Personality Type – A Valid Indicator of Security Champions?

T.Gabriel[1], S.M.Furnell[1] and K-L.Thomson[2]

[1]Centre for Security, Communications and Network Research, Plymouth University, Plymouth, UK
[2]School of Information and Communication Technology, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa
e-mail: info@cscan.org

Abstract

Information security training and awareness raising are widely recognised as particularly difficult areas to address. Aspects such as organisational behaviour, the incorporation of educational learning theories and adult education best practise appear to be commonly overlooked in existing security training approaches.

An initial study into security assessment of personnel via psychometric testing appears to provide a cost effective solution. A security assessment questionnaire is designed and constructed the results of which are compared with personality features from psychometric tests using multiple regression. Statistical analyses reveal that a number of personality attributes appear to correspond with an information security inclination. In particular the combination of 'imagination' and 'immoderation' appear to provide good predictive results.

Keywords

Information security, personality, psychometrics, organisational behaviour, educational theory.

1 Introduction

The difficulties of implementing effective security training are widely recognised as long standing issues; Lacey (2009) providing excellent coverage. It seems appropriate, therefore, to investigate the educational difficulties associated with the area. The focus of this paper is to understand the main problems at a theoretical level and suggest recognised approaches to minimising their effects. The main topics are considered to be organisational and group behaviour, adult education and learning theory, and crucially, the identification of staff that are supportive or averse to security related concepts and procedures.

2 Organisational behaviour

The effects of peer pressure on individuals' behaviour are a well known and documented phenomenon; the consequences of which go largely unnoticed among day-to-day activities. In the context of security training it can be a significant barrier, providing a largely transparent resistance to change throughout the workforce. In the

majority of cases a person joining a group, very quickly and unwittingly adopts its attitudes and practises. The consequences, when a person joins a group that is not security conscious, are clear.

A less well-known (and perhaps less understood) phenomenon is minority influence; as studied by Moscovici, Lage and Naffrenchoux (1969) and Asch (1956). Under particular circumstances a very few, or even a single, individual can slowly influence the majority, effectively reversing the commonly held view of peer pressure (majority effect). One significant difference is the speed of change. Minority influence is a slow, but again, subliminal process. The requirements for this phenomenon are a moderate degree of authority, a consistent yet flexible opinion, repetition, and persistence. When the above are viewed from educational perspectives it can be seen that these are common attributes to many forms of education. Education is commonly a slow constant pressure applied to the majority (students) by the minority (the educator) to impart new and alternative perspectives.

3 Educational Theory

Armitage et al (2007) acknowledge the shortfalls of learning theories but accept that they continue to provide a useful framework on which to build.

Sensory stimulation theory suggests that learning best occurs when each of the senses are stimulated in unison. Reinforcement learning is based upon reward and sanction. Cognitive-Gestalt approaches relate to pattern, relationship and insight based upon prior experience. Facilitation theory sees the educator employed as a learner's assistant – where learner and educator are equals. Action learning is a not too dissimilar approach but the emphasis shifts toward learners sharing their views and experiences amongst themselves with the educator playing a steering and supporting role.

Oxford Brookes University (Dunn, 2002) provides an insightful and succinct view of these and more learning theories.

In addition Tough reveals important personal characteristics which will benefit the trainer; he or she...

"... views personal interaction with the learner as a dialogue, a true encounter in which he or she listens as well as talks. Help will be tailored to the needs, goals, and requests of this unique learner. The helper listens, accepts, understands, responds, helps. These perceptions are in sharp contrast to those of "helpers" who want to control, command, manipulate, persuade, influence and change the learner.

...Such a helper perceives the learner as an object, and expects to do something to that object. He is not primarily interested in that person as a person, and in his needs, wishes, and welfare." (Tough 1979 p91)

By contrast, an afternoon browsing information security sites including NIST, Microsoft, SANS, ICO and ISACA reveals no mention of trainer selection. The Get Safe Online (2010) website mentions the need to "train the trainer" but the idea is not

expanded upon. The ENISA (2010) "Train the trainers - SMEs security" page contains links to materials that can be used in trainer training, but these offer only a walk through of the training material provided. Google searches for "training the trainer" and "trainer training" in relation to information security also produced nothing of relevance. A common theme however is the approach taken by, and available from, the National Institute of Standards and Technology (NIST) website...

