Enhancing Security Education
Recognising Threshold Concepts and Other Influencing Factors

Ismini Vasileiou[1] and Steven Furnell[1,2]
[1]*Centre for Security, Communications and Network Research, University of Plymouth, Drake Circus, Plymouth, U.K.*
[2]*Centre for Research in Information and Cyber Security, Nelson Mandela University, Port Elizabeth, South Africa*

Keywords: Security, Education, Awareness, Threshold Concepts.

Abstract: Users are frequently recognised as lacking a necessary level of security education, and even where efforts are made to provide it, they are rarely matched directly to the needs of the audience. This paper examines the gap between the typical provision of security education and what could be achieved via an approach that recognises differences between the individuals that are being targeted. The discussion highlights baseline areas of security literacy that are applicable to all users, but then illustrates how variations in individuals' understanding of threshold concepts could complicate the task of delivering the related education. An approach is proposed in which security education becomes more tailored, recognising factors such as the user's prior knowledge, learning style, and existing perception of security, leading to a personalised security education plan that is framed towards individual needs.

1 INTRODUCTION

Achieving a baseline understanding of cybersecurity is now a fundamental requirement for all users of IT, in both personal and workplace contexts. Unfortunately, this is far from a guarantee that it actually receives the attention and resourcing that it deserves.

For personal users, we have not yet reached a point where security awareness and education can be assumed to exist as standard. Indeed, many current IT users are still from a generation that would be regarded as digital immigrants (Prensky, 2001). Meanwhile, even the digital natives who grew up with the technology may not have received a necessary emphasis upon security issues, as these have become progressively more pronounced since the advent and growth of online services. It might reasonably be hoped that someone being schooled today would find security receiving some attention, but the various generations of current users that preceded them will be at varying levels of familiarity and competence.

In the workplace context, organisations depend upon their staff to be security-aware, but consistently fail to devote attention towards supporting this. For example, findings from the UK's Cyber Security Breaches Survey 2017 reveal that only 30% of organisations provide user awareness and education versus 90% and 89% indicating attention towards technical controls malware protection and network security (Klahr et al. 2017). Moreover, the situation is no different at higher levels of the organisation, with 68% of Boards indicating they have received no training for cyber security incidents (HM Government, 2017).

There are some aspects of security that *all* users need to know about, regardless of the specific technologies, applications and data that they use. This can be regarded as ensuring baseline cybersecurity literacy. However, what can sometimes be overlooked is that the baseline security literacy itself needs to be built on top of a solid foundation of basic IT and information literacy. If users are lacking these aspects, then it is unlikely that the security lessons will make sense, and they may still find themselves lacking the practical IT skills to enact what is required of them.

The traditional paucity of security awareness and education provision means that it is often seen as an achievement to find it being given any attention at all. However, although some provision is going to be better than none, the chances of it having the desired effect are limited unless it has been appropriately planned and considered. For example, many organisations rely upon a one-size-fits-all approach, where the same security training is made available to

Vasileiou, I. and Furnell, S.
Enhancing Security Education - Recognising Threshold Concepts and Other Influencing Factors.
DOI: 10.5220/0006646203980403
In *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018)*, pages 398-403
ISBN: 978-989-758-282-0

all staff (often via an e-learning package and/or other online resources). While this at least serves to ensure that staff have had the opportunity to become acquainted with the issues, it is rarely going to deliver the best results in terms of developing true awareness and understanding of security. To achieve this more fully, the provision ideally needs to be tailored to the needs of the individual learner.

Focusing in this paper around security awareness for end users, in other words on those soft skills people need to acquire, we are exploring how we can more effectively address the issues around lack of security education. Is it down to security managers? Is it down to the training material? Or is it down to the individuals? The likely answer is a combination of all of them, but the recognition of the individual in the process is key. It is argued that we need to design and deploy cybersecurity awareness, training and education programmes with a clear understanding of who we are addressing and how they are positioned in terms of factors such as prior knowledge, learning style, and perception of security.

