Behavioural Thresholds in the Context of Information Security

D.P. Snyman and H.A. Kruger

North-West University, Potchefstroom, South Africa
{dirk.snyman;hennie.kruger}@nwu.ac.za

Abstract

This research presents the exploratory application of behavioural threshold theory on group behaviour related to information security. Behavioural threshold analysis is presented as a possible tool for aiding the development of security awareness programs. Generic behavioural threshold analysis is presented and then applied in the domain of information security by collecting data on the behavioural thresholds of individuals in a group setting and how they influence each other when it comes to security behaviour. The results of behavioural threshold analysis are presented in order to illustrate the feasibility of the approach as an aid for the development of security awareness programs.

Keywords

Information Security; Human Behaviour; Behaviour Threshold Analysis; Security Culture; Information Security Awareness Programs

1. Introduction

On the terrain of information security research, one of the prevailing themes is that of the human factor. Humans have even been branded to be the weakest link in the fragile information security chain (Soomro *et al*., 2016; Tsohou *et al*., 2015; Yildirim *et al*., 2011). In fact, in a recent summative study of literature pertaining to information security management, Soomro *et al.* (2016) found the human factor to be one that is recurrently identified and researched and is often classified under themes like “human aspects in information security” (Safa *et al*., 2016), “information security awareness” (Tsohou *et al.* 2015), and “information security culture” (Dhillon *et al.*, 2016). The influence of this factor continues to have a far reaching impact on the security and integrity of computerised systems due to the inherent imperfections that humans exhibit when compared to technical layers of security (Richardson, 2010; 2008; Berger, 2012). People can be easily influenced by circumstances and they may divulge sensitive information (sometimes unwittingly, other times with specific intent) that could have a detrimental effect on the security and integrity of the systems with which they interact (Richardson, 2010). One way to deal with these shortcomings (in terms of information security) is to ensure that security awareness programs are implemented in organisations. The goal of such programs is to educate and instruct the members in an organisation about issues regarding information security and to influence their behaviour, or the reigning information security culture, in a positive manner (Tsohou *et al*., 2015). Information security culture is said to be the system of shared patterns or beliefs, in terms of information security, held by members of an organisation. The security culture of an organisation is governed by a shared system of beliefs, influenced by the members of the organisation (Dhillon *et al.*, 2016).

Having security awareness programs that function effectively is crucial in managing the information security culture of any organisation. Developing and employing these programs take time and effort which make them costly. Security awareness programs should therefore be tailored to fit the group to ensure that the programs succeed in their goal. The approach highlighted by Tsohou *et al.* (2015) would be to analyse the behaviour in the organisation through the lens of different behavioural models to determine the reason why the individual, and later the group, behaves in a certain way. The reasons for the way in which behaviour within an organisation is formed are not always overt, but according to Tsohou *et al.* (2015), behaviour of the individual and the group may be influenced by cognitive and cultural biases. These biases affect the way in which they (the organisation as individuals and as a group) adopt information security regulation and policies. By keeping these factors in mind, security awareness programs may be optimised.

Granovetter (1978) presents a behavioural model based on the premise that group behaviour is determined by the influence that individuals have on one another. Specifically how an individual reacts to the actions (or absence of actions) of others (see Section 2.2). This reaction is said to be based on an intrinsic threshold that an individual has to participate, given the number of others that already participate. This behavioural model may prove useful to assess security culture and determine how the individual and the group is influenced by peer behaviour (Herath and Rao, 2009). E.g. if high personal thresholds for an information security related topic (like password security) is noted, it would suggest that users are unlikely to be influenced by the behaviour of others. This would indicate that little focus on password security is warranted in a security awareness program. Conversely, if a low personal threshold is noted, users should be more likely to be influenced by the behaviour of others. Security awareness programs should therefore have its focus on the relevant topics in order to influence security behaviour in a positive way. This should contribute to the economics of security awareness by only including suitable topics in security awareness programs in order to limit the high cost (in terms of time and money) usually associated with the development of such programs. Furthermore, the modern user gets overloaded with security information and has become security fatigued (Furnell and Thompson, 2009) and by tailoring the content of security awareness programs security fatigue may be prevented in order to promote the effectiveness of security awareness programs.

