2017-12

Security education and awareness: just let them burn?

Furnell, S

10.1016/S1353-4858(17)30122-8
Network Security
Elsevier

Short abstract (25-30 words):
Security awareness and education are frequently overlooked or provided in a one-size-fits-all approach. A more personalised approach is advocated, tailored towards the individual's circumstances and needs of the staff concerned.

Long abstract (120 words):
Lack of security awareness, training and education is a contributing factor to many security breaches, but these aspects continue to receive insufficient attention in practice. Many organisations still do nothing at all, while others rely upon one-size-fits-all solutions that are unlikely to influence all staff in a uniform manner. This discussion advocates the value of tailoring security awareness to individual needs, taking account of factors such as the individual's role, prior knowledge, learning style, and perception of security as a basis for devising personalised awareness, training and education that targets recipients more specifically. The concept is illustrated by showing how the topic of password security could be framed in different ways to suit learners of different types.

Security Education and Awareness: Just let them burn?

Steven Furnell and Ismini Vasileiou
Centre for Security, Communications and Network Research, University of Plymouth, UK

It is now readily recognised that cybersecurity is not just a technical issue, with many breaches highlighting insufficient attention towards human aspects. One of the fundamental reasons for this is that people are not naturally equipped with the skills, instincts and behaviours required to ensure appropriate protection, and so need support in order to help them understand what they should be doing and learn how to do it. However, looking at the evidence from various surveys over the years, it becomes clear that security awareness, training and education often hold the curious distinction of being overlooked as key controls, while the lack of provision is readily recognised as a key cause of incidents. As such, this remains an area in which more could be done, and how it is done could arguably be improved.

While the terms are often used interchangeably, awareness, training and education have distinct meanings and contribute towards different phases of a learning continuum. Prior work from NIST dating back to 1998 distinguishes their use in a security context as follows [1]:

- **Awareness**: To focus attention on security.
- **Training**: To produce relevant and needed security skills and competency.
- **Education**: To integrate all (security skills and competencies) into a common body of knowledge, adding a multidisciplinary study of concepts, issues, and principles.

.To an extent, whatever we call it is somewhat academic in the first instance, because current evidence suggests that we are not doing enough of it, and what *is* being done may not be delivering the desired results. The discussion here begins by presenting evidence to support the first point, before proceeding to consider how

organisations that wish to take security awareness more seriously might consider a more targeted and tailored approach for their staff.

Cyber insecurity - Unaware, untrained and uneducated?

As an indication of the current lack of provision, we can look at the findings from the 2017 Cyber Security Breaches Survey [2] in the UK, and in particular the extent to which organisations reported the provision of security-related training for their staff. Considering respondents of all sizes (from micro firms through to large organisations) only 20% of the 1,523 businesses surveyed reported that their staff had received cyber security training the last 12 months. Perhaps unsurprisingly, the picture was best amongst the 175 large firms, where 63% responded positively. However, there is also the question of what qualified as training and who was exposed to it. The definition of 'training' here included attending internal or external training, or attending seminars or conferences on cyber security. The inclusion of the latter possibly explains why IT staff were dominant amongst those reported as recipients (with 79% of those in large organisations being claimed to have received training). Meanwhile, the proportion of other staff (i.e. those that are not cyber security or IT specialists) receiving training was a meagre 29%. So, many organisations fail to provide training at all, and even those that do often fail to extend it to the general populous that might benefit from it.

Given that these particular findings are from the UK, it is worth noting that 'User Education and Awareness' is one of the UK National Cyber Security Centre's *10 Steps to Cyber Security* (which have been advocated to UK businesses since 2012). To quote from the summary, this step is described as follows:

> *"Users have a critical role to play in their organisation's security and so it's important that security rules and the technology provided enable users to do their job as well as help keep the organisation secure. This can be supported by a systematic delivery of awareness programmes and training that deliver security expertise as well helping to establish a security-conscious culture."* [3]

As with all of the 10 Steps, achieving this could actually represent more of a leap than a step, depending upon how an organisation is initially positioned, and it is interesting to note the degree to which it is achieved in practice. Referring again to the Cyber Security Breaches Survey, another question specifically polled the degree to which respondents considered themselves to be complying with each of the 10 Steps. The findings are depicted in Figure 1, with the Steps listed from left to right in order of the highest to lowest level of compliance in the most recent survey results. As can be seen, while education and awareness has seen a marginal (perhaps negligible) increase, it is still dwarfed the levels of compliance seen for more technical controls.