2 BACKGROUND

While it is commonplace to cite users as a weak link in security, and bemoan their lack of attention to relevant practices and safeguards, it is fair to say that they are rarely going to be positioned to know (and do) the right things if they have not been provided with prior support. Indeed, if we think of the hurdles that a user needs to overcome in order to be in a position to understand and take responsibility for security, there are number of distinct points and associated questions that users may be asking themselves as a result (Furnell, 2010):

- **Perception (what is it?):** how threats and their associated security measures are viewed and understood by those that they may affect.
- **Priority (how important is it?):** the ability to recognise the importance of security and protection aspects are when set alongside other activities and commitments.
- **Responsibility (what do I need to do?):** the extent to which relevant individuals accept, understand and undertake their security responsibilities
- **Capability (can I do it?):** the extent to which users actually have the knowledge and skills required to undertake their responsibilities.

All of these issues require appropriate awareness and understanding to have been established in order to enable users to answer the associated questions. If this is not the case, the they will potentially be left ill-prepared to do what is expected of them.

In practice, many security managers pay more attention on technical issues such as firewalls and intrusion detection/prevention systems, and tend to overlook (or omit) soft issues such as efforts toward reducing the hazards caused by end users. Information security awareness should be seen by managers as one of the organisation's missions. They should put in place such mechanisms that will enhance it, and ensure that end-users of all levels and all backgrounds will be able to make it part of their everyday skills.

Many people confuse awareness with publicity. They often think just because there has been a presentation or an email on a specific security-related topic it will be enough for people to understand the issues and dangers involved. What they omit is the attention to behaviours. Behaviour is a result of a decision-making process that is being formulated on individual basis by knowledge, prejudice, psychological aspects and cultural backgrounds. Security managers often they are not able to predict certain behaviours because of the aforementioned focus on technical aspects, and even within security awareness itself it is easy to find the focus being given more towards the use of technical controls and safeguards rather than helping to develop a security mind-set and culture. Security managers need to think more how to meet awareness needs and this can only be done by identifying and recognising the different behaviours. Training material must be developed and produced in such a way that emphasis will be given on the soft skills people need to acquire.

Security awareness can be broken down into two categories. One is the content, and the other is the framework within which this is provided. The content will, of course, ultimately depend upon what the user needs to know, but the next section covers some baseline issues as examples. While the content is clearly important in determining what people will ultimately know about, the framework aspect is arguably more challenging as it affects the likelihood of the content addressing and reaching the target audience in an appropriate way. This aspect consequently forms the mainstay of the discussion in sections 4 and 5.

3 BASELINE SECURITY LITERACY

One of the fundamental questions to address when considering security awareness and education is what

people should actually be expected to know about it. Clearly the specifics will ultimately depend upon the technology, systems and data that someone uses, and (in the workplace) the expectations of their organisation and the role they hold within it. However, there are certainly some things that all users should arguably know about, in order to be able to follow basic good practice and protect themselves from harm. As an example, prior work has proposed a series of eight key areas in which users should have a knowledge of the related security issues, as well as an appreciation of how to deal with them in practice (Furnell and Moore, 2014). The core areas, and what users should understand about them are summarised as follows:

- **Authentication:** The role of authentication in preventing unauthorised access.
- **Backup:** The risks to systems and devices that may result in data loss, and the impact that such a loss may have for them.
- **Malware protection:** The potential impacts of malware and the possible routes for infection
- **Mobile devices:** The risks that devices can face from both technical threats and the physical environment.
- **Privacy and data leakage:** The sensitivity of different types of data, and the ways in which it could be misused (e.g. to support identity theft).
- **Safe Internet access and web browsing:** The existence of threats such as phishing, malicious sites, and unsafe downloads.
- **Secure networking:** The risks posed by using unprotected or unknown networks.
- **Software updates:** The reason why software updates are released and the importance of patching vulnerabilities

Each of these then has an accompanying set of basic things that users should be able to *do* to support themselves in achieving the associated protection. In some cases, this will require more active involvement on the part of the user than others, as there are increasingly system-automated features that can cover basic safeguards (provided that they are enabled and permitted to work). For example, in the case of authentication, core skills would include the ability to choose and use suitable passwords, and then follow good practice in terms of managing them. So, in this case it requires the user to have some ability to discern and make the correct decisions. Meanwhile, for malware protection, the basic requirement is for the user to have the ability to check that appropriate antivirus protection is installed, enabled, and up-to-date (i.e. beyond this there is not much they will routinely be required to do in an active sense).