With this in mind, this paper aims to perform an exploratory investigation into the feasibility of behavioural threshold analysis as a possible aid in developing the right (especially content-wise) security awareness programs for a given group or organisation. In order to achieve the abovementioned aim this paper is structured as follows: Section 2 describes literature from related work pertaining to security awareness programs, behavioural thresholds and instruments that can be used to analyse these thresholds. Section 3 demonstrates a typical behaviour threshold analysis. Section 4 presents an illustrative example of threshold analysis with specific focus on its application in Information Security. Finally, Section 5 summarises the findings of this study and looks towards future directions for this research.

2. Literature review

This section shows cursory examples of the related literature, highlighting issues in security awareness programs, behavioural thresholds, and behavioural threshold analysis techniques.

2.1. Security awareness programs

Security awareness programs play an important part in managing the Information Security culture of an organisation (Tsohou *et al*., 2015). They convey information about the security policies and possible security threats within an organisation. They serve as a mechanism to educate users and create awareness about relevant security issues that face the organisation. It is usually assumed that the users within an organisation are prone to risky behaviour in terms of security because they are unaware that their behaviour is risky, and even when informed to the contrary they are unaware of the potential consequences of their actions. Tsohou *et al*. (2015) further state that even though there are guidelines and standards that govern the development of security awareness programs, they often fail because they fail to provide for the way in which users form ideas and opinions on a cognitive level. By not taking this into account these programs merely bombard the user with information that does not influence the security behaviour of users as it is supposed to do. This cursory overview is due to space limitations. For further reading on security awareness programs, including comprehensive literature surveys, see Safa and Von Solms (2016), Soomro *et al*. (2016), and Lebek *et al*. (2013).

2.2. Behavioural thresholds

Granovetter (1978) (and later Granovetter and Soong (1983)) argues that the preferences, norms or beliefs of an individual are seldom formed without the influence of the environment (especially the interaction with others) in which the individual finds himself. He further argues that these norms can change due to the influence of the behaviour of a group of people, even to such an extent that the behaviour of the individual can change to the exact opposite of said individual’s prevailing norms. This phenomenon can occur even without direct confrontation of the individual by any member(s) of the group. This trigger of paradoxical behaviour may be attributed to be due to humans having an inherent threshold for the acceptance of, and participation in behaviour in a group setting. For instance when protesters gather to further a specific cause, emotions and convictions can cause the situation to be volatile. When a core individual or group starts acting violently the situation can easily escalate to a full blown riot. Suddenly all of the (once peaceful) protesters participate in acts of vandalism and the like. E.g. Person A is a peaceful protester and believes in peaceful resolution of differences, however he is willing to commit to violence if at least a certain critical mass of others in the protest commits to violence. This phenomenon can be translated to an organisational setting where, for example, management want to implement a new information security policy and want to generate acceptance for the policy among the members of the organisation. They need only influence a critical mass of members and the others will follow in acceptance. Contrariwise when a certain critical mass of members deviate from the prescriptive policies, there could be a detrimental effect in the overall compliance as the remaining members will once again follow in example, but in a manner that is contraindicated.

A proposed model by Granovetter (1978) aims to analyse the inherent thresholds of the individuals that make up a group and predict the outcome of situations where a critical mass influences the remainder of individuals. This model is referred to as "Behavioural threshold analysis" and is based on circumstances where the actors (members of a group) only have two discrete and opposing avenues of pursuit. Usually choosing the behaviour in one direction has a supposed positive result and the other has a negative result. The analogy (as explained in above) of either participating in a riot or not participating, is used to emphasise these two opposing views but Granovetter (1978) argues that the model is applicable to any contrasting binary decision. See Granovetter, (1978) and Growney (1983) for further analogical situations.

The inherent personal cost vs. gain of committing to either of these choices is what determines the individual's threshold pertaining to participation or abstention. The perceived cost of participation differs for each individual that a group consists of. Some individuals require little to no motivation to participate in an activity and can be seen as instigators, while others need to be swayed to join in uncharacteristic activity due to the perceived gain outweighing the cost. Some perceive the cost as being infinitely high and will never join in.

