Adapting Cyber-Security Training to Your Employees

M. Pattinson[1], M. Butavicius[2], B. Ciccarello[1], M. Lillie[1],
K. Parsons[2], D. Calic[2] and A. McCormac[2]

[1]Adelaide Business School, University of Adelaide, South Australia
[2]Defence Science and Technology Group, Edinburgh, South Australia
e-mail: {malcolm.pattinson, beau.ciccarello, meredith.lillie}@adelaide.edu.au;
{marcus.butavicius, kathryn.parsons, dragana.calic,
agata.mccormac}@dst.defence.gov.au

Abstract

The aim of this paper is twofold. First, it introduces the concept of a framework of controls that relates to the human aspects of cyber security, which is adaptable to different types of organisations and different types of employees. A review of the literature confirmed that Adaptive Control Frameworks (ACFs) for cyber security exist, but only in terms of hardware and software controls. The second aim of this paper is to empirically test the effectiveness of one of these adaptive controls, namely, the type of training provided. A total of 1048 working Australian adults completed the Human Aspects of Information Security Questionnaire (HAIS-Q). This included questions relating to the types of cyber-security training they had received and how often it was provided, and a set of questions called the Cyber-security Learning Styles Inventory to identify their preferred learning styles for training. The frequency of training did not directly predict Information Security Awareness (ISA) levels. However, the extent to which the training received was matched with an individual's learning preferences was positively associated with ISA levels. This finding supports the hypothesis that if training interventions are adapted to the learning styles of individuals, their level of ISA will improve and therefore their non-malicious behaviour, whilst using a digital device to do their work, will be safer. The practical implications of this finding, as well as suggestions for further research on the ACF, are also discussed.

Keywords

Information Security (InfoSec), Human Aspects of Cyber Security (HACS), Human Aspects of Information Security Questionnaire (HAIS-Q), Adaptive Control Framework (ACF), Information Security Awareness (ISA), Learning Styles, Training.

1. Introduction

It is increasingly acknowledged that the most effective means of mitigating information security (InfoSec) risks within an organisation is to address the behaviour of employees who use digital devices to do their work (Proofpoint 2018). This implies that human vulnerabilities should be addressed in parallel with, but not instead of, implementing hardware and software controls (Furnell, S 2008).

1.1. Aim of this Paper

The aim of this paper is twofold. First, it is to introduce the concept of a framework of controls relating to the human aspects of cyber security. A review of the major International Standards shows that control frameworks exist and are recommended for non-human aspects of cyber security. For example, the Australian Standard (AS_ISO/IEC_27002 2015) provides adaptive controls for hardware and software. However, such standards do not cover controls such as education, training and awareness sessions. Consequently, there is a need to develop an ACF for these types of controls. The second aim of this paper is to validate an aspect of an ACF relating to human behaviour, in an online study. Specifically, this involves an empirical demonstration of how training controls can be adapted to an organisation's needs by providing training that matches with the preferred learning styles of employees who use digital devices to do their job.

The next section provides a review of the literature relating to ACFs, individual learning styles and ISA. This is followed by an explanation of the methods used to collect and analyse the survey data. The findings and results are then presented, limitations are acknowledged and conclusions are stated.

2. Literature Review

For the purposes of this paper, a cyber-security ACF is defined as a set of identified controls, or countermeasures together with instructions on how to implement them, such that they will prevent, deter, detect, and enable recovery from cyber-security breaches. These controls include policies, procedures, software and hardware. This will ensure that the confidentiality, integrity and availability (CIA) of digital information is maintained at an acceptable level. The framework is 'adaptive' because the controls are tailored to suit the organisation and its employees.

For the purposes of this paper, the term 'information security', that is InfoSec, refers to the preservation of the CIA of all forms of information, namely, written, printed, digital, transmitted and internet-based. On the other hand, 'cyber security' is a subset of 'information security' and refers to "protecting the CIA of digital-information assets against threats and attacks that use the internet in some manner;" (von Solms, B & von Solms, R 2018, p. 6).