Unfortunately, while it may be easy to agree that these areas are indeed reasonable baseline areas in which to expect security knowledge and skills, it is less easy to be sure of where and how they should be acquired. For example, many organisations would seem to implicitly believe that such knowledge would be acquired elsewhere, and so provide little work-place support for developing them. In practice however, users are frequently not pre-equipped with a uniform and sufficient understanding of either the security basics or the underpinning IT aspects, and so still require support to operate effectively. A further complication to providing such support comes from how the variations in individuals' prior knowledge (or lack of it) may represent a barrier to their further learning. As such, it is relevant to understand how each person is positioned and what is potentially standing in their way, as discussed in the next section with the notion of threshold concepts.

4 THE ROLE OF THRESHOLD CONCEPTS

Meyer and Land (2003) introduce the ideas of threshold concepts and troublesome knowledge in a way to help educators of any field and/or discipline to understand the barriers in people's learning cycle. Threshold concepts are those characteristics learners have in any kind of learning environment that form the ontological concepts of that individual. The integration of information through progress towards understanding of a subject often becomes troublesome for the learners. Threshold concepts demand the integration of the concepts and deeper understanding the learner needs to acquire and develop their ideas. This results in learners accepting that their individual learning will transform.

The notion of threshold concepts is now seen as a valuable tool to understand, facilitate and aid the development of learning and awareness in a rapidly expanding field. In this paper, we suggest that the threshold concepts approach could be a useful tool for security managers to reconsider their way of planning and delivering their security awareness training. With the threshold concept approach, during the development of the training material and also during the training sessions there will be more linkages between thinking and practising. Meyer and Land (2003) suggested five key characteristics:

- **Transformative**: When the idea is understood, a threshold concept can change the end user's views.
- **Irreversible**: Given their transformative potential, threshold concepts can be irreversible.
- **Integrative**: Once learned, it is more likely to bring together different aspects and opinions and become more related.
- **Bounded**: Identifying the conceptual space, serving a specific and limited purpose
- **Discursive**: Crossing thresholds will incorporate a greater level of understanding and engagement in the field.

From the above characteristics, bounded and integrated together identify the episteme of the security awareness discipline. It can assist in exploring the particular behaviours and ways of thinking and practising. One characteristic cannot happen without the other four characteristics. Concepts are, and need to be, integrative and transformative. Security managers need to aim for further change so continuous development of the training and re-training is highly needed. By using the threshold concepts approach, managers will be in a better position to identify and define the boundaries and make sense of specific problems. In other words, why end users do not always apply security measurements.

Table 1, based on Davies and Mangan (2005), shows some differences between the conceptual change in the acquisition of basic and new concepts.

When producing and delivering security awareness and training material, the human factors must be considered. The need for a multi-disciplinary approach not only has been acknowledged in many different fields, but it is also known as empowering and contextualising the involvement of the users with the systems. The employee's role in adhering to the security standards should be a number one priority and this can only be done by implementing such security policies that take into account the human factor.

In terms of security goals and objectives, organisations should be looking not only to invest on technical aspects but also on socio-cultural and educational aspects too. The way manuals and guidelines are produced should be in an interdisciplinary manner. Although organisations feel they provide enough and adequate training to their employees, we often find they forget the human factors, the socio-economic issues, and training is seen as basic and barely practised.

Table 1: Definition and exemplification of three types of conceptual change.

Type of Conceptual change	Types of transformation and integration	Examples in Security Awareness
Basic	Understanding everyday experiences of security issues through integration of personal experiences with ideas	• Understanding the role of each of the baseline areas of cybersecurity literacy. • Understanding the differences between basic security methods such as authentication, data encryption.
Security Awareness Threshold Concepts	Understanding of other subject ideas integrated and transformed through acquisition of theoretical perspective	• Understanding how to combine controls in order to ensure a holistic approach to security compliance (e.g. recognising what might meaningfully work together to provide a required form or level of protection). • Requires people to know the basic roles of the distinct elements of protection, and be able to make the connections between them.
Procedural (how awareness models are constructed + evaluated)	Ability to construct discipline-specific narratives and arguments, transformed through acquisition of ways of practising	• Users are able to continue and advance their understanding and application of security awareness well after their training • Identifying the need for security in situations that had not previously been introduced (e.g. identifying that the content of a document is sensitive, and then judging the appropriate protection to apply).