The aim of this model is to describe the outcome of a situation given the collection and distribution of individuals (each with their own threshold) that are involved therein by predicting the number of individuals opting for each of the opposing behaviours. As mentioned in the Introduction (see Section 1), this model may be implemented as an aid in determining the content of security awareness programs by analysing the susceptibility of users to influence by others in terms of information security issues. Using this model as a barometer, only relevant information may be included in security awareness programs, possibly saving time and money. The following section describes the typical analysis of recorded thresholds based on the analysis as presented by Growney (1983).

3. Typical threshold analysis

Growney (1983) posits that in order to obtain the individual threshold values from a group a simple standard questionnaire can be employed. The individuals in a group are requested to truthfully respond to a set of questions about two discrete outcomes (see Section 2.2) of a situation in which the individuals as part of a group may find themselves. The individuals (respondents) are asked to complete a value for *x* in 2(b) of Figure 1. The value quoted represents the inherent threshold for the individual in question.

Questionnaire

1. Choose one of the following outcomes that is preferable:
   a. Outcome A
   b. Outcome B
2. Regardless of the outcome selected above, respond to the following statements:
   a. I will never participate in Action A
   b. I will participate in Action A when at least *x* number/percent of group members choose to participate in Action A.

Figure 1: Threshold questionnaire (Growney, 1983)

After the responses are received from the respondents the responses can be tabulated and represented in a graph format. Threshold analysis (see Section 2.2) can then be performed on the observed values in order to predict the outcome of the behaviour of the group under observation. Observe the following set of cumulative thresholds (Table 1). These thresholds were obtained for an imaginary group of people in an imaginary setting as if they had completed a questionnaire like the one in Figure 1. Let the two mutually exclusive outcomes as mentioned earlier be Outcome A (negative) and Outcome B (positive). The thresholds tabulated in Table 1 represent an individual's threshold to participate in an action (Action A) that will lead to Outcome A. In other words: how many individuals have to perform Action A before the individual, whose threshold is being noted, will join in and also perform Action A. E.g. note the number of individuals with a given threshold of 20. These 15 individuals will be inclined to perform Action A when 20 or more people already participate. The cumulative frequencies (column 3) indicate that there are 30 people in total with the threshold of 20 or less which means that the 15 people with the threshold of 20 will join in Action A. The participating group will continue to grow as long as the thresholds in column 1 are exceeded by the cumulative frequencies in column 3. The complete behavioural threshold analysis is based on the comparison of all the individual behaviour thresholds - noted across the group in question - to a uniform distribution of thresholds said to be the equilibrium. A graphic representation of Table 1 is presented in Figure 2. Note: To simplify the analysis all values have been expressed as percentages and thresholds adjusted to intervals of 10 (Granovetter, 1978; Growney, 1983).

Thresholds	Number of individuals with given threshold	Cumulative frequencies of individuals with a threshold <= given threshold
0	0	0
10	15	15
20	15	30
30	10	40
40	30	50
50	10	80
60	0	90
70	0	90
80	0	90
90	0	90
100	0	90
No Threshold:	10	

Table 1: Threshold analysis (Growney, 1983)

With reference to Figure 2, when observing the threshold line segments to either the left or right of an intersection with the equilibrium line the gradients of these line segments describe the stability of the group's behaviour against deterioration (heading towards Outcome B) or escalation (heading towards Outcome A). When the line segment to the *left* of an equilibrium intersection has a gradient of less than one the equilibrium that has been reached is said to be stable against decrease (towards B) and a segment with a gradient of less than one to the *right*, stable against increase (towards A). If both conditions of line segment with gradients less than one is met, the equilibrium is said to be stable and the group will remain in its current state, otherwise there will be a movement towards one of the extreme outcomes (A vs. B). Upon inspection of the resulting graph (Figure 2) an upward trend with a positive gradient is identified up to the (60, 90) co-ordinates. Thereafter a gradient of 0 (horizontal line segments) is noted for the remainder of the graph. When an equilibrium is reached at the intersection (90, 90) the conditions for a stable equilibrium is reached and no further deterioration or escalation is possible. The following section will present an illustrative example to show how the principles of behavioural threshold analysis (as explained in Section 3) are applied in the context of information security.