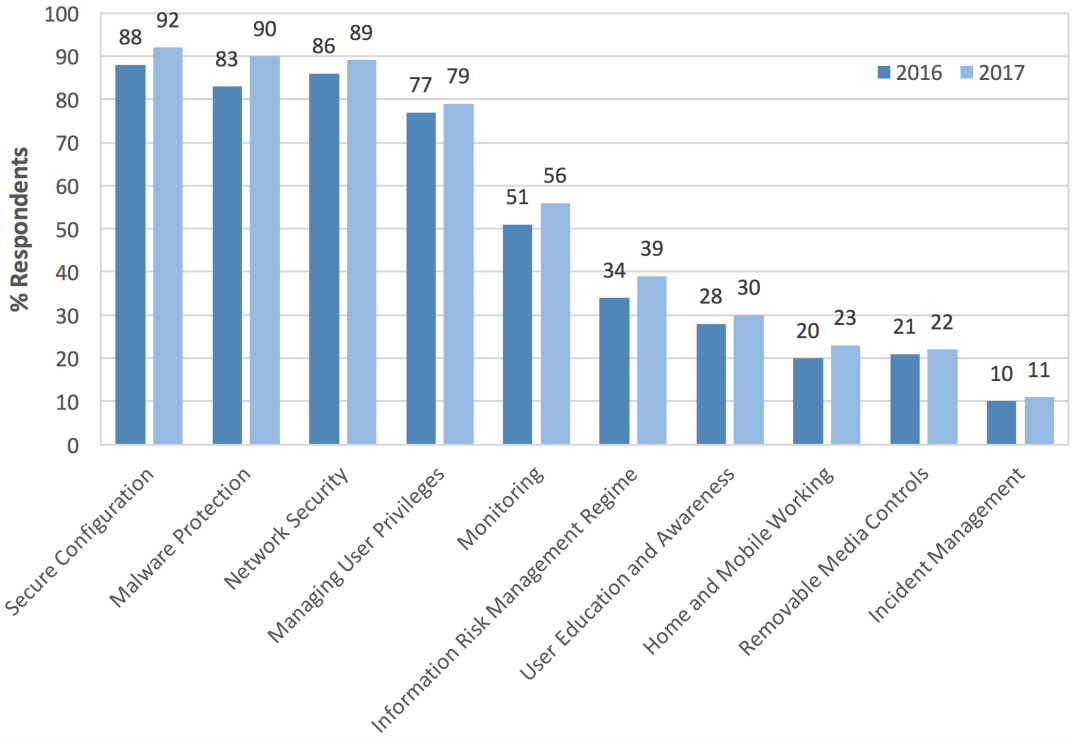

Figure 1 : Compliance with the 10 Steps to Cyber Security

Given that all of the 10 Steps are actually related to baseline security, the picture across the board should ideally be healthier than this, but for the purposes of the current discussion the key point is that less than a third of respondents consider themselves compliant with activities around awareness-raising, and generally tend to be overlooking it despite clearly giving attention towards other aspects of security. Such a finding raises the question of whether it does not receive attention because it actually does not need to. However, looking at further results from the same survey revealed that almost a fifth of respondents believed that the factors behind the breaches they experienced were staff lacking awareness or knowledge (7%) or human error (11%). Added to this, 42% of respondents were unsure of the contributing factors, so there could conceivably have been more cases hidden amongst these in which awareness and education could have been relevant to help.

Going beyond the UK and taking a broader view of the issue, Figure 2 draws upon EY's Global Information Security Survey (GISS) series, and clearly shows evidence that lack of awareness consistently contributes to the most highly-rated area of vulnerability [4].