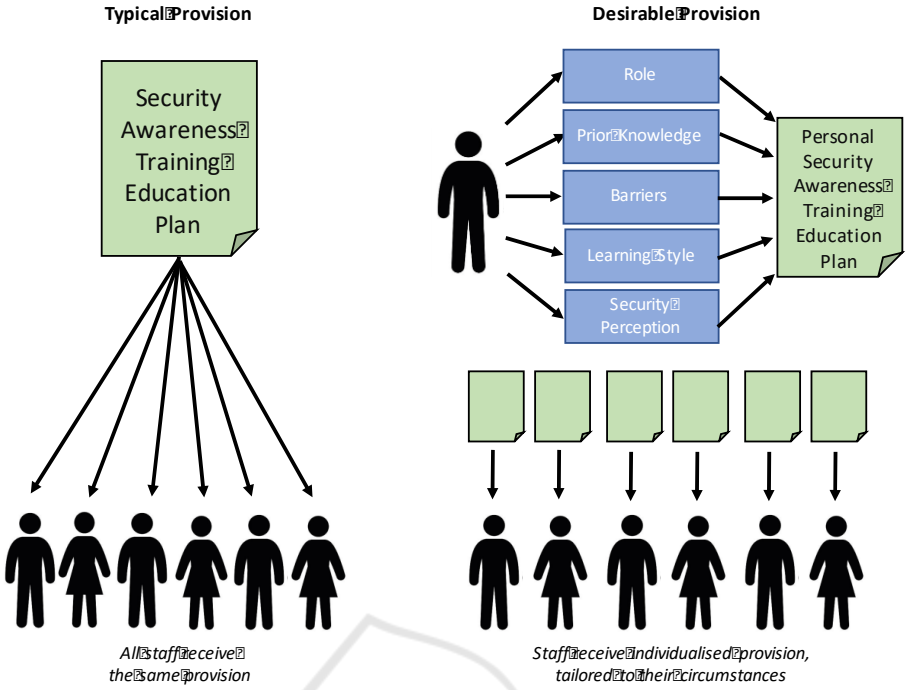

Figure 1: Comparing current and proposed modes of delivering security awareness and education.

5 ESTABLISHING A FRAMEWORK FOR INDIVIDUAL SECURITY LEARNING

If we understand a given user's position in relation to the threshold concepts, then we are immediately better placed to support them in developing their security-specific learning. For example, users may be far less concerned about indiscriminate data sharing if they do not appreciate concepts such as network interconnectedness and the inability to fully retract data once shared.

As previously indicated, another aspect the comes into play when considering security at the individual level is the diversity of learning styles that can be encountered. People learn in different ways, and so presenting the materials and framing the messages in ways that suit their individual preference is likely to yield better results (Talib, 2014). As an example of the approaches underlying this, Fleming (2006) proposes the VARK (Visual, Aural, Read/write and Kinaesthetic) model, reflecting four sensory modalities that may be used for learning information (e.g. some like to 'read' texts rather than look at 'diagrams', while others prefer to 'listen' to a lecture rather than 'doing' a practical session). Similarly, if we have an appreciation of the individual's prior knowledge and their existing predisposition towards security, then this could be used to further tailor the way in which things are presented to them. For example, are they already compliant with policy or tending toward disobedience? Are they risk averse or risk tolerant? Are they accepting of security or resistant towards it? Having appropriate insights here could affect the way in which the awareness and education messages are framed in order to reach different portions of the audience (Pattinson and Anderson, 2005). All of this, combined with a recognition of their role within the organisation, can help to tailor things more specifically to their needs.

While security is often recognised as important in concept, in practice many users see it as a chore or an overhead that is endured rather than embraced. If this is their stance when being exposed to security-related training and education, then there is clearly a different starting point to someone that has bought into the concept and is more actively ready to learn. Even if there is not active resistance, it is fair to say that cybersecurity itself is a topic area that may not naturally engage or excite the majority of the target audience. In this sense, those attempting to promote the issues are arguably disadvantaged from the outset.