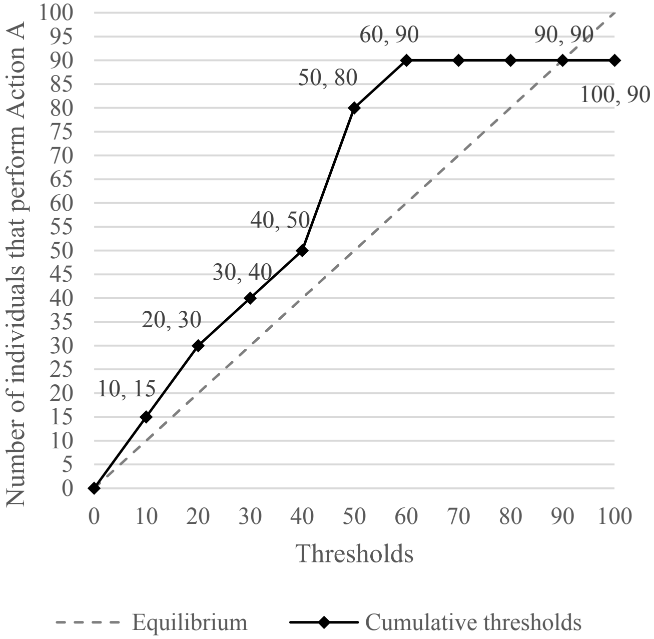


Figure 2: Threshold analysis example (Growney, 1983)

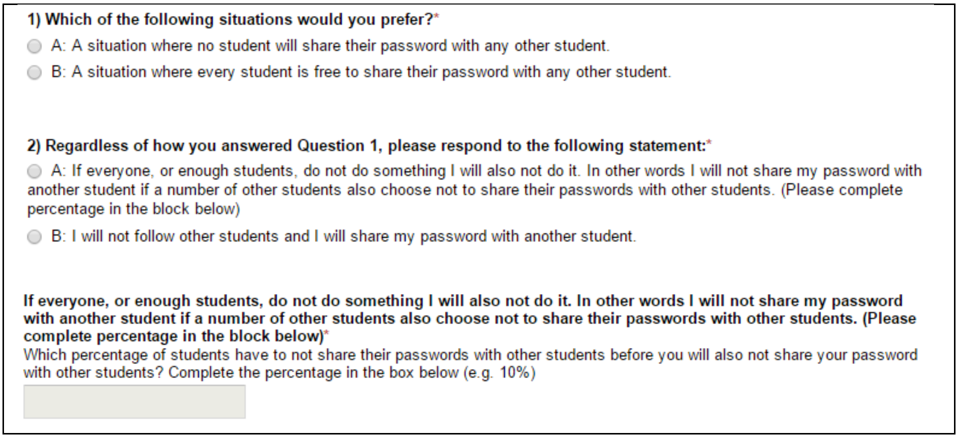
4. Illustrative example of threshold analysis in the context of Information Security

In order to meet the aim of this study (see Section 1) a threshold analysis is to be performed in terms of information security in order to gauge the effectiveness thereof as a tool for the development of security awareness programs. The example mentioned in this section is still in an exploratory phase. It was the very first experiment to test the behavioural threshold analysis concepts in the context of information security. The experiment was carried out with students as a test group and the initial results, which are used here only as an illustration, will be used to improve the security questions that are asked as well as refine the experimental process as a whole.

4.1. Data collection

The questionnaire that is used for data collection for this research was based on the questionnaire that is presented in Section 3. The questionnaire was supplemented with questions to determine basic demographic information such as gender, age etc. This questionnaire was distributed under a group of first year engineering students at a South African university. The questionnaire was hosted on Google Forms to facilitate the distribution of the questionnaire to the students and capture their responses. Out of a possible 70 students, 22 had responded resulting in a response rate of 31.4%. Of these 22 students 13 identified themselves as Male and 9 as

Female. An example of the questionnaire is presented below in Figure 3. The section of the questionnaire that contains questions about demographic information in not shown due to space considerations. Because of the exploratory nature of this research, it was opted to use a simple information security aspect for behavioural threshold analysis. Passwords were used as the basis for the questions as all students need to use passwords on a daily basis and should be familiar enough for them to relate to. Students were asked whether they would share their passwords if enough other students opt to do so and if so, how many students need to share their passwords before they also share their passwords.



1) Which of the following situations would you prefer?*

○ A: A situation where no student will share their password with any other student.

○ B: A situation where every student is free to share their password with any other student.

