Combating Information Security Apathy by Encouraging Prosocial Organisational Behaviour

K. Thomson[1] and J. van Niekerk[2]

Center for Information Security Studies
Nelson Mandela Metropolitan University, South Africa
e-mail: {kerry-lynn.thomson|johan.vanniekerk}@nmmu.ac.za

Abstract

The protection of organisational information assets is a *human* problem. It is widely acknowledged that an organisation's employees are the weakest link in the protection of the organisation's information assets. Most current approaches towards addressing this human problem focus on awareness and educational activities and do not necessarily view the problem from a holistic viewpoint. Combating employee apathy and motivating employees to see information security as *their* problem is often not adequately addressed by "isolated" awareness activities. This paper examines the motivation of employees to actively contribute towards information security from an organisational science perspective through *prosocial* organisational behaviour.

Keywords

Information security, prosocial organisational behaviour, goal-setting theory, information security corporate culture

1. Introduction

It is commonly acknowledged that employees are often the weakest link when it comes to protecting information assets. Very often this is due to the apathetic behaviour of employees which leads to a diffusion of responsibility on the part of employees. In other words, each employee believes that information security is not *their* responsibility (Kabay, 2002).

It is, therefore, important that a corporate culture of information security be cultivated to ensure that employees' behaviour reflects the information security goals of management, and that miscommunication of goals is avoided. Miscommunication is a common factor in everyday life and becomes even more complex in organisations. Miscommunication could occur between employees, but more importantly, between management and its employees. Even though establishing a corporate culture will not eliminate miscommunication completely, it does reduce the possibility that the members of an organisation will misunderstand one another. Corporate culture enables this in two ways. Firstly, there is no need to communicate things about which shared beliefs and values exist. Secondly, shared beliefs and

values assist employees in interpreting the messages from management in the same way (Sathe, 1983).

This paper will investigate *Goal-setting Theory* and how this theory could be used to encourage *prosocial* organisational behaviour. In terms of information security, *prosocial* organisational behaviour is demonstrated through employees voluntarily protecting information assets. In order to encourage *prosocial* organisational behaviour the goals of an organisation must be outlined and the commitment to these goals must be fostered. Ultimately, if all employees exhibit *prosocial* behaviour and are all working towards the same information security goals, then an information security corporate culture will begin to emerge.

2. Organisational Environments

There are generally three key organisational environments that could exist. These environments dictate how the organisation is run and how employees react in certain circumstances. These environments are Coercive, Utilitarian and Goal Consensus (Schein, 1992).

The Coercive Environment is one where employees feel frustrated or dissatisfied and seek to leave the environment if possible. Peer relationships in this environment are typically established in defence of management. A Coercive Environment usually undermines employees' autonomy, which reduces their intrinsic motivation, making employees less likely to respond to management. Employees in this environment perform tasks because they are obliged to do so, typically because of consequences, rather than because they agree with the actions, decisions or goals of management (Schein, 1992; Layton, 2005).

The Utilitarian Environment is one where employees participate in their organisation by evolving workgroups based on an incentive system. In this environment, employees will do as management wishes because of the rewards that they will receive. These rewards may increase the possibility of desired behaviour, but only while the rewards are still given. Therefore, the employees in a Utilitarian Environment might still not necessarily agree with management's goals, but will work towards them when, and only if, rewarded for desired behaviour (Schein, 1992; Layton, 2005).

In both these environments, management may force employees to comply with its policies and procedures through rewarding correct behaviour or disciplining incorrect behaviours. While this approach may succeed in trying to change or shape a corporate culture, management cannot anticipate all the contingencies that could arise in its organisation.

When an unexpected contingency arises, management should rely on the cooperation of the employee to adhere to what is best for the organisation. The degree of true cooperation on the part of employees is influenced by shared beliefs and values, or, in other words, the corporate culture. Therefore, ideally, an information security

corporate culture should be cultivated to ensure that management and employees are working towards common information security goals (Sathe, 1983). The third organisational environment, the Goal Consensus Environment, could lead to a corporate culture which is in line with the information security vision of management.

In the Goal Consensus Environment, employees are morally involved with the organisation. They identify with the organisation, share the same beliefs and values of management, and they are striving towards the vision and goals of management. In this environment, employees' actions are not as a result of being forced to do so or because of a reward, but because they are in agreement with the way things are done in the organisation (Schein, 1992). To ensure that the organisation is adaptable and can respond to change, it is imperative that all levels of employees and management be involved in the initiation and implementation of change by working towards the same goals (Griffin et al, 2004). This would mean that 'right' decisions and actions of employees become second-nature and part of their culture (Schein, 1999).