"Roles and responsibilities of agency personnel who should design, develop, implement, and maintain the awareness and training material, and who should ensure that the appropriate users attend or view the applicable material;..." (Wilson and Hash, 2003)

The language used gives the impression that trainees will have material pressed upon them, that they will be summoned to sessions, and will have little if any say in the content presented. Such an approach appears to be in direct contradiction to learning theories and to Knowles' (2005) views on adult education.

In addition, no consideration is given to the role, skills, character and influence of the educator. Is this one of the missing pieces in the security puzzle? Have security specialists and business managers focussed so strongly upon content (if security training has been considered at all) that the psychological and educational theories have been overlooked? If this is the case, perhaps a softer but persistent approach is required; one that advocates educational theory and the exploitation of minority effect? This concept seems to fly in the face of current views however, the consensus being (from those who care sufficiently) to get tough on security issues.

4 Mentoring

If a move toward gentler but persistent training is indeed appropriate, coaching or mentoring appears to provide the right approach. Organisational behaviour becomes less of an issue when colleagues carry out the training. The effort is sustained and relevant to the role, the mentor is readily available to offer advice and assistance, and is better placed to monitor behaviour. In effect the trainer is well known, on hand, helpful and supportive, and advice is relevant – aspects recognised by Knowles (2005) as beneficial to adult learning. In addition the unwittingly erected barriers of classroom environments are removed – learners often bring with them the (often negative) personal experiences of similar previous activities, discomfort, a potential for underachievement, embarrassment, lack of relevance and more. There are a number of downsides to mentoring however, namely the high set up costs and effort of mentor training and selection.

5 Mentor selection

The quote below is, in the authors' view, as important in a mentoring environment as in a classroom situation. The presentation skills mentioned are perhaps less relevant – the contact being less formal – but selecting an individual with the interpersonal skills to fulfil the role is still a priority.

"If you're going to do your training in the classroom, you've got to be prepared to find good presenters – whether that's someone already in your organization, or hiring someone from outside.

At the risk of generalizing, your information security and/or IT staff are seldom the right people to be handling this. Not only are they rarely comfortable in presenting to audiences, they tend to allow themselves to be drawn into too much technical detail…" (Security Awareness Training, 2010)

But equally, an interest and affinity with security concepts is necessary. The social skills required can be largely deduced from daily behaviour and interaction with others, but security interests are less likely to be recognisable. In addition latent interest might exist, but through lack of experience or exposure to materials, remain unrecognised even by an individual themselves. What is needed is a means of identifying individuals with security interests; be they latent or not. These persons might then be offered the opportunity to become mentors and trained to carry out the responsibility.

On the other hand, security assessments, standards and processes for personnel selection, or any other purpose, appear to be conspicuous by their absence, and would not in any case determine the *qualities* of those who lack security knowledge or experience. This is a potentially critical point in promoting sufficient numbers to the role of security champion within an organisation, department or team. The numbers of security aware individuals (coupled with the required interpersonal skills) are perceived to be low - a quick and at least moderately accurate selection process of those with latent talent is needed.

6 Personnel selection using psychometrics

Until this point little if anything new has been discussed other than bringing together theories and elements from fields typically removed from the subject of security training. Here however, a novel selection process is proposed and an initial study conducted.

A group of 20, white, European employees and managers, who work within the technology sector were appraised by colleagues and awarded security ratings. The security assessments consist of 17 questions and are based upon 5 categories: passive compliance, active compliance, external pressures, motivation and awareness. Of these, only motivation and active and passive compliance are used within the regression analysis. Awareness and external pressure are considered much less attributable to an individual's personality and are excluded on this basis. In parallel the group undertook personality tests from the International Personality Item Pool; a freely available test instrument similar to the copyright protected NEO-PIR. Available via a research website, the test's short form was used, consisting of 120 questions and taking each individual around 15 minutes to complete. Results consist of percentage scores for thirty personality attributes. The entire group were retested at approximately monthly intervals, the results of which reveal good inter-test consistency. Security assessment results, however, displayed greater inter-assessor variations as might be expected from survey based data. 3 assessors where

employed; selected as a result of their (moderate) security knowledge, interest and how well they know the working practises of fellow participants.

When multiple regression analysis is used to compare the security assessments and personality test results obtained, a number of personality factors with moderate correlations are revealed; primarily imagination and immoderation, as shown in Figure 1.

```
Call:
lm(formula = secData$SecAssessment ~ secData$Imagination + secData$Immoderation)

Residuals:
     Min       1Q   Median       3Q      Max
-19.1630  -8.1126  -0.6558   7.8306  21.9328

Coefficients:
                    Estimate Std. Error t value Pr(>|t|)
(Intercept)          59.76113    5.66338  10.552    7e-09 ***
secData$Imagination   0.28607    0.09683   2.954  0.00888 **
secData$Immoderation -0.24418    0.09930  -2.459  0.02495 *
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1

Residual standard error: 12.25 on 17 degrees of freedom
Multiple R-squared: 0.4503,     Adjusted R-squared: 0.3857
F-statistic: 6.964 on 2 and 17 DF,  p-value: 0.006178
```

Figure 1 - Multiple Regression Results

The key points above are that p is significantly below the commonly recognised value of 0.05 (0.0062) indicating that the probability of the result being incorrect is just 0.62%. The multiple R^2 value is substantial (0.45), equating to a large (according to Cohen (1992)) effect size: 0.82 – see Figure 2 below.

The sample population size of twenty, was initially considered too small to produce results of significance, but power tests reveal that regression using two independent variables alone (personality factors) can identify medium to large effect sizes – as defined by Cohen (1992).

Power test results - Figure 2 - indicate that given v (population size - 1 - the number of independent variables used: 20-1-2 =17) the regression analysis power (96%) exceeds the standard benchmarks of 80 or 90 percent. Further tests reveal that the use of 3 or more independent variables does not meet the 80% criteria, in turn highlighting that alternative solutions based upon 3 or more variables may remain undiscovered.

```
> library(pwr)
>   R2 = 0.4503
>   f2 <- R2 / (1 - R2)
> pwr.f2.test(u = 1, v = 17, f2 = f2, sig.level = 0.05, power = NULL)

     Multiple regression power calculation

              u = 1
              v = 17
             f2 = 0.8191741
      sig.level = 0.05
          power = 0.9602808
```

Figure 2 - Power Calculation Results

Therefore, imagination and immoderation provide the best model so far revealed within this data set. Where regression is conducted in parallel against these two variables, strong results (taking the social data factor into consideration) indicate that a predictive measure is available.

Security Rating = (imagination score * 0.28607) +
(immoderation score * -0.24418) + 59.76

When the boundaries of this equation are explored the model's limitations are revealed; the maximum and minimum scores achievable being 88 and 35 respectively using scores of 1 to 100. However, this may not detract from its potential to subdivide a population into 3 security groups which, based upon a 15 minute test, might still provide a useful function in the absence of other options.

It should be noted that correlation must not be confused with causation, however. An unknown third variable, associated with both imagination and immoderation, might be at work.

A key observation of this study is that distinguishing features appear to lie with combinations of personality facets as opposed to the trait level. Traits being groups of facets measuring related attributes. As far as can be determined little if any career-based analysis has been conducted at this level of detail, and none whatsoever has been found with regard to information security and its various roles.

7 Conclusions

The use of personality tests to identify an individual's security inclination remains unproven in both a theoretical and practical sense. It ignores too the ability of an individual to take up and succeed in the mentoring role. However, a parallel investigation into the personality attributes of successful adult educators may reveal that similar descriptive factors exist.

Results for thirty personality attributes were obtained. The 8 strongest indicators of an inclination for security concepts found thus far are; imagination, emotionality, anxiety altruism, immoderation vulnerability, morality and openness to experience.

Immoderation – a tendency to react in favour of short term gains as opposed to longer term consequences – provides the only negative correlation. The weakest indicators found are gregariousness, self-discipline, neuroticism, trust and dutifulness.

It should again be noted that correlation must not be confused with causation - or lack of it. An unknown third variable, associated with any combination of trait or facet may be at work.

The results obtained thus far indicate that personality test results may possess a predictive value. Where further investigations reveal similar results and establish a relevance to the general population, the approach might be used in wider and, as yet, unforeseen contexts in addition to the proposed trainee categorisation and mentor or security champion selection processes.