2) Regardless of how you answered Question 1, please respond to the following statement:*

○ A: If everyone, or enough students, do not do something I will also not do it. In other words I will not share my password with another student if a number of other students also choose not to share their passwords with other students. (Please complete percentage in the block below)

○ B: I will not follow other students and I will share my password with another student.

If everyone, or enough students, do not do something I will also not do it. In other words I will not share my password with another student if a number of other students also choose not to share their passwords with other students. (Please complete percentage in the block below)*

Which percentage of students have to not share their passwords with other students before you will also not share your password with other students? Complete the percentage in the box below (e.g. 10%)

Figure 3: Behavioural threshold questionnaire

Initial pilot runs of this questionnaire proved troublesome with students being unsure of how to answer the questions relating to their password sharing behaviour, specifically question 2(A) as it was not clear to respondents that they needed to nominate a threshold value (as described in Section 2.2) resulting in a majority of unusable responses. This prompted a redesign of the presentation of the questions about their security behaviour. It is noted that the manner in which the questions are structured in this questionnaire (Figure 3) may seem reversed when compared to the example in Section 3 and that seen in literature. This is due to Growney (1983) proposing that issues with responses on the questionnaire, where the question was not understood by the respondents, may be solved by reversing the order in which the different outcomes are presented. This lead to interpretable results that can be displayed in an analogical manner of the way in which behaviour threshold analysis may be implemented in an information security behaviour setting. The questions on information security behaviour, specifically on passwords, still need to be re-evaluated and refined to ensure operability in a real-world analytical setting. The following section presents the results of the group behaviour threshold analysis for the above mentioned questionnaire.

4.2. Results

Figure 4 shows the results of the responses received from the questionnaire from Section 4.1. The resulting graph shows a positive gradient of up to the (10, 9.09) coordinates where the graph intersects the equilibrium line. The line segment to the left of the intersection with the equilibrium line has a gradient of 0.454 (less than one), which indicates stability against decrease. The line segment to the right of the intersection with the equilibrium line has a gradient of 0 (less than one) which in turn indicates stability against increase. An equilibrium is reached at the intersection and the conditions for a stable equilibrium is met and no further deterioration or escalation is possible.

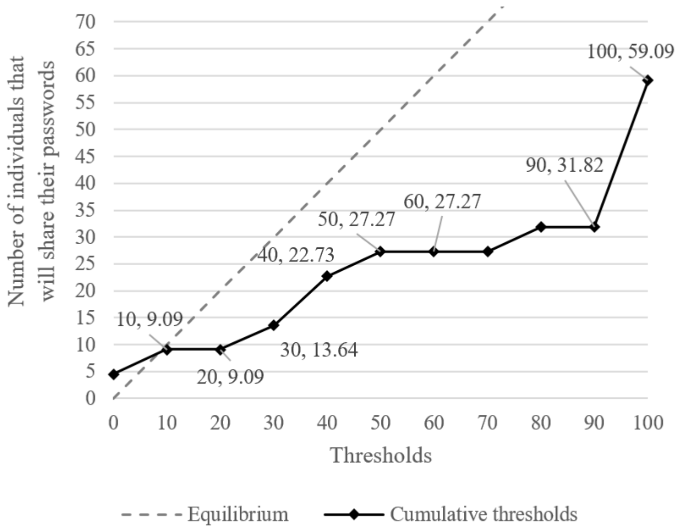


Figure 4: Results for threshold analysis

When this is interpreted in terms of information security and the questions posed in the questionnaire (whether students will share their passwords when other students also do it), there will be an increase in participation to the point where almost 10% of the students are influenced to join in and share their passwords with others. This number should remain stable as there is not enough momentum for this trend to catch on to the other students. This is due to the equilibrium being reached at a point where there are no more growth opportunities where the self-reported thresholds of the students are exceeded and students will not be influenced to join in. The stability in password sharing behaviour that is noted from the analysis may now be used to determine whether “passwords and password confidentiality” is a suitable subject to include in security awareness programs for this specific group. Depending on other considerations in information security that an organisation might have and need to address, they might decide that 10% of users sharing their passwords is a problem that needs addressing immediately (rather than any other current security matters) and opt to include password education in security awareness programs. Inversely, they may decide that other matters are more pressings than the sharing of passwords and because of the stability (i.e. the problem is not a growing one) they may opt to leave password education out of a security awareness program for possible inclusion a later date.