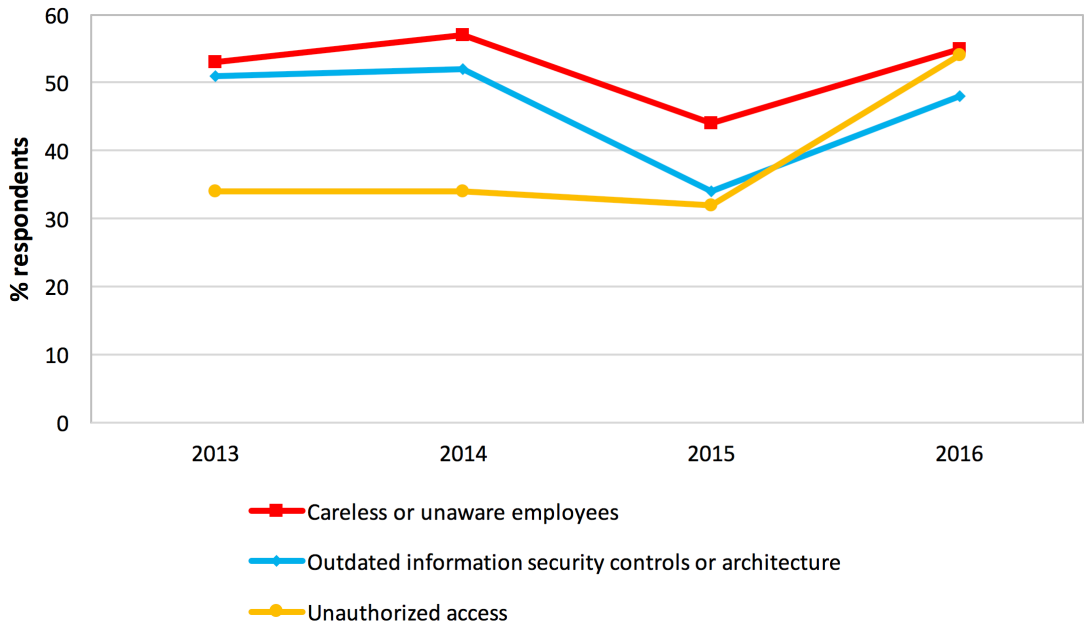

Figure 2 : Top-rated vulnerabilities 2013-2016

The 2016 survey asked respondents about the main risks associated with the use of mobile devices within the organisation, and by far and away the most significant problem was deemed to be 'Poor use awareness/behaviour', with 73% of respondents citing it (ahead of 50% and 32% indicating loss of a device and device hijacking, which were the second and third most-cited issues).

Misdirecting our efforts?

It is clear from the above that the results collectively suggest an awareness-related problem. This in turn prompts the question of what organisations are doing in response. Looking at examples of the GISS surveys from 2010 to date, Figure 3 shows whether the respondents expected to be adjusting their spending on security awareness and training in the year ahead. It is notable that the 2016 survey is the only case in which the largest proportion of respondents intend to spend *more* on the issue rather than for their expenditure to remain the same. It also made it the top-ranked area for additional spending amongst the 27 areas of security listed in the survey. Aligning with this, 55% of the respondents flagged it the area as high priority for the next 12 months (making it the third highest ranked issue, behind business continuity and data leakage prevention). Moreover, only 7% ranked it as a low priority – apparently making it the least likely area of security to be seen as low priority.