Current results show predictive levels that might be used to categorise individuals into one of perhaps three security inclination groups. Initial impressions are that this process may lack precision, but in the absence of other approaches and for the purposes of targeted training it is considered to be of a sufficient level of definition. Where the aim is to identify mentors it is highly likely that an interview process will need to follow, confirming the findings, ensuring that candidates are willing participants and are capable of fulfilling the mentor role.

The combination of accurately identifying suitable individuals, training them in the necessary educational and psychological principles, and empowering them in the workplace with a view to the long term, is in the authors' opinion a more effective way of increasing security awareness and compliance. The cost and effort required, especially by businesses that barely recognise the need, will, however, lead to its rejection in almost all cases at the present time. The proposed approach is not cheap, but in the longer term may well prove cost effective where widespread compliance levels are considered essential.

This in turn raises the issue of just what is required for senior managers to recognise and fulfil security requirements. The answer almost certainly lies in legislation and wider publicity. Where organisations suffer data losses the full consequences of a breach should by widely publicised in a constructive manner. Only when the financial costs and reputational damage are recognised and fully acknowledged by senior managers will the need be addressed.

Primarily, future research suggestions include reviewing and refining the assessment process after conducting greater analytical investigation of assessment results. Regression analysis should then be repeated on larger data sets, to establish the legitimacy of current findings.

8 References

Armitage,A., Bryant,R., Dunnill,R., Flannagan,K., Hayes, D., Hudson, A., Kent, J., Lawes, S., Renwick, M., (2007*). Teaching and Training in Post-Compulsory Education. (3rd ed)*, Maidenhead, Open University Press. ISBN 0-3352-2267-6

Asch,S.E., (1956). *Studies of independence and conformity; A minority of one against a unanimous majority*, Psychological Monographs, Vol. 70(9)

Cohen,J., (1992). *A Power Primer*, Psychological Bulletin, Vol 112(1), July 1992, 155-159. http://137.148.49.106/offices/assessment/Assessment%20Reports%202006/CoS/Psychology%203%20of%203.pdf (Accessed 11/7/2010)

Dunn, L., (2002). *Learning and Teaching Briefing Papers Series - Theories of Learning*, http://www.brookes.ac.uk/services/ocsd/2_learntch/briefing_papers/learning_theories.pdf (Accessed 02/07/2010)

ENISA (2010). http://www.enisa.europa.eu/media/news-items/train-the-trainers-smes-security http://www.enisa.europa.eu/act/ar/deliverables/2010/e-mail-security_train-the-trainer-guide (Accessed 03/07/2010)

Get Safe Online (2010). http://www.getsafeonline.org/nqcontent.cfm?a_id=1108 (Accessed 03/07/2010)

ISACA, (2009). *An Introduction to the Business Model for Information Security*, Rolling Meadows, Illinois.
http://www.isaca.org/Knowledge-Center/Research/Documents/Intro-Bus-Model-InfoSec-22Jan09-Research.pdf (Accessed 03/07/2010)

IPIP, (2010). *International Personality Item Pool: A Scientific Collaboratory for the Development of Advanced Measures of Personality Traits and Other Individual Differences*, http://ipip.ori.org/ (Accessed 20/12/2009)

Knowles, M. S., Holton, E. F., & Swanson, R. A., (2005). *The Adult Learner (6th ed.).* Burlington, Massachusetts, Elsevier Butterworth-Heinemann, ISBN 0-7506-7837-2

Lacey, D., (2009). *Managing the Human Factor in Information Security*. Chichester, John Wiley & Sons, ISBN 978-0-470-72199-5

Moscovici, S., Lage, E., & Naffrechoux, M. (1969). *Influence of a consistent minority on the responses of a majority in a color perception task*. Sociometry, 32(4), 365-380

Security Awareness Training, (2010). http://www.security-awareness-training.com/ (Accessed 03/07/2010)

Tough, A., (1979). *The Adults Learning Projects (2nd ed.).* Toronto, Ontario Institute for Studies in Education. ISBN 0-8938-4054-8

Wilson, M., Hash, J., (2003). *Building an Information Technology Security Awareness and Training Program*,
Gaithersburg, Maryland: NIST http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf (Accessed 03/07/2010)