From an information security perspective, the Goal Consensus Environment is the desired environment for an organisation. In many organisations, the information security vision or goals of management and that of the employees is immensely disparate, resulting in management and employees actually working in 'opposing directions', as indicated in Figure 1. The consequence of this is that minimal achievement of organisational goals is evident in an organisation and information security is, therefore, not successfully integrated into the organisational corporate culture.

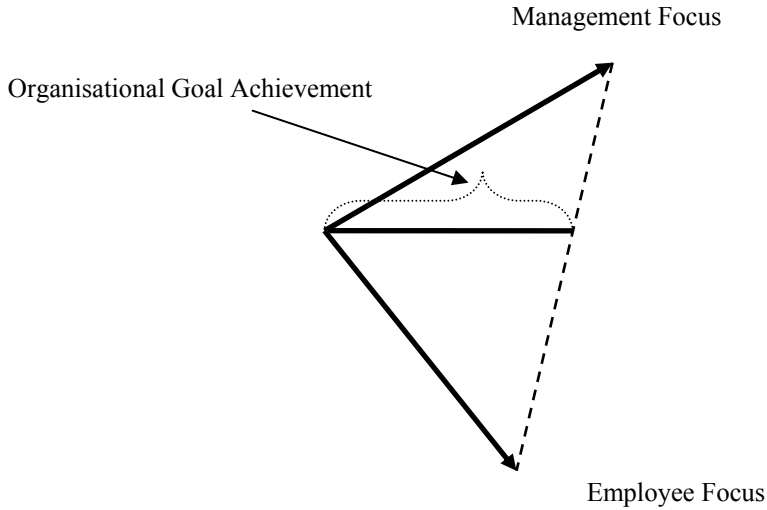

Figure 1: Minimal organisational goal achievement
(Source: Accel-Team, 2000)

The challenge in most organisations is to ensure that the information security vision or goals of management are essentially supported by the employees, primarily through their exhibited behaviour and reactions to certain situations. This should result in management and employees working towards the same organisational goals. The closer the focus of management and employees are aligned, the greater the chance of the achievement of the organisational goals, as indicated in Figure 2.

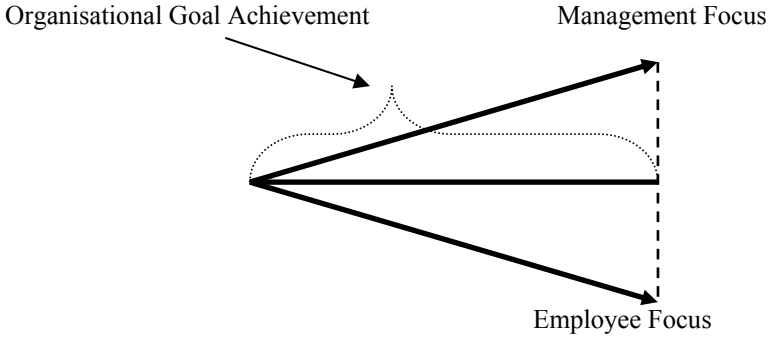

Figure 2: Increased organisational goal achievement (Source: Accel-Team, 2000)

Therefore, in order to achieve the information security goals of an organisation, it would be beneficial to encourage a Goal Consensus Environment, where management and employees are all working towards the same goals. Over time, this could evolve into an information security corporate culture, where management and employees are committed to and working towards the same goals. However, a common hindrance to the creation of an environment where management and employees are working towards the same information security goals is the apathy of employees.

3. Information Security *Schema*

As mentioned earlier, it is widely acknowledged that employees are the weakest link in information security and are often apathetic to their role in information security. In many cases, the problems encountered with employee actions and behaviour reflects the social nature of human beings. In daily activities, people base their judgments on a picture of reality that each individual constructs. This picture, according to psychologists, is referred to as a person's *schema*. This *schema* assists a person by defining what is appropriate and what is inappropriate in a given situation (Mitnick & Simon, 2002; Kabay, 2002).

Schemata influence what a person perceives. In other words, faced with the same situation, different people could interpret the situation in different ways, depending on their *schema*. *Schemata* also influence what a person remembers. If an employee

is faced with information that is not consistent with their *schema*, together with information that fits their *schema* then, typically, the inconsistent information is discarded. As *schemata* influence what people perceive and remember, it is vital that a consistent view of information security is introduced to employees before culture change is attempted through the implementation of policies and procedures.

An employee may have a certain *schema* of his or her organisation and environment. In most cases, the introduction of information security policies and procedures will challenge or even conflict with an employee's *schema*. This could lead to employee anxiety as employees prefer stability in their environment and the traditions that are inherent in this environment are difficult to change. These information security policies and procedures will, most likely, require a change in the employee's environment. Further, any prospective change in an environment in which employees are comfortable could lead to massive amounts of anxiety and resistance to change (Drennan, 1992; Schein, 1999, Kabay, 2002).