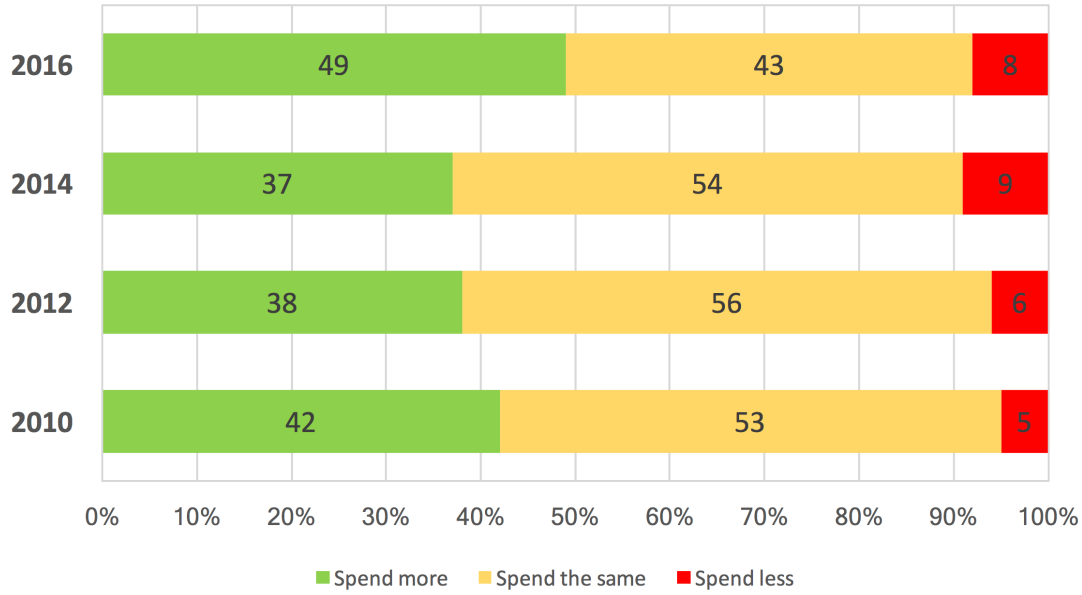

Figure 3 : Planned level of spending on Security Awareness and Training

It may be increasing, but this leaves the question of whether the spending is effective. Even in the prior years, approximately 40% of respondents were claiming they would be spending more, but it does not appear to have had any tangible effect upon the problem posed by unaware employees (which Figure 2 has already shown to have been fairly static over the most recent 4-year period, and remains the most acute area of vulnerability). So, assuming that some organisations actually did spent more (and that some who spent more in the past then continued to spend the same), why has the situation not improved? Certainly, some commentators have directly dismissed putting efforts and resources towards security awareness as "a waste of time" [5]. This is clearly a harsh view, and to be honest can be easily disproved in certain contexts. For example, prior work in terms of assessing password practices has clearly demonstrated that users' selections become demonstrably better if they are provided with guidance to support their choices (with a 30% decrease in explicitly weak passwords being observed simply by providing on-screen guidance) [6]. This helps to illustrate that some users will respond positively if they are given some indication of what they are supposed to be doing.

Nonetheless, a view also prevails that no matter how much training you throw at them, some staff *can* still end up doing the same things wrong. As a result, one can easily end up feeling like the frustrated hotelier Basil Fawlty attempting to hold a fire drill (which, if you are unfamiliar with the comedy scenario, ends with the sentiment "I don't know why we bother, we should let you all burn..."). But this does not really serve to help anyone, and unlike the fire scenario – where it would be Basil's guests that perished if they didn't pay attention – in the security awareness context it is still the organisation that ends up paying the price if its staff fail to get on board.

So, to answer the question posed in the paper title, we should not just let our staff burn, and perhaps a different approach is needed in order to get their attention and buy-in. In this sense, it is worth recognising that many current attempts at awareness-raising are implicitly based upon an assumption of one-size-fits-all. The extent to which it works, however, will very much depend upon the extent to which the chosen approach happens to match the needs of the audience receiving it. Even in the best case, there are likely to be some people that are not reached as effectively as

others, and it would be preferable to consider ways in which efforts could be more usefully tailored to the needs of the recipients. In short, the focus here is not concerned with *what* staff need to know, but rather *how* we can get them to know it.

Personalising Security Awareness, Training and Education

The idea of improving and targeting security awareness is by no means a new one. Prior works have suggested the use of various psychological triggers, such as fear appeals [7], shaming [8] and emphasis of personal benefits, some of which doubtless have the likelihood of hitting the target for some people. However, looking beyond such attempts to leverage human nature, there is potentially a lot to be learned from broader fields such as education, marketing and communications.