2.1 Adaptive Control Framework (ACF)

ACFs are not a new concept. For example, in the field of electrical and electronic engineering, Tayebi, A and Chien, C-J (2007) proposed "a unified framework for adaptive iterative learning control design for uncertain nonlinear systems" (p. 1907). Furthermore, in the field of urban planning and development, Liu, HX *et al.* (2007) presented an ACF for traffic management systems for the betterment of emergency evacuations when natural disasters occur. In the field of InfoSec, the National Institute of Standards and Technology document (NIST 2017) describes its framework as "adaptive to provide a flexible and risk-based implementation that can be used with a broad array of cybersecurity risk management processes" (p. 6). They insist that this framework should be adapted by organisations to suit the organisation's policies and procedures.

Generally, the current information security auditing frameworks, guidelines and standards are still heavily focused on the technical components (AS_ISO/IEC_27002 2015; ISACA 2012; NIST 2017). Although these guidelines and standards recognise the importance of user awareness and training, they do not provide detailed instructions or implementable strategies, but at least they acknowledge that this area is often overlooked (Cichonski, P *et al.* 2012). Similarly, ISACA's COBIT5 (ISACA 2012) also recognises the human element, but does not include human factors as an auditable component of an IT audit. The human aspects (i.e., culture, ethics and behaviour) are considered to be the worst governed and managed areas with regard to InfoSec (ISACA 2012).

In summary, there is scant evidence of any existing literature on frameworks that include controls that are adaptable to human factors within the context of digital InfoSec. However, research by Abawajy, J (2014) showed that the most effective ISA delivery method was one that was preferred by users, although a combination of delivery methods proved to be more effective than any single method.

The next section, examines how cyber-security training can be adapted to the preferred learning styles of an employee and how this impacts on their ISA.

2.2 Learning Styles

Organisations deliver InfoSec training and awareness programs to their employees in a wide range of formats, including (but not limited to) videos, interactive modules and tests, infographics, posters, podcasts, newsletters, phishing simulations and seminars. Each of the different formats has the potential to either correspond or conflict with an employee's learning preferences. For example, a visual learner prefers to learn using predominantly visual formats. Felder, RM (1996) defines an individual's learning style as "characteristic strengths and preferences in the ways they take in and process information" (p. 1).

Researchers have developed reliable tools for measuring individual differences in learning preferences (Leite, WL *et al.* 2010). The existence of individual differences in learning preferences suggests that training may be most effective when the training mode is consistent with an individual's learning style. In the literature this is referred to as the 'meshing hypothesis', that is, an individual will experience a better learning outcome when taught in a manner that matches their learning preferences.

The meshing hypothesis and its application in education settings has received criticism from several authors due to inconclusive evidence (Kirschner, PA 2017; Newton, PM & Miah, M 2017; Pashler, H *et al.* 2008). However, several studies in the field of information systems have demonstrated the benefit of meshing learning styles and training (Recker, J *et al.* 2014). Cegielski, CG *et al.* (2011) examined learning styles and object-oriented computer programming and found that performance increases when the instructional strategies closely matched the student's preferred learning styles.

Several models and assessment tools have been developed within the learning style preference literature. Examples include the Felder, RM and Soloman, BA (2000) Index of Learning Styles Questionnaire (FSLSM), the Kolb Learning Styles Inventory (Kolb, AY 2005) and the VARK Learning Styles Inventory (Fleming, ND 2001). The VARK Learning Styles Inventory is widely used because it is brief, freely available, easy to administer and has clear practical implications for modifying the format of training to match the preferences of different learners. The simplicity of the VARK Learning Styles Inventory also means it can be easily adapted to suit a specific research purpose. Therefore, we chose to adapt the VARK model for this current study which relates to cyber-security training. The VARK model uses 16 items to assess an individual's learning preferences across four different perceptual modalities: visual (V), aural (A), read/write (R), and kinaesthetic (K). Individuals can have a single learning preference for one of the four modalities, or a preference for multiple modalities, including all four.

2.3 Information Security Awareness (ISA)

In this study, the effectiveness of a training intervention was determined by an ISA score. ISA is defined as an individual's knowledge of, and attitude towards, safe, risk-averse behaviour when using a digital device such as a workstation computer at work, a home laptop, a mobile phone or a tablet device. In other words, 'Am I doing anything that may put at risk the confidentiality, the integrity or the availability of digital data'? This data may belong to the individual, the organisation they work for, or another individual or organisation. This current research uses Parsons, K *et al.* (2014) definition of ISA. This definition is made up of the following three components:

a) What a person 'knows' about behaving in a safe manner (Knowledge);

b) How a person 'feels' about behaving in a safe manner (Attitude) and

c) What a person actually 'does' when using a digital device (Behaviour).

Parsons, K *et al.* (2017) have demonstrated that an individual's ISA, as measured by the Human Aspects of Information Security Questionnaire (HAIS-Q) (McCormac, A, Zwaans, T*, et al.* 2017), is a valid indication of how well the individual behaves when using a digital device.

3 Method

Using the Qualtrics survey platform, a population of Australian adults was invited to take part in an online study. These participants were required to be over the age of 18, currently employed, and working in Australia. The survey contained questions on demographics and ISA. To measure ISA, we used the HAIS-Q (Parsons et al., 2014; 2017) and in our study this achieved an acceptable Cronbach's alpha score of .96

overall (for further details see McCormac, A, Calic, D*, et al.* (2017). The survey also contained questions on the types of InfoSec training the participants had received and their preferred learning styles in the context of cyber security. To achieve this, the VARK Learning Styles Inventory (Fleming, ND 2001), which was originally designed to investigate general learning preferences across a range of activities, was modified and adapted to a cyber-security context. The instructions were modified to read:

> 'Choose the answers that best describe your preference when *learning about using computers for work*. For each statement, please select *more than one* if a single answer does not match your preference.'

Also, six of the original sixteen items from the VARK instrument (Fleming, ND 2001) were modified to relate to learning about computers at work (see Table 1 below). Participants responded by selecting one or more response options. Note that in Table 2 below the type of learning style is indicated by the letters V, A, R and K, but participants did not see this information when completing the survey. This new set of questions represents the Cyber-security Learning Styles Inventory.

Item	Response Options
You are participating in training that includes a test you are required to pass. You would learn most from:	Seeing examples. (V)
	Listening to the presenter. (A)
	Reading written instructions. (R)
	Watching a demonstration. (K)
Remember a time when you learned how to do something new on a computer. You learned best by:	Watching a demonstration. (K)
	Listening to somebody explaining it and asking questions. (A)
	Looking at visual cues, e.g., diagrams or charts. (V)
	Reading written explanations, e.g., a manual or blog. (R)
You want to learn a new computer program. You would:	Read the written instructions that came with the program. (R)
	Talk with people who know about the program. (A)
	Learn how to use it through trial and error. (K)
	Follow the diagrams in the instructions. (V)
I like websites that have:	Things I can click on or interact with. (K)
	Interesting design and visual features. (V)
	Interesting written descriptions, lists or explanations. (R)
	Audio channels where I can hear podcasts, radio programs or interviews. (A)
Do you prefer a presenter or instructor who uses:	Demonstrations or practical sessions. (K)
	Question and answer sessions or guest discussions. (A)
	Handouts, books, or readings. (R)
	Diagrams, charts or graphs. (V)
You have completed a test at the end of a training course, and would like to receive feedback. You would like to receive feedback by:	Having your results displayed visually, e.g., on graphs or diagrams. (V)
	Using examples from what you have done. (K)
	Having someone talk you through it. (A)
	Using a written description of your results. (R)

Table 1: Cyber-security Learning Styles Inventory

Participants were also asked two questions about the nature of cyber-security training they had received at work. The first question related to the frequency of such training (see Training Frequency in Table 2 below), with 7 forced-choice options. Only 3.5% of the participants selected the final response option of 'Other (Please specify)' and an analysis of the associated open-text responses did not reveal any consistent themes. Therefore, these responses were excluded from analysis. The second question, about the cyber-security training that participants had received, related to the mode of training (see Training Type in Table 2 below). The response options were modelled on the VARK instrument (Fleming, ND 2001), but adapted to InfoSec education and training, and participants responded on a five point Likert scale (where '1' = 'Strongly disagree' and '5' = 'Strongly agree').

Item description	Item	Response Options
Training Frequency	How frequently does your place of work provide information security education, training or awareness programs?	Never
		Every two years
		Annually
		Twice a year
		Every three months
		At least once a month
		Other (please specify)
Training Type	Please indicate whether the following statements apply to the security education, training and awareness programs that you have received in your place of work	They include speaking and listening (e.g., discussions, seminars). (A)
		They include reading or writing (e.g., handouts, note-taking). (R)
		They include visual depiction of information (e.g., diagrams, graphs, charts). (V)
		They include experience and practice, either simulated or real (e.g., real-life examples, demonstrations, guest lecturers). (K)

Table 2: Training Items

4 Results

After filtering and quality checks, 1,048 responses (from participants that were over the age of 18, currently employed, and working in Australia) were analysed. Of these, 51% were females and participants were evenly distributed across age categories, with 11.8% of them aged between 18 and 29, 23.8% aged between 30 and 39, 21.4% aged between 40 and 49, 23.4% aged between 50 and 59 and 19.3% aged 60 and over.

The six items of the Cyber-security Learning Styles Inventory were summed to create Visual, Aural, Read/Write and Kinaesthetic subtotals for each participant with a range of 0 to 6. These were then recoded such that sub-totals of more than 4 were designated as ‘Preferred’ and the remaining were coded as ‘Not preferred’. Scores on the Training Type question were recoded such that where participants indicated that they ‘Agree’ or ‘Strongly agree’ on the Likert scale they were classified as ‘Received’ whilst all other responses (i.e., ‘Disagree’, ‘Strongly disagree’ and ‘Neither agree nor disagree’) were classified as ‘Not received’.

Overall analysis of training modes indicated a disparity between the modes of training that people preferred, compared to the mode of training they had received. Preliminary analysis of the responses to ‘Training Modes Received’ showed that, across the sample, the training modes were evenly split across the four learning-style categories (see Table 3 below). However, an examination of the 'Preferred Learning Styles' showed a different pattern of results, with a higher percentage of respondents indicating that kinaesthetic training would be their preferred method for learning about using computers for work.

	Visual	**Aural**	**Read/write**	**Kinaesthetic**
Training Modes Received	55.7%	57.8%	55.7%	57.9%
Preferred Learning Styles	24.4%	28.6%	35.1%	45.5%

Table 3: Overall comparison between training modes received and preferred learning styles.

To more closely examine the relationship between preferred and received modes of training, the data was examined at an individual level. A new variable, 'Training Match', was calculated to indicate whether the learning style preference matched with the training mode received or not. A score of one indicated that the participant received training in a least one style that was consistent with their learning preferences. All other participants received a score of zero. In addition, participants who responded inconsistently to the questions by indicating that they received no cyber-security training for the 'Training Frequency' question but indicated that they had received certain types of cyber-security training in the 'Training Type' question were classified as a Non-match (i.e., 0). Overall, 39.6% (N = 415) of the sample were classified as having received matched training.

An examination of the Pearson correlation coefficient between the variables (see Table 4 below), showed that Age, Gender and Training Match all correlated significantly with ISA. In addition, Age correlated significantly with Gender whilst Training Frequency was also positively and significantly correlated with Training Match.

In order to tease apart the relative contribution of these variables in predicting ISA, a three-stage hierarchical multiple linear regression (refer Table 5 below) was conducted. In the multiple regression, there were no signs of multi-collinearity with Variance Inflation Factors (VIF) for all independent variables less than 2. In addition, there was no evidence of outliers with Cook's distances being less than 1 for these variables. In the first stage of the regression, Age and Gender were entered to control for the effects of these demographic variables as demonstrated in previous research (McCormac, A, Zwaans, T*, et al.* 2017). In the second stage, Training Frequency was entered to examine the role of increased training opportunities. In the third and final stage, Training Match was entered to examine whether matching training mode to learning style for cyber-security training improved ISA over and above the effects of demographic variables and increased training frequency.

Variable	Mean	SD	VIF	1	2	3	4
1. Age Range	N/A	N/A	1.04				
2. Gender	N/A	N/A	1.03	-.18**			
3. Training Frequency	2.5	1.6	1.65	-.06	-.02		
4. Training Match	.4	.5	1.65	-.02	-.01	.63**	
ISA	257.2	32.1	-	.27**	.08*	.06	.12**

(= correlation significant at the .05 level, ** = correlation significant at the .01 level, two-tailed).*

Table 4: Descriptive statistics and correlations

At Stage 1, both Age and Gender were significant and together explained 8% of the variance in ISA (*F*(2,1008) = 46.63, *p* < .001). In Stage 2, adding Training Frequency improved the fit of the model, and the Training Frequency variable was significant. However the overall fit increased by less than half a percent (*F*(3,1007) = 33.55, *p* <.001). In Stage 3, the additional Training Match variable was significant, however, its inclusion caused Training Frequency to be removed from the final model (*F*(4,1006) = 27.74, *p* < .001). In other words, while Training Frequency appeared to be associated with improved ISA in the second model, much of its contribution was negated once the more predictive variable of Training Match, with which it covaries, was included in the final model. Overall, this final model explained approximately 10% of the variance in the data with the strongest predictor being Age followed by Gender and then Training Match.

5 Discussion of Results

The frequency of training did not appear to directly predict ISA. However, the extent to which the training received actually matched (i.e. meshed with) an individual's learning preferences was positively associated with ISA. Increased frequency of training may be important only in so much as it may provide greater opportunity for the training messages to be presented in a variety of formats. This, in turn, would increase the likelihood that an employee's preferred learning style was 'covered'. Ultimately, it was the matching of the training mode with the employee's preferred learning style (for cyber-security training) that was positively associated with their ISA score. This finding supports the ACF hypothesis; namely, that training interventions should be adapted to the needs of the individuals for higher ISA scores and therefore more risk-averse InfoSec behaviours.

Our results also validated previous research that showed that older employees and females tended to have better ISA (McCormac, A, Zwaans, T, *et al.* 2017). In fact, Age and Gender were stronger predictors of ISA than the variables associated with training. However, changing the age and gender profile of an organisation's employees is not ethical or practical. In contrast, modes of training may be easily measured and this information can be used to address training needs to directly improve ISA.

Variable	Model 1			Model 2			Model 3		
	B ***(SE)***	***β*** *standardised*	***t***	***B*** ***(SE)***	***β*** *standardised*	***t***	***B*** ***(SE)***	***β*** *standardised*	***t***
Age Range	6.95 (.75)	.28	9.26**	7.07 (.75)	.29	9.43**	7.04 (.75)	.29	9.42**
Gender	8.46 (1.96)	.13	4.32**	8.61 (1.95)	.13	4.40**	8.59 (1.95)	.13	4.41**
Training Frequency				1.63 (.62)	.08	2.62*	.10 (.79)	.01	.12
Training Match							7.81 (2.53)	.12	3.08**
Adj *R²*	.08			.09			.10		
Δ Adj *R²*	.08			.05			.01		
F	46.63			33.55			27.75		

(= correlation significant at the .05 level, ** = correlation significant at the .01 level, two-tailed).*

Table 5: Summary of hierarchical, three-stage, multiple linear regression analysis of variables predicting ISA

6 Limitations and Future Directions

In the real world, it may be impractical to survey the training mode needs of all staff and then tailor the training to each individual preference. However, it may still be beneficial to understand learning preferences within certain organisational teams or groups. Rather than surveying all the employees, this approach would involve surveying only a sample of people in different work areas using the Cyber-security Learning Styles Inventory. This learning style profile could then be used to tailor training packages for these work areas (rather than individuals). However, it is a question for further research as to how much ISA can be improved by tailoring training at a group level. Further research should also investigate how individual tailoring of other aspects of the ACF (e.g., cyber-security awareness messaging such as intranet posts and posters) may improve ISA.

7 Conclusions

This paper reported on a research project that established the need for a framework of human controls that could be adapted to the different types of employees within an organisation. This paper also reported on the results of an online survey that collected and analysed data relating to one of these adaptive controls, namely, the cyber-security training that employees had received, and its impact on their naïve and accidental InfoSec behaviour when using a digital device for work.

The concept of an ACF is referred to by International Standards (AS_ISO/IEC_27002 2015; ISO_3100 2018; NIST 2017) and by training organisations Proofpoint (2018) and MediaPro (2017) as an important approach to mitigating cyber-security risks. Despite this need, this study found that current standards and guidelines are devoid of any such mechanism when it comes to educating, training and communicating with employees. More specifically, a review of the standards mentioned above revealed no published guidance on human-based controls. This led to the hypothesis that if cyber-security training is adapted (i.e. meshed) to the needs of an individual, the naïve and accidental behaviour of this individual should be safer. Hence, this paper presented a case study which supports this hypothesis by showing that an individual's level of ISA is increased if the training is meshed with an individual's preferred learning style.

There is a developing body of academic literature focusing on the human aspects of cyber security, such as user vulnerability to phishing attacks (Furnell, S 2007), ISA (Parsons, K *et al.* 2014) and InfoSec culture (Da Veiga, A & Eloff, J 2010). The ACF conceptualised and tested in this paper seeks to formalise this research into practical guidelines that can be implemented in any organisation to evaluate and improve their InfoSec posture.

In line with this goal, our research suggests that an organisation could improve ISA by simply increasing the amount of training it provides. However, this is an inefficient and costly strategy. Rather than just increasing the amount of training, an organisation can save time and money by ensuring that the training is provided in formats relevant, or matched, to its employees. This is consistent with the ACF such that the human-based control known as 'training' is most effective when it is adapted to the needs of the employees and that this, in turn, should improve an organisation's level of security of its digital information assets.

8 References

Abawajy, J 2014, 'User preference of cyber security awareness delivery methods', *Behaviour & Information Technology*, vol. 33, no. 3, pp. 237-248.

AS_ISO/IEC_27002 2015, *Information Technology - Security Techniques - Code of practice for Information security management,* (27002:2015), Standards Australia.

Cegielski, CG, Hazen, BT & Rainer, RK 2011, 'Teach them how they learn: Learning styles and information systems education', *Journal of Information Systems Education*, vol. 22, no. 2, pp. 135-146.

Cichonski, P, Millar, T, Grance, T & Scarfone, K 2012, 'Special Publication 800-61 Revision 2', *Computer Security Incident Handling Guide*.

Da Veiga, A & Eloff, J 2010, 'A framework and assessment instrument for information security culture', *Computers & Security*, vol. 29, no. 2, pp. 196-207.

Felder, RM 1996, 'Matters of style', *ASEE prism*, vol. 6, no. 4, pp. 18-23.

Felder, RM & Soloman, BA 2000, 'Learning styles and strategies', *At URL: http://www. engr. ncsu. edu/learningstyles/ilsweb. html*.

Fleming, ND 2001, *Teaching and learning styles: VARK strategies*, IGI Global.

Furnell, S 2007, 'Phishing: can we spot the signs?', *Computer Fraud & Security*, vol. 2007, no. 3, pp. 10-15.

Furnell, S 2008, 'Securing the Human Factor', in H Lacohée, P Cofta, A Phippen & S Furnell (eds), *Understanding Public Perceptions: Trust and Engagement in ICT Mediated Services*, International Engineering Consortium.

ISACA 2012, *COBIT5: A Business Framework for the Governance and Management of Enterprise IT*, ISACA, USA.

ISO_3100 2018, *Risk management - Guidelines*, International Standards Organization.

Kirschner, PA 2017, 'Stop propagating the learning styles myth', *Computers & Education*, vol. 106, pp. 166-171.

Kolb, AY 2005, 'The Kolb learning style inventory–version 3.1 2005 technical specifications', *Boston, MA: Hay Resource Direct*, vol. 200, p. 72.

Leite, WL, Svinicki, M & Shi, Y 2010, 'Attempted validation of the scores of the VARK: Learning styles inventory with multitrait–multimethod confirmatory factor analysis models', *Educational and Psychological Measurement*, vol. 70, no. 2, pp. 323-339.

Liu, HX, Ban, JX, Ma, W & Mirchandani, PB 2007, 'Model reference adaptive control framework for real-time traffic management under emergency evacuation', *Journal of urban planning and development*, vol. 133, no. 1, pp. 43-50.

McCormac, A, Calic, D, Butavicius, M, Parsons, K, Pattinson, M & Lillie, M 2017, 'Understanding the Relationships between Resilience, Work Stress and Information Security Awareness', in S Furnell & N Clarke (eds), *Proceedings of the 11th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2017),* Adelaide, South Australia, pp. 80 - 90.

McCormac, A, Zwaans, T, Parsons, K, Calic, D, Butavicius, M & Pattinson, M 2017, 'Individual differences and information security awareness', *Computers in Human Behavior*, vol. 69, pp. 151-156.

MediaPro 2017, *Best practices guide for comprehensive employee awareness programs*, viewed 12 June 2018, <https:www.mediapro.com/blog/white-paper-best-practices-guide-comprehensive-employee-awareness-programs/>.

Newton, PM & Miah, M 2017, 'Evidence-Based Higher Education–Is the Learning Styles ‘Myth’Important?', *Frontiers in psychology*, vol. 8, p. 444.

NIST 2017, *Framework for improving critical infrastructure cybersecurity*, National Institute of Standards and Technology.

Parsons, K, Calic, D, Pattinson, M, Butavicius, M, McCormac, A & Zwaans, T 2017, 'The human aspects of information security questionnaire (HAIS-Q): two further validation studies', *Computers & Security*, vol. 66, pp. 40-51.

Parsons, K, McCormac, A, Butavicius, M, Pattinson, M & Jerram, C 2014, 'Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q)', *Computers & Security*, vol. 42, pp. 165-176.

Pashler, H, McDaniel, M, Rohrer, D & Bjork, R 2008, 'Learning styles: Concepts and evidence', *Psychological science in the public interest*, vol. 9, no. 3, pp. 105-119.

Proofpoint 2018, *The Human Factor - people-centred threats define the landscape*, USA, viewed 7 June 2018, <www.proofpoint.com/>.

Recker, J, Reijers, HA & van de Wouw, SG 2014, 'Process model comprehension: the effects of cognitive abilities, learning style, and strategy', *Communications of the Association for Information Systems*, vol. 34, no. 9, pp. 199-222.

Tayebi, A & Chien, C-J 2007, 'A unified adaptive iterative learning control framework for uncertain nonlinear systems', *IEEE Transactions on Automatic Control*, vol. 52, no. 10, pp. 1907-1913.

von Solms, B & von Solms, R 2018, 'Cybersecurity and information security–what goes where?', *Information & Computer Security*, vol. 26, no. 1, pp. 2-9.

Acknowledgements. This project is supported by the Defence Science & Technology Group (DSTG)