It is important that information security becomes part of an employee's *schema* and it not an obligation, with associated consequences, as would be required in a Coercive Environment, or associated with rewards, as in the Utilitarian Environment. However, as mentioned previously, neither employees in a Utilitarian Environment nor those in a Coercive Environment necessarily agree with management and, therefore, are only working towards common goals because of rewards and/or consequences.

Furthermore, enforcing correct information security behaviour through rewards and consequences is not ideal because, without strict enforcement, employees may stray from the correct information security practices if an 'out of the ordinary' situation presents itself. Ideally, the information security *schema* of each employee should change to incorporate the information security goals as defined by management in information security policies and procedures. Once each employee's information security *schema* is in line with the goals of management, a Goal Consensus Environment will have been cultivated. In addition, it would be expected that in such a Goal Consensus Environment, behaviour that is beneficial to the overall information security goals of the organisation would be considered to be *prosocial*, and such *prosocial* behaviour would thus be evident in the environment.

4. *Prosocial* Organisational Behaviour

In social psychology terms, a person exhibiting *prosocial* behaviour is one who comes to the aid of others. For example, in an emergency or threatening situation, a *prosocial* person would react and assist – someone who is not *prosocial* would not be inclined to help. In order for a person to react in a *prosocial* way, the person first has to notice an emergency or threat. The person then needs to define the situation as an emergency or threat and comprehend that action should be taken. Through *prosocial* behaviour, it is expected that a person reacts voluntarily to a situation, without the expectation of receiving a reward for their action (Kabay, 2002; Brief & Motowidlo, 1986).

Within an organisational context, *prosocial* organisational behaviour is performed by an employee of an organisation and the behaviour is conducted with the purpose of promoting or protecting an organisation. Employees who are *prosocial* are not apathetic to organisational requirements. Further, *prosocial* behaviour is influenced by the environment is which a person works. A person who is in a 'bad mood' as a result of their working environment is less likely to act *prosocially*, while 'good moods' positively influence *prosocial* behaviour.

Another factor which influences *prosocial* behaviour is leadership style. Management who is seen to be considerate to its employees could be seen as *prosocial* role models. This increases the likelihood that employees will react *prosocially* to the organisation. Therefore, a Coercive or Utilitarian Environment, where employees are not committed to the goals of an organisation could result in employees being dissatisfied in their environment. In addition, an environment where employees are highly stressed and pressurized will reduce the probability of *prosocial* behaviour (Messer & White, 2006; Kabay, 2002; Brief & Motowidlo, 1986).

One of the thirteen identified *prosocial* organisational behaviours is compliance with the policies and goals of an organisation. This compliance includes demonstrating behaviour that adheres to organisational policies and procedures. This behaviour shows an acceptance of the organisational values and goals (Brief & Motowidlo, 1986).

Ideally, employees in an organisation should exhibit *prosocial* behaviour when it comes to the protection of information assets. Any situation that is identified as an emergency or threat to information assets should trigger a *prosocial* reaction from employees. *Prosocial* information security behaviour should result in employees reacting willingly and spontaneously in the protection of information assets.

As mentioned previously, however, for an employee to react *prosocially* it is necessary for the employee to identify an emergency or threat. In the context of information security, this means that security threats to information assets must be easily identifiable by employees for them to react. Therefore, it is vital that there exist clearly written information security policies and procedures. Further, the contents of these policies and procedures should be communicated to employees, as well as how to identify security threats, through comprehensive information security awareness and training programs.

With regard to learning in an organisation, through information security awareness and training programs, management's attitude and contribution towards learning greatly influences the success of these programs. In some organisations, specific strategies are adopted to promote and facilitate learning (Brief & Motowidlo, 1986; Srivastava & Frankwick, 2011). An in-depth discussion on information security awareness and training programs, though, is beyond the scope of this paper.

However, such strategies would ensure that employees could identify a threat to information security assets – but how can it be ensured that employees will react to these situations? How could management encourage employees to incorporate information security relevant behaviour into a *prosocial* context? One possible approach would be through the application of Goal-setting Theory.

5. Goal-setting Theory

Goal-setting Theory proposes that working towards a goal is a key motivation tool in an organisation. Goals specify to employees what needs to be done. In addition, more identifying and setting specific goals leads to better performance compared with a vague goal of, for example, 'just try your best'. Further, goals that are seem as difficult or more challenging result in better performance than easily obtained goals. Also vital in Goal-setting Theory is the role of feedback. Feedback identifies discrepancies between what has been done and what still needs to be accomplished. Therefore, feedback can be used to guide behaviour. It has also been shown that self-generated feedback, where an employee can monitor their own progress, is a better motivator than receiving external feedback. Further, Goal-setