of taxonomy, so that it is easier to appreciate the distinctions between them. Such a classification is presented in Figure 4, which shows the four different types of certification (or qualification) that have been mentioned in this section, and shows how they fit together in terms of the knowledge and skills that someone certified at each level is likely to have acquired.

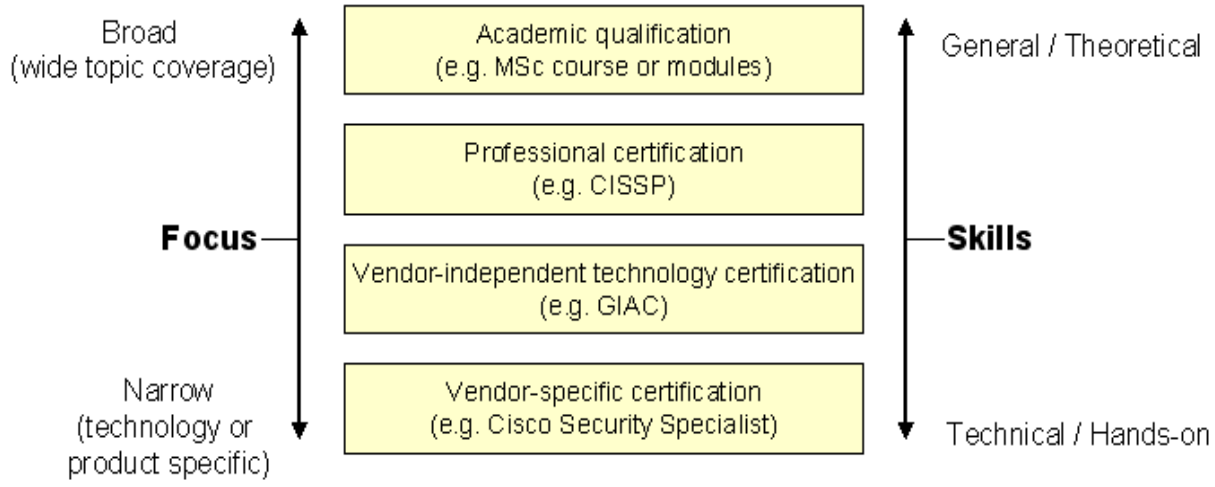


Figure 4: A taxonomy of security qualifications

In addition to the skills that a qualified individual will be equipped with, another consideration is the longevity of their qualification. While academic qualifications will not expire, the professional certifications need to be periodically renewed to maintain their currency. In addition, the more specific the focus of the certification, the more likely it is to date (e.g. as a product is replaced by the next generation release, and the security considerations change).

The points to take away from this discussion are that security certification does not come down to recommending one type of scheme over another, and there is no 'best' option that is suitable in all contexts. The important thing is to understand the type of expertise that you, or your business, require and then aim to locate someone who can demonstrate a suitable qualification in that area.

As with end users, the security knowledge at this level will still require potential reinforcement and update. For example, organisations will need to ensure that updates in technologies are accompanied by updates in the relevant administrator skills.

Conclusions

Security awareness and training are important elements in establishing a security culture within an organization. The management of the organisation needs to appreciate where their problems lie, and what each awareness or education option could consequently do to help. However, it is clearly not a 'one size fits all' situation, and therefore consideration is required to determine which approaches will work in which context.

If employees are not given appropriate advice and guidance, then organisations should not be surprised to find them doing things wrong. Similarly, if individuals with key responsibilities for security do not have the appropriate background and skills, then they will not be best placed to operate in a confident manner. In addition, however, it is important to realise that management or the board of an organisation may also need to be kept aware - in order gain their support for education and training initiatives. As such, it is necessary for other staff to ensure that details of threats and actual incidents are

reflected up to this level in a meaningful fashion. In this way, those who should be promoting the security culture will have more incentive to ensure they also facilitate it.

References

Bennett, M. 2003. "Usage Policies Limit Liabilities". IT Week. www.itweek.co.uk

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

Crown. 1998. Data Protection Act. Crown Copyright. http://www.hmso.gov.uk/acts/acts1998/19980029.htm.

Ernst & Young. 2004. Global Information Security Survey 2004. Assurance and Advisory Business Services. Ernst & Young. EYG No. FF0231.

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

Furnell, S.M, Warren, A.G. and Dowland, P.S. 2003. "Improving Security Awareness through Computer Based Training", Security Education and Critical Infrastructures, C.Irvine and H.Armstrong (eds): 287-301.

Furnell, S.M. 2004. "Getting caught in the phishing net", Network Security. May 2004. pp14-18.

GIAC. 2004. Global Information Assurance Certifications (GIAC). See http://www.giac.org.certifications.php.

Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Richardson, R. 2004. Ninth Annual CSI/FBI Computer Crime and Security Survey. Computer Security Institute.

(ISC)2. 2004. "CISSP Certification", International Information Systems Security Certifications Consortium (ISC)2. http://www.isc2.org.

KPMG. 2002. 2002 Global Information Security Survey. KPMG, United Kingdom.

NIST. 1996. An Introduction to Computer Security: The NIST Handbook. Special Publication 800-12. National Institute of Standards and Technology, Technology Administration. U.S. Department of Commerce.

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

Zone-H. 2004. "Stats & graphs", Zone-H.org, http://www.zone-h.org/en/stats (accessed 23 October 2004).