Information Security Competence Test with Regards to Password Management

Paul Tarwireyi
Department of Information Systems
Univesity of Fort Hare
East London, South Africa
ptarwireyi@gmail.com

Stephen Flowerday
Department of Information Systems
University of Fort Hare
East London, South Africa
sflowerday@ufh.ac.za

Anass Bayaga
Department of Information Systems
University of Fort Hare
East London, South Africa
abayaga@ufh.ac.za

***Abstract*— It is widely acknowledged that when it comes to IT security the human factor is usually the weakest link. In an effort to strengthen this link, most CIO's are embracing the deployment of security awareness programmes. It is accepted that these programmes can create an information security-aware culture where security risks can be reduced. Even though work has been done in ensuring that these programmes include mechanisms for changing behaviour and reinforcing good security practices, there is a lack of work on measuring the effectiveness of such programmes. Competence based questions have long been used in HR to select employees with the skills that are necessary to perform effectively in a job. Competence based tests focus mainly on the behaviours and traits critical for success on the job and how they have been demonstrated in the past. This current paper presents the description of an approach that uses competency based behavioural questions to measure security competence levels at a university with regards to password management. A sample of 140 students participated in the study. The findings revealed that even though students were aware of the procedures, many failed to implement them. For example, 48.6% of students would share their passwords even though they know it was wrong. It was also found that there is a positive relationship between the year of study and the creation of strong passwords (n=140; r=+0.268; p=0.007).**

Keywords- Information Security Behaviour, Information Security Awareness, Password Management

I. INTRODUCTION

An information system is composed of technology, people and processes. It therefore follows that any effort to secure this system should regard all the system components as equally important and should also identify how these components are intertwined. This means that a holistic approach to security, which integrates technology, people, and processes, needs to be taken. However, in many cases, the solutions being produced are technical in nature. They involve the deployment of trusted technical infrastructure and reliable internal processes [1]. Research has shown that an over-reliance on technology without the integration or consideration of other factors such as the human factor, usually does not yield the desirable results [2] [3] [4] [5] [6] [7].

Accordingly, even the best technical solutions are of little value if insiders do not follow sound security procedures. This means that after the implementation of technical solutions, the human factor needs to be managed – aligning people and practices with security goals. The human factor specifically refers to people who are within the organization [2]. This encompasses company directors, employees and interns [8]. According to the 2010 Data Breach Investigation Report by Verizon [8], insiders are responsible for the larger proportion of data breaches within organisations, such as misuse of information assets. Hackers usually exploit the weakest link in the organization's IT security, the human factor. This is often done by using various social engineering techniques to lure employees into divulging information or to unintentionally give the hacker access to information [5] [9] [10].

This necessitates that organisations develop security awareness programmes that can create an information security-aware culture where the security risks posed by insiders can be reduced. These mechanisms should focus on changing employee behaviour or reinforcing good security practices so that a security-aware culture can develop [11]. ICT security awareness programs are regarded as the key defence in the fight against security incidents that involve humans [1].

Even though work has been done in ensuring that these programmes include mechanisms for changing behaviour and reinforcing good security practices, work on measuring the effectiveness of such programmes is still in its infancy [10].

Therefore, it is difficult to manage something that is not measured. When a doctor is trying to assess whether one has high blood pressure, he/she measures your blood pressure in order to make a decision. Just as technological solutions are measured using metrics such as intrusion attempts, uptime and downtime; security competence levels can also be measured.

The primary objective of this paper is to present the findings of a study that examined password management practices of 140 students at a university. Passwords were chosen as the subject matter because it was felt that they are a good starting point for information security and that all participants understand what passwords are.

The remainder of the paper consists of the following sections. Section 2 provides a theoretical background while the empirical work is described in section 3. Section 4 discusses the way forward and Section 5 concludes the paper with some general comments.

II. THEORETICAL BACKGROUND

Even though there have been advances and several success stories in technical security solutions, the area of end-user security continues to lag behind. It is widely believed that by addressing the end-user security behaviour, information systems security will become more proactive than reactive [10]. With the advances in security technologies, security behaviours such as patch management and antivirus updates are now being automated to reduce the burden on users. However, there are some behaviours such as email and password habits that cannot be automated and are often addressed through the use of security awareness programmes [5] [10] [6] [12].