If adopted in full, the contrast between the current approach to delivering security education (if indeed provision is made at all) and the proposed approach would be quite pronounced. Figure 1 illustrates this

difference, with the left-hand diagram representing the typical one-size-fits-all approach, while the right-hand side represents the approach advocated here. The latter requires a variety of information to be gathered for each user in order to establish their individual circumstances (and hence associated effort to do so), but if this were to be done then it clearly has the potential to deliver a far more tailored security education experience (which in turn would be hoped to yield better results in terms of acceptance, understanding and compliance).

The requirement for upfront data gathering points towards the desirability of designing and evaluating a questionnaire that organisations could use as a diagnostic tool to determine where their staff members are currently positioned in relation to each of the factors that may affect their learning. This in turn will help to determine the most appropriate starting point for different staff members, both in terms of their pre-existing IT and/or security knowledge, as well as the delivery mode that maps best to their learning style

6 CONCLUSIONS

Security awareness and education are indisputably important issues for today's users of information technologies and services. However, as the discussion has indicated, an effective solution is unlikely to be achieved via approach that implicitly assumes all staff to be part of a homogenised group with the same prior experience and understanding. As with other topics, there are clear benefits to be gained by tailoring and framing the learning experience to suit more specific, individual needs, and hence we can usefully adopt these wider educational principles in pursuit of improving security. Security trainers and educators need to start taking into account the learning aspects and barriers to understanding that may exist amongst their target audience.

In practice, the challenge is that we are often nowhere near even achieving a one-size-fits-all approach, let alone a tailored experience, and so the ideas outlined here are longer-term aspirations for how to take things further. Nonetheless, advancing such an approach would represent a positive step, and the authors intend to focus attention towards the type of diagnostic tool/test that would be needed to start the process. Of course, this in itself only represents one element within a broader set of requirements. Having assessed the individuals and established how their personal plans should look, there is then the requirement to be able to deliver the content in a manner that matches. Appropriate awareness, training and educational materials would then need to be sourced or created to map onto the different requirements that would emerge. In this sense, as with many other aspects of security, the desired outcome is relatively easy to describe in concept, but significantly more challenging to achieve in practice.

REFERENCES

Davies, P., and Mangan, J., 2005. "Recognising Threshold Concepts: an exploration of different approaches", *European Association in Learning and Instruction Conference (EARLI)*, 23-27 August 2005, Nicosia, Cyprus.

Fleming, N. D., 2006, *Teaching and learning styles: VARK strategies*, Second edition, Christchurch, New Zealand: Neil D Fleming.

Furnell, S., 2010. "Jumping security hurdles", *Computer Fraud & Security*, June 2010, pp10-14.

Furnell, S. and Moore, L., 2014. "Security literacy: the missing link in today's online society?", *Computer Fraud & Security*, May 2014, pp12-18.

HM Government, 2017. *FTSE 350 Cyber Governance Health Check Report 2017*, Department for Digital, Culture, Media and Sport, London, UK. July 2017. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/635605/tracker-report-2017_v6.pdf

Klahr, R., Shah, J. N., Sheriffs, P., Rossington, T., Pestell, G., Button, M., and Wang, D.V, 2017. *Cyber security breaches survey 2017*. Main report. Department for Culture, Media & Sport, April 2017.

Meyer, J. H. F. and Land, R., 2003. "Threshold Concepts and Troublesome Knowledge – Linkages to Ways of Thinking and Practising" in *Improving Student Learning – Ten Years On*. C. Rust (Ed), OCSLD, Oxford.

Pattinson, M., and Anderson, G., 2005. "Risk Communication, Risk Perception and Information Security", *Security Management, Integrity and Internal Control in Information Systems, Proceedings of IFIP TC-11 WG11.1 & WG11.5 Joint Working Conference*, Fairfax, Virginia, USA, December 2005, pp175-184.

Prensky, M., 2001. "Digital Natives, Digital Immigrants". On the Horizon: MCB University Press, 9 (5): pp1-6.

Talib, S., 2014. *Personalising Information Security Education*, PhD thesis, University of Plymouth. https://pearl.plymouth.ac.uk/bitstream/handle/10026.1/2896/2014talib10137661phd.pdf