The key argument here is that security is more likely to be accepted and acted upon if staff feel the message is directed specifically and appropriately at them rather than generically at everyone. Not only does the latter approach fail to tailor the message to individual circumstances and needs, but it also has the potential to create an implicit impression that security can be someone else's problem (or at least no more particularly my responsibility than anyone else's). At present, any tailoring of security awareness materials is often, at best, done from the perspective of framing the messages to match the type of organisation or sector concerned (e.g. talking about patient data in hospitals versus customer data in banks). It is rare to see anything getting down to the level of what each user might actually need based on their learning style or prior predisposition towards security.

There are, however, various ways in which messages and materials can be framed and communicated to achieve better effect. For example, one might consider the effect of push or pull styles of influencing, depending upon the perceived predisposition of the staff concerned. Push approaches basically seek to tell people what to do, and are based around techniques such as reward and punishment, and assertive persuasion, whereas pull-based methods are geared towards encouraging them what to do, with methods based around participation and trust, and establishment of a common vision. Indeed, prior work has considered how these might be applied in the context of promoting security and policy compliance [9].

With the above in mind, Figure 4 compares traditional style of security awareness, training and education (where basically the same provision is pushed out to everyone), with a personalised approach that is arguably more desirable [10]. This personalisation attempts to take factors that relate to the individual who is the intended target of education, with a view to tailoring the provision more closely to their needs, preferences and perceptions. As shown in the figure, a number of factors could be usefully employed here:

- **Role:** This relates to what someone does in terms of the responsibilities they hold, and data and systems they use.
- **Prior knowledge**: Encompassing aspects such as what someone already knows about security, the organisation's policy, and their technology literacy, all of which may affect their understanding of, and response to, awareness and education efforts.
- **Barriers**: This refers to barriers to being able to apply knowledge, such as personal and cultural values that could potentially stop knowledge to be absorbed and applied.
- **Learning Style**: Recognising that people learn in different ways (e.g. the VARK - Visual, Aural, Read/write and Kinaesthetic - model reflects four sensory modalities that may be used for learning information [11]), and so presenting the materials in a manner that suit an individual's preference may deliver better results.
- **Security perception**: This essentially reflects the individual's attitude towards security. For example, are they already compliant with policy or tending toward disobedience? Are they risk-tolerant or risk-averse? Are they accepting of security or resistant towards it?