Security awareness is defined as the knowledge and attitude that employees of an organisation have regarding the protection of information assets of that organisation [5]. Being security-aware implies an understanding of the risks associated with organisational information assets and how to safeguard these assets. Security awareness programmes help to make information security part and parcel of the internal controls that govern operations and processes in an organisation.

Information security is a diverse area with many topics. The importance of each topic varies from one organisation to another depending on the nature of risks faced. For example, phishing is of more concern in financial institutions, while most organisations share concerns over passwords [8]. Authentication is one of the most important mechanisms used to restrict access to information assets [13]. Passwords remain one of the most commonly used authentication methods for IT systems. It was estimated that in 2009, 86% of companies in the USA used password authentication [14]. The literature reviewed provides many examples of good password practices. Changing default passwords, creating strong passwords and not sharing passwords are some of the practices that users have to adopt as part of good password behaviour [13] [14][15] [16] [10].

As stated, this study focuses on the assessment of password management practices of undergraduate students in a university environment (*cf.* introduction). Nowadays, universities operate in a similar manner to other businesses. They rely on ICT facilities for many of their critical tasks such as payroll, HR, registration, examination and fees. Students make use of the university's network and their failure to practise good password behaviour as a habit can compromise the integrity, confidentiality and availability of the university's information [17]. Moreover, universities and other vocational training institutions are amongst the top suppliers of skilled employees to the labour market. It is therefore important to determine if their education equips students with the necessary skills required to enter the workplace and the 'cyber world'.

According to the Conscious Competence Learning Model which describes the stages of learning a new skill or behaviour, learning can be classified into four distinct stages [18]. At the first stage, **unconscious incompetence**, people are not aware of the skills that are required from them whilst at the second stage, **conscious incompetence**, they are aware of the skills they should possess but have not acquired those skills yet. At the third stage, **conscious competence**, even though they have acquired the skills they need to possess, they still need to pay attention when performing these skills. At the final stage, **unconscious competence**, people have perfected performing the skills such that they no longer have to think about how to perform the skills [18].

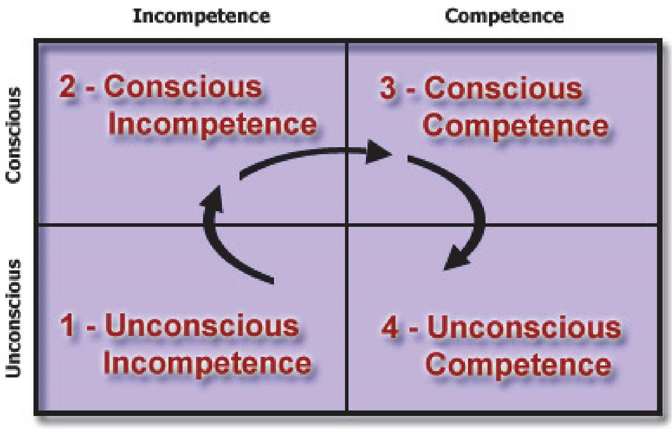

Incompetence
Competence
Conscious
Unconscious
2 - Conscious Incompetence
3 - Conscious Competence
1 - Unconscious Incompetence
4 - Unconscious Competence

Figure 1. Conscious competence learning matrix [19]

NIST presented the IT Security Continuum, a role-based model which defines the IT security learning needed as a person assumes different roles within an organisation [20]. This model is based on the premise that learning is a continuum. The model has three stages and follows a bottom up approach, where its first stage is "Security Awareness". As shown in Figure 2, security awareness is explicitly required for all employees in an organisation whereas the second stage, "Security Basics and Literacy" which provides the foundation for subsequent training, is required for all those employees who are involved in any way with IT systems [20]. Obviously, in today's terms this means all employees within an organisation should be at this level.

These two models present a stratified view of the levels of skills and knowledge; however, they do not give the assessment criteria or metrics which can be used to classify employees into their respective strata based on their level of knowledge or on their behaviour.

Some authors have used different techniques such as knowledge and attitude amongst others to assess Internet Security Awareness and Culture in Organisations [21]. But this study is based on the premise that knowledge, attitude or simply being aware is not enough. It is how one behaves that matters. This view is that since an organisation's success or failure effectively depends on things that its employees do or fail to do, the information security strategy in the organisation should pay close attention to employee behaviour [1].

Behaviour involves making decisions on how to respond to stimuli. Misbehaviour which is usually a result of bad decision making can be discouraged through punishment while good behaviour can be encouraged through reinforcement [22]. Behaviour is a philosophy of psychology which refers to all things that organisms do in response to certain stimuli [22]. Behaviour can be classified into two main categories, overt behaviour and private experiences [23].

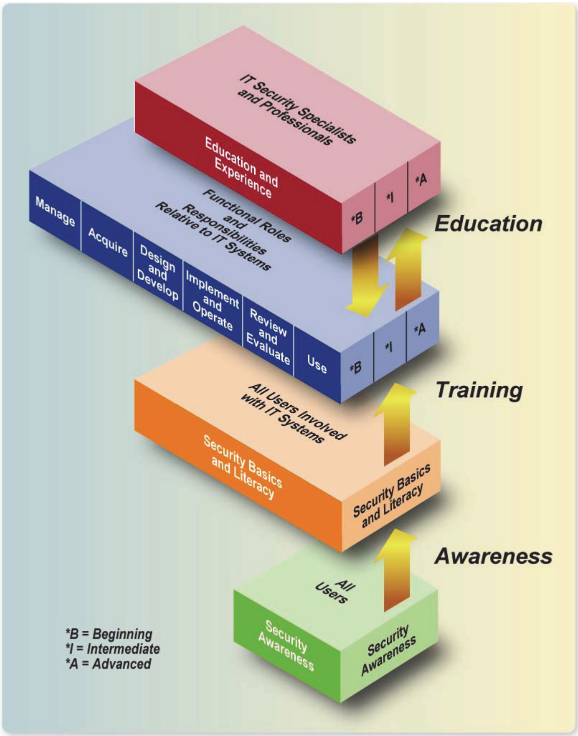


Figure 2. The IT Security Continuum [20]

Overt behaviour can be described as the way people can be observed to demonstrate, while private experiences are things that take place in a person's mind. Thus, behaviour can be represented using the formula:

Behaviour = Overt behaviour + Private experiences

From this deduction, the authors are of the opinion that one can effectively evaluate the security competence of an individual by assessing the way they behave in certain security scenarios. Depicting normal behaviour consistently usually implies having the appropriate knowledge, but having the relevant knowledge does not imply normal behaviour. Normal behaviour in the case of students means that the students are listening and acting on measures to prevent, deter, detect and defend against information security breaches [13].

Whilst awareness and culture are equally important, more emphasis should be put on monitoring behaviour so that effective behaviour modification techniques can be implemented. It is therefore important to develop an approach that comprehensively measures behaviour. In this case; password management behaviour.

To determine the password behaviour a survey of password management practices of students was carried out. The information gathered was used in the assessment and identification of areas of weakness and strength. The approach followed in this assessment provides a way of measuring the information security competence levels. This measurement approach can be used either to benchmark the security competence level before a security awareness programme or to measure the effectiveness of such programmes.

The next section describes the research methodology used and the measurement approach that was developed.

III. COMPENTENCE BASED QUESTIONS: EMPERICAL WORK

This current study ascertains the security competence levels of university students with regards to password management. To achieve this, an anonymous questionnaire using competency based behavioural questions, was administered to first year students - those coming straight from matric and final year students – those who are completing their degree programmes and ready to enter the workplace.

Competence based questions have long been used in HR to select employees with the skills, necessary to perform effectively in the job [24] [25]. These skills are usually referred to as key competencies. Competence is the ability to apply knowledge, skills, abilities and traits to perform tasks in an efficient and effective manner that yields desirable results [25].

Competence based tests focus on the behaviours and traits that are critical for success on the job and how they were demonstrated in the past. This is an effective way to uncover behavioural facets of an individual in a quick and precise manner [26]. It is important to note that behavioural questions do not look for opinion, but rather seek past behaviour. Some of the advantages cited for this approach are [27]:

- It reduces misunderstandings about past experience
- Reduces effort to make a good impression
- Provides actual examples of knowledge, skills and attributes
- Provides direct evidence of the actual state of an individual's competence
- It also promotes consistency in interviews and assures all key areas for success are covered.

For example: competence based questions have also been long used in nursing schools for determining the ability and readiness of health workers to provide quality services [28][29][30][31]. This current study uses competence based questions to determine information security competence.

Participants were asked questions that allowed them to choose options that best describe their behaviour in the following password management areas.

- Sharing passwords with friends
- Storage of passwords
- How often passwords are changed
- Using the same password for multiple accounts
- Choosing the "remember" password option and

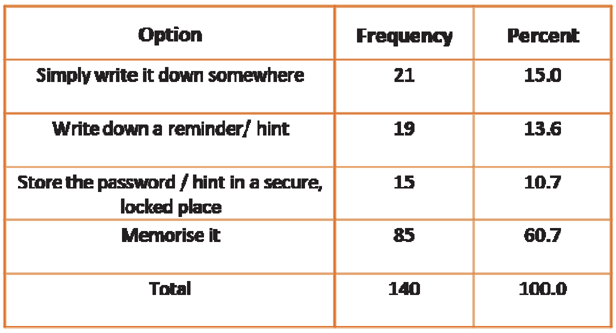
- Using default passwords.

An example of questions that were used to assess students' behaviour on how they kept passwords is given below.

In terms of a new password. How do you store your password if you don't want to forget it?

The options which students were given to choose from and frequencies of their answers are illustrated in table 1.

TABLE 1: HOW PASSWORDS ARE KEPT



Option	Frequency	Percent
Simply write it down somewhere	21	15.0
Write down a reminder/ hint	19	13.6
Store the password / hint in a secure, locked place	15	10.7
Memorise it	85	60.7
Total	140	100.0

Literature was reviewed in order to ensure the survey fully captured and represented the concept under study thus ensuring content validity [13] [14][15]. Furthermore, before the survey was administered, it was sent to a small test group within the target population to ensure that we were asking the right questions and this helped to refine the research instrument.

A. Data Analysis and Interpretation

There were 140 usable responses. 73 responses were from first year students whilst 67 responses came from third year students. These questionnaires were analysed in SPSS (Statistical Package for the Social Sciences) for correlation and other measures. The levels of competence at the different years of study were compared and conclusions were drawn regarding the level of password management competence of each group. Those students who exhibited good behaviour can be regarded as being competent whilst the others are said to have not yet reached the required password management competence level.

B. Research Findings

In this section the main research findings are presented. The research objective in the application of this study's measurement method was to investigate if there was a relationship between the year of study and security competence. In answering this question, it was important to address the following:

- Are third year students generally more competent than first year students?
- Which areas noted the greatest improvement?
- Which area is of greatest concern?

The data analysis revealed that 38.4% (n = 73) of first year students will share their passwords whilst 59.7% (n = 67) of third year students will do the same. Of these figures, 19.2% and 22.4% of first years and third years respectively will share their passwords even though they know there is a risk.

There is a weak negative relationship between the year of study and sharing passwords *(*n=140; *r = -0.295, p=0.021).* It is the authors' view that this is probably a compliance issue; more third years than first years will share their passwords even though they know it is against the security policies (first years are more compliant than their seniors). These results resonate with the findings of another study which was conducted in a mining company where a 60% behaviour level was also noted on sharing passwords [32].

Further evidence suggests that first year students create weaker passwords than third year students. Almost two thirds, (63%) of first year students compared to 41.8% third year students. This probably suggests that the years spent in university have taught them to improve their password strength. Because humans have limited capacity to remember passwords, one tends to create simple and predictable passwords [14].

There is a relatively weak positive relationship between the year of study and the creation of strong passwords *(*n=140; *r=+0.263, p=0.007).*

Additionally, the evidence suggests that 69.9% first year students do not change their default passwords, whilst 40.3% third years also do not change default passwords. This might also suggest that the years spent in university have taught the students to change default passwords.

There is a positive relationship between the year of study and the changing of default passwords *(*n=140; *r=+0.268, p=0.001).*

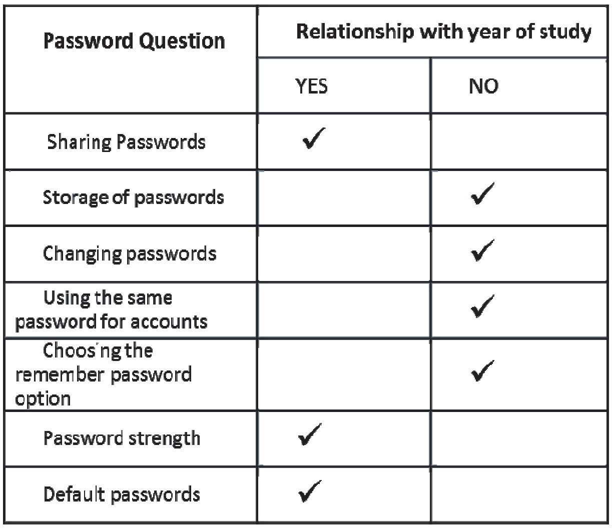
Table 2 below summarises the relationships between the year of study and the different password management competencies. No relationships were noted between the year of study and how often passwords were changed, storage of passwords, using the same passwords and choosing the "remember" password option. This might be an indication that student behaviour in these areas does not change significantly from first year to third year.

Over two thirds of students (71.4%) were generally competent in their password storage practices. However, 15% of the students wrote their passwords down. This is in line with another research which reported that 15-20% of users wrote down their password on a note attached to the computer monitor on a regular basis [14].

Besides the year of study, the field of study was also considered.

For first year students, there was no relationship between field of study and the password management competencies. However, at third year it was noted that students who were studying towards IT related degrees created stronger passwords than students from other degrees *(*n=67; *p=0.038).* Also in general, students doing IT related degrees were found to be more competent than others.

TABLE 2: RELATIONSHIPS BETWEEN YEAR OF STUDY AND PASSWORD COMPETENCIES



Password Question	Relationship with year of study	
	YES	NO
Sharing Passwords	✓	
Storage of passwords		✓
Changing passwords		✓
Using the same password for accounts		✓
Choos'ng the remember password option		✓
Password strength	✓	
Default passwords	✓	

The results also show that doing computers at high school did not make any difference in the password management practices of students.

On the relationship between the different password management competencies, it was found that people who do not change default passwords also do not frequently change their other passwords *(n=140; r=+0.38; p<0.001)*. Furthermore, these areas were also found to be the most problematic areas in terms of password management behaviour with 55.7% and 74.3% students respectively failing to demonstrate good password behaviour. Figure 3 and 4; illustrate how the students behaved in these areas.

Further evidence suggests that about three quarters of the students do not change their passwords often, regardless of the year of study or field of study.

To answer the first sub question, on average, 47.4% first year student responses were on the competent side of the spectrum as compared to 60.8% of third years. This shows an overall 13.4% improvement in competence. From this statistic it is evident that about 39.2% third year students leave university without having achieved the required password management competence levels.

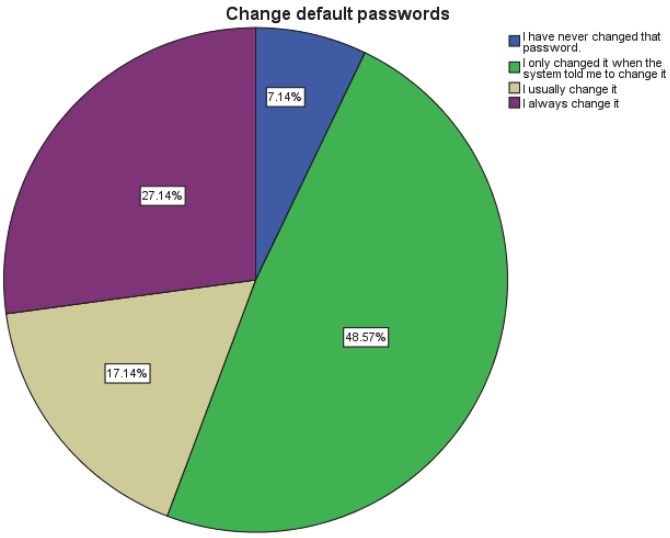


Figure 3: Student behaviour on changing default passwords

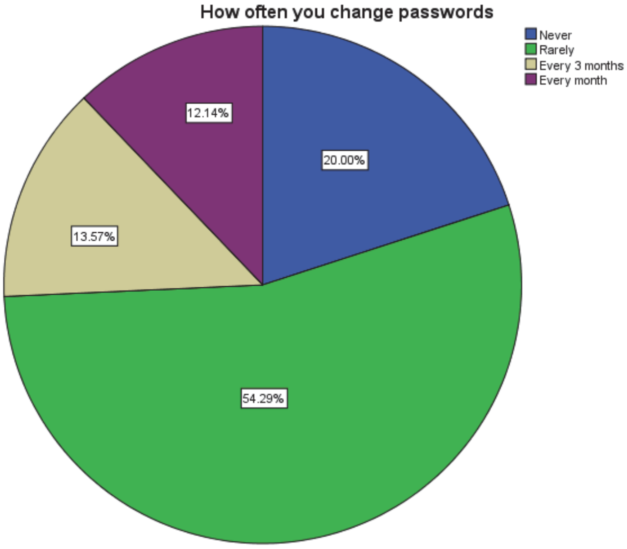


Figure 4: Student behaviour: How often passwords were changed

Improvements in the respective areas of password management are shown in Table 3 that follows.

The greatest improvement, 29.6% was observed in changing default passwords, whilst 15.2% was noted in password strength and 14.4% was noted in choosing the remember password option when logging to systems.

TABLE 3: COMPARISON OF AVERAGE COMPETENCE PERCENTAGE BETWEEN DIFERENT YEARS OF STUDY

Password Competence	Competent percentage	
	1st years	3rd years
Sharing Passwords	61.7	40.3 ↓
Storage of passwords	68.5	74.7 ↑
Changing passwords	30.1	20.9 ↓
Using the same password for different accounts	42.4	53.8 ↑
Choosing the remember password option	61.7	76.1 ↑
Password strength	37	52.2 ↑
Default passwords	30.1	59.7 ↑

Using the same technique, this concept can be applied to assess the effectiveness of a security awareness program, thereby providing a measurement tool.

IV. THE WAY FORWARD

The results are promising because they allow one to draw conclusions between the levels of competence at the different years of study and to identify the relationships between password behaviour and levels of study.

Nonetheless, research is still needed to enhance this measurement approach. The approach should be applied in a different setting to assess the information security competence of different groups. Since passwords are only a part of information security management, it should also be applied to other areas such as social engineering and phishing. Furthermore, future work will also focus on enhancing the data collection strategies. Instead of relying on one question per sub area, it might be important to ask a number of questions so that accurate behaviour in that area can be learnt.

This can also be used as a valuable tool for measuring security competence before and after the implementation of a security awareness program to assess the effectiveness of the program.

The results from this method can also be triangulated with results from other metrics from audit reports such as the number of students who do not change default passwords, and number of people who use weak passwords.

As a way of stratifying these levels of competence, this study employs a coloured scheme scale which has four levels. These scales are based on standard examination grading scales such as:

a) Distinction

b) Credit

c) Pass

d) Fail

These scales can be mapped to the different quadrants of the Conscious Competence Learning Matrix [19] and where appropriate, action needs to be taken to move users from one quadrant to the other.

TABLE 4: COLORED CODED SCHEME SCALE (ADAPTED FROM [32])

Competent: No action required	>=80	🟩
Average: Action maybe required	70 - 79	🟨
Semi -average :Action required	60 - 69	🟧
Poor: Action required	<=59	🟥

Using this scheme, the overall competence of students at third year level is illustrated below. Table 5 shows that students have not reached the required levels of competence; hence, behaviour changing intervention mechanisms are needed.

TABLE 5: GRADED COMPETENCE LEVELS AT THIRD YEAR

Password Competence	Competent percentage	
	3rd years	Colour
Sharing Passwords	40.3	🟥
Storage of passwords	74.7	🟨
Changing passwords	20.9	🟥
Using the same password for different accounts	53.8	🟥
Choosing the remember password option	76.1	🟨
Password strength	52.2	🟥
Default passwords	59.7	🟥

According to this coloured scheme scale, one can conclude that students generally employ poor password management practices and therefore are at the bottom level, “Security Awareness”, of the IT Security Continuum [20]. However, in this information technology era, all employees need to be at the

"Security Basics and Literacy" stage. This also suggests that action needs to be taken if students are going to leave university with the required security competencies.

This means security awareness programmes which emphasis the areas identified as most problematic, need to be implemented. Through regular measurement/feedback, competence in these areas can be improved.

V. Conclusion

Security awareness programmes employ mechanisms that focus on reinforcing good security practices and changing employee security behaviour. However, the implementation of such programmes does not mean that all employees will automatically become security competent. Knowledge, attitude or simply being aware is not enough. It is how one behaves that affects security. It is therefore necessary to have a way of measuring the extent to which good security practices can be reinforced. With a structured measurement approach, it becomes easy to monitor the security practices of users.

This paper describes the development and application of a security competence measurement approach that uses competency based behavioural questions at a South African university. Behavioural questions are an effective way to uncover the behavioural facets of an individual in a quick and precise manner [26]. They do not look for opinion or attitude, but rather examine past behaviour and this provides direct evidence of the actual state of an individual's competence.

The approach was successfully applied to measure the security competence levels of students at different years of study with regards to their password management practices. The findings are encouraging, and it is intended, to apply the approach to other security areas such as phishing and to implement measures that enhance the validity and reliability of the data collected.

References

[1] A. Da Veiga and J. H. P. Eloff, "A framework and assessment instrument for information security culture," *Computers & Security*, vol. 29, no. 2, pp. 196-207, Mar. 2010.

[2] C. Colwill, "Human factors in information security: The insider threat - Who can you trust these days?," *Information Security Technical Report*, vol. 14, no. 4, pp. 186-196, Nov. 2009.

[3] S. Furnell and K.-L. Thomson, "From culture to disobedience: Recognising the varying user acceptance of IT security," *Computer Fraud & Security*, vol. 2009, no. 2, pp. 5-10, Feb. 2009.

[4] H. A. Kruger and W. D. Kearney, "Consensus ranking - An ICT security awareness case study," *Computers & Security*, vol. 27, no. 7-8, pp. 254-259, Dec. 2008.

[5] K.-L. Thomson and R. von Solms, "Towards an Information Security Competence Maturity Model," *Computer Fraud & Security*, vol. 2006, no. 5, pp. 11-15, May. 2006.

[6] K.-L. Thomson, R. von Solms, and L. Louw, "Cultivating an organizational information security culture," *Computer Fraud & Security*, vol. 2006, no. 10, pp. 7-11, Oct. 2006.

[7] D. Ashenden, "Information Security management: A human challenge?," *Information Security Technical Report*, vol. 13, no. 4, pp. 195-201, Nov. 2008.

[8] W. Baker et al., "Data Breach Investigations Report." Verizon, 2010.

[9] H. Kruger, L. Drevin, and T. Steyn, "A framework for evaluating ICT security awareness," 2006.

[10] T. Herath and H. R. Rao, "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness," *Decision Support Systems*, vol. 47, no. 2, pp. 154-165, May. 2009.

[11] SANS 27001, "Informationtechnology – security techniques – information securitymanagement systems – requirements.," *Standards South Africa*, 2006.

[12] E. C. Johnson, "Security awareness: switch to a better programme," *Network Security*, vol. 2006, no. 2, pp. 15-18, Feb. 2006.