This initial analysis of security behaviour by using behavioural threshold analysis is still in its infancy, but shows promise as a tool for measurement, analysis and prediction of security behaviour and awareness. However there are still problems which would need to be addressed. The measurement instrument (questionnaire) still needs refinement in order to ensure the results obtained is representative of the security behaviour in the group. Respondents may be influenced by social desirability (Fisher, 1993) i.e. they identify one of the two responses as being the “correct” or “expected” one to choose rather than reporting on their true behaviour. The choice of what is to be measured should be investigated as passwords (which were chosen as the basis for the behavioural threshold questionnaire) may already be one aspect of information security that the respondents are too familiar with and may be security fatigued due to overexposure to awareness campaigns which taints their answers to the questionnaire.

5. Conclusion

This paper presents an original inquiry into the application of behavioural thresholds and group dynamics in analysing the human factor of information security. The initial experimental results show that behavioural threshold analysis is feasible in the context of information security and may provide useful guidelines on how to construct information security awareness programs. The threshold analysis method may contribute to security awareness in the following ways: 1) By helping to determine which security issues are easily susceptible to peer pressure or easily influenced by peer behaviour. If such topics can be identified it means that these are the topics that should be concentrated on in security awareness campaigns. 2) By identifying the key issues on which to concentrate in security awareness programs, the threshold analysis method may serve as a countermeasure against security fatigue. 3) Provide a positive contribution to the economics of security awareness, by helping to save time and money. 4) The threshold analysis method can be used later on, after interventions by means of security awareness campaigns, in a follow-up to track progress of security awareness levels. E.g. if 90% of users said they will follow others in doing something that is against Information Security policies, but in the follow-up only 10% say they will follow other and also do something against information security policies, an improvement can be noted. This improvement may indicate success in the security awareness programs. 5) Finally, the threshold analysis method gives a new way to measure the importance of security awareness issues in an organization.

6. References

Berger, U. (2012). CSI/FBI Computer Crime and Security Survey 2011-2012. CSI Computer Security Institute.

Dhillon, G., Syed, R., and Pedron, C. (2016). Interpreting Information Security culture: An organizational transformation case study. Computers and Security, 56, 63-69.

Fisher, R. J. (1993). Social desirability bias and the validity of indirect questioning. Journal of consumer research, 303-315.

Furnell, S., and Thomson, K. L. (2009). Recognising and addressing ‘security fatigue’. Computer Fraud and Security, 2009(11), 7-11.

Granovetter, M. "Threshold models of collective behavior." American journal of sociology (1978): 1420-1443.

Granovetter, M., and Soong, R. (1983). Threshold models of diffusion and collective behaviour. Journal of Mathematical Sociology, 9(3), 165.

Growney, J. (1983). I will if you will: Individual thresholds and group behaviour. Applications of algebra to group behavior. Lexington, MA: COMAP, Inc. 108-137.

Herath, T., and Rao, H. R. (2009). Encouraging Information Security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47(2), 154-165.

Lebek, B., Uffen, J., Breitner, M. H., Neumann, M., and Hohler, B. (2013). Employees' information security awareness and behavior: A literature review. In 46th Hawaii International Conference on System Sciences (HICSS), 2978-2987.

Richardson, R. (2008). CSI computer crime and security survey. Computer Security Institute, 1, 1-30.

Richardson, R. (2011). 15th annual 2010/2011 computer crime and security survey. Computer Security Institute, 1-44.

Safa, N. S., and Von Solms, R. (2016). An information security knowledge sharing model in organizations. Computers in Human Behavior, 57, 442-451.

Safa, N. S., Von Solms, R., and Furnell, S. (2016). Information security policy compliance model in organizations. Computers and security, 56, 70-82.

Soomro, Z. A., Shah, M. H., and Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. International Journal of Information Management, 36(2), 215-225.

Tsohou, A., Karyda, M., and Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of Information Security policies: Recommendations for Information Security awareness programs. Computers and Security, 52, 128-141.

Yildirim, E. Y., Akalp, G., Aytac, S., and Bayram, N. (2011). Factors influencing Information Security management in small-and medium-sized enterprises: A case study from Turkey. International Journal of Information Management, 31(4), 360-365.