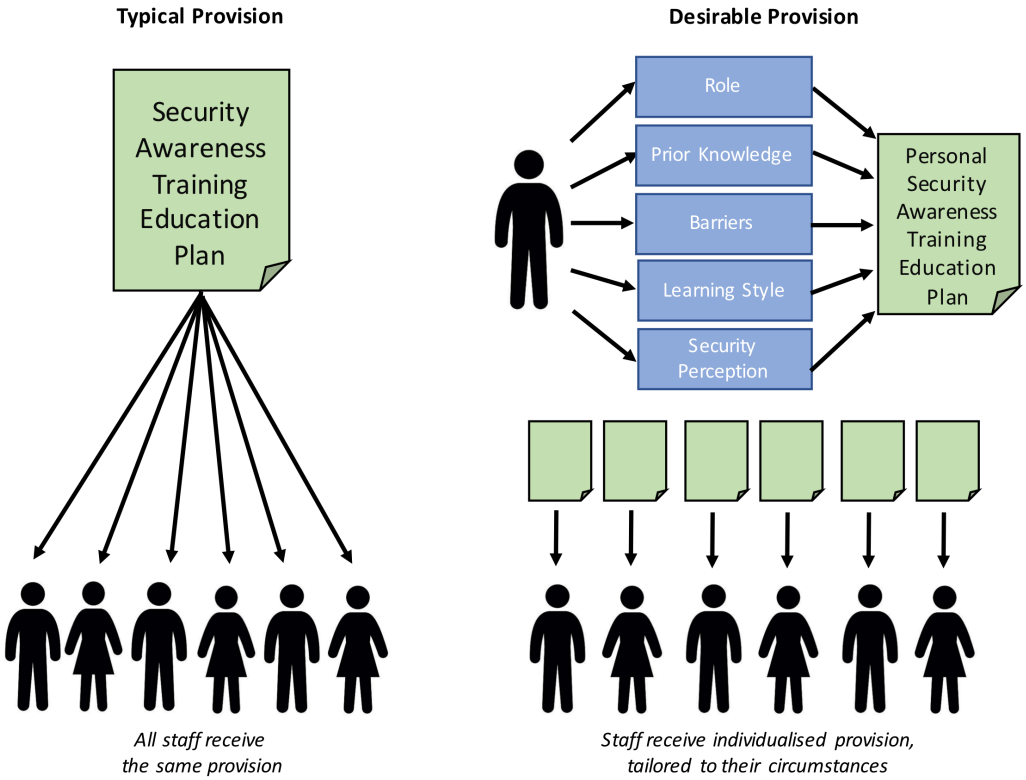

Figure 4 : Contrasting typical and desirable provision of security awareness, training and education

All of the above could be put into one category named attitude. We need to research and identify each individual's positive and negative feelings and factors towards understanding and applying security awareness. When the above are put together we can then have a full picture of someone's attitude and design a training session accordingly. When planning training we need to take into account all the possible types of learners that could attend, their potential understanding of the problem and, through the training, be able to inform and (where necessary) convince the participants about the importance of the issues. When giving out instructions, we need to ensure there has been some level of reflection in defining the types of users participating and the training session to be designed in an inclusive way. The delivery of the training should be seen as an intervention to the different types of learners that could attend and ensuring that all participants can engage. Participant engagement can be seen in many ways. Activities and instructions should be seen in a facilitative way in order to be seen not as a one-off session, but as an ongoing need for the individuals and the organisation.

In terms of how this may look in practice, Table 1 contrasts how the topic of password education might be personalised for two different staff members according to the sort of characteristics outlined above. This clearly requires more effort to engineer in the first instance, but is likely to deliver better results in terms of reaching and educating the individuals concerned.

User	Characteristics	Implications	Personal Plan
A	• Departmental Manager, with access to HR, Finance and other	Has access to highly sensitive systems, and	• Push-based influencing

	corporate information systems • Visual learner • IT-literate, but does not see the point in security, and so inclined to disregard or resist it • Has previous incidents of lax password practice	so clearly needs to use passwords appropriately Personal plan needs to combine elements of trying to bring them on-side along with clear message that they are expected and required to do it right	• Use an awareness video, appealing to the user's sense of humour and pushing the security message more softly • Support this with assertive persuasion • Ensure and emphasise awareness of sanctions for bad practice • Assist/nudge towards good practice by providing a password meter
B	• Sales executive, routinely accessing client and product databases on mobile devices while away from base. • Kinaesthetic learner • Accepting of security but lacking understanding of passwords and what passwords strength means • Not overly IT-literate, and so tends to learn tasks and operations by rote on each specific system	Will not need to be convinced to use passwords, but will need to be helped to understand how to do it properly.	• Pull-based influencing • Emphasis upon supporting the organisation and colleagues via good password practice • Provide clear description of password rules and system-specific instructions on how to do it • Provide a means for the user to practice password selection • Guide via Informative feedback from password meter

Table 1 : An example of tailoring security education to individual circumstances

Conclusions

It is clear from the evidence that security awareness and education is still an area in which many organisations are lacking, and are suffering as a consequence. Of course, no approach is going to represent a silver bullet, and some staff will remain resolutely resistant to any approaches to educate them or raise their awareness. For others, however, making an attempt to tailor towards their needs has the potential to increase their buy-in and understanding. The proposed approach of tailoring the provision is, of course, a non-trivial step, given than many are still lagging behind even in traditional provision. However, this is not a reason to disregard it, and if organisations are starting from a low base then it may be better to aim straight towards something that is more personalised and inclusive from the outset.

Moreover, leveraging alternative education strategies and approaches can potentially be taken further. For example, one area in which the authors have been active in computing and wider STEM education is Peer Learning. This could be applied in a security context by creating teams of people who would then support each other in improving security awareness and a higher level of resulting compliance. So far from just leaving people to burn as a result of their own ignorance, there are

actually many further opportunities to explore to help them avoid the fire in the first place.

About the authors

Steven Furnell is a professor of information security and leads the Centre for Security, Communications & Network Research at Plymouth University. He is also an Adjunct Professor with Edith Cowan University in Western Australia and an Honorary Professor with Nelson Mandela University in South Africa. His research interests include usability of security and privacy, security management and culture, and technologies for user authentication and intrusion detection. He has authored over 290 papers in refereed international journals and conference proceedings, as well as books including Cybercrime: Vandalizing the Information Society and Computer Insecurity: Risking the System. Prof. Furnell is the current Chair of Technical Committee 11 (security and privacy) within the International Federation for Information Processing, and a member of related working groups on security management, security education, and human aspects of security. He is also a board member of the Institute of Information Security Professionals, and chairs the academic partnership committee and southwest branch.

Ismini Vasileiou is a Lecturer in Information Systems at the University of Plymouth, with research interests including security education and technology-supported learning. She holds an EdD in Flexible Learning for Computing Degrees in Higher Education, and is a Senior Fellow of the Higher Education Academy. She has previously published on topics including blended and flexible learning, and technology-supported delivery, and has delivered a variety of invited presentations and keynote talks into relation to topics such as unconscious bias and stereotypes in STEM topics. She is also specifically involved in security education, and is a member of the related Working Group within the International Federation for Information Processing. Dr Vasileiou is currently the Chair of the STEM special interest group within the International Academic Peer Learning Leadership group, and is also actively involved in professional body activities for the computing sector, including current roles within the BCS Learning and Development Specialist Group, and BCSWomen.

References

1. Wilson, M., de Zafra, D.E., Pitcher, S.I., Tressler, J.D. and Ippolito, J.B. 1998. *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, NIST Special Publication 800-16, Technology Administration, National Institute of Standards and Technology. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-16.pdf
2. 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
3. NCSC. 2015. "10 Steps: User Education and Awareness", National Cyber Security Centre, 29 September 2015. https://www.ncsc.gov.uk/guidance/10-steps-user-education-and-awareness
4. EY. 2016. *Path to cyber resilience: Sense, resist, react. EY's 19th Global Information Security Survey 2016-17*. EYG no. 04260-163GBL, EYGM Limited. ey.com/giss.

5. Schneier, B. 2013. “On Security Awareness Training”, DARKReading, 19 March 2013. https://www.darkreading.com/risk/on-security-awareness-training/d/d-id/1139381
6. Furnell, S. and Esmael, R. 2017. “Evaluating the effect of guidance and feedback upon password compliance”, *Computer Fraud & Security*, January 2017, 5-10.
7. Johnston, A.C. and Warkentin, M. 2010. “Fear Appeals and Information Security Behaviors: An Empirical Study”, *MIS Quarterly*, vol. 34, no. 3, pp549-566.
8. Harris, M. and Furnell, S. 2012. “Routes to security compliance: be good or be shamed?”, *Computer Fraud & Security*, December 2012, pp12-20.
9. Chipperfield, C. and Furnell, S. 2010. " From security policy to practice: Sending the right messages”, *Computer Fraud & Security*, March 2010, pp13-19.
10. Vasileiou, I. and Furnell, S. 2018. “Enhancing Security Education: Recognising Threshold Concepts and other influencing factors”, to appear in *Proceedings of 4th International Conference on Information Systems Security and Privacy (ICISSP 2018)*, Madeira, Portugal, 22-24 January 2018.
11. Fleming, N.D., 2006, *Teaching and learning styles: VARK strategies*, Second edition, Christchurch, New Zealand: Neil D Fleming.