[13] B. Grawemeyer and H. Johnson, "Using and managing multiple passwords: A week to a view," *Interacting with Computers*, vol. In Press, Corrected Proof, 2011.

[14] T. V. Laptyeva, S. Flach, and K. Kladko, "The weak password problem: chaos, criticality, and encrypted p-CAPTCHAs," *Cornell University, Cryptography and security*, Mar. 2011.

[15] N. Gunson, D. Marshall, H. Morton, and M. Jack, "User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking," *Computers & Security*, vol. In Press, Corrected Proof, 2011.

[16] D. Nelson and K.-P. L. Vu, "Effectiveness of image-based mnemonic techniques for enhancing the memorability and security of user-generated passwords," *Computers in Human Behavior*, vol. 26, no. 4, pp. 705-715, Jul. 2010.

[17] L. Drevin, H. Kruger, and T. Steyn, "Determinants of password security: some educational aspects," *IFIP TC3 World Conference on Computers in Education*, vol. 9, 2009.

[18] K.-L. Thomson, R. von Solms, and L. Louw, "Cultivating an organizational information security culture," *Computer Fraud & Security*, vol. 2006, no. 10, pp. 7-11, Oct. 2006.

[19] B. Bloom, "Testing & Evaluation." 2003.

[20] M. Wilson, D. E. de Zafra, S. I. Pitcher, J. D. Tressler, and J. B. Ippolito, "Information Technology SecurityTraining Requirements:A Role- and Performance-Based Model." National Institute of Standards and Technology Gaithersburg, MD 20899-0001, 1998.

[21] L. Drevin, H. A. Kruger, and T. Steyn, "Value-focused assessment of ICT security awareness in an academic environment," *Computers & Security*, vol. 26, no. 1, pp. 36-43, Feb. 2007.

[22] P. R. Martin and P. Bateson, *Measuring behaviour: an introductory guide*. Cambridge University Press, 1993.

[23] L. Hauser, "Behaviorism," 2005. [Online]. Available: http://www.iep.utm.edu/behavior/. [Accessed: 07-Dec-2010].

[24] V. Vathanophas and J. Thai-ngam, "Competency Requirements for Effective Job Performance in TheThai Public Sector," *Contemporary Management Research*, vol. 3, no. 1, pp. 45-70, 2007.

[25] T. J. Maurer, K. A. Wrenn, H. R. Pierce, S. A. Tross, and W. C. Collins, "Beliefs about 'improvability'of career-relevant skills: relevance to job/task analysis, competency modelling, and learning orientation," *Journal of Organizational Behavior*, vol. 24, no. 1, p. 107–131, 2003.

[26] R. S. Mansfield, "Building competency models: Approaches for HR professionals" *Human Resource Management*, vol.35,1, p.7–18, 1996.

[27] A. Lado and M. Wilson, "Human resource systems and sustained competitive advantage: A competency-based perspective," *The Academy of Management Review*, vol. 19, no. 4, p. 699–727, 1994.

[28] D. T. Cowan, D. Jenifer Wilson-Barnett, I. J. Norman, and T. Murrells, "Measuring nursing competence: Development of a self-assessment tool for general nurses across Europe," *International Journal of Nursing Studies*, vol. 45, no. 6, pp. 902-913, Jun. 2008.

[29] T. McCready, "Portfolios and the assessment of competence in nursing: A literature review," *International Journal of Nursing Studies*, vol. 44, no. 1, pp. 143-151, Jan. 2007.

[30] L. Weiss Roberts et al., "Assessing medical students' competence in obtaining informed consent," *The American Journal of Surgery*, vol. 178, no. 4, pp. 351-354, Oct. 1999.

[31] A. Nikula, H. Nohynek, P. Puukka, and H. Leino-Kilpi, "Vaccination competence of graduating public health nurse students," *Nurse Education Today*, vol. 31, no. 4, pp. 361-367, May. 2011.

[32] H. Kruger and W. Kearney, "Measuring information security awareness: A West Africagold mining environment case study," *Proceedings of the 2005 ISSA Conference, Johannesburg, South Africa*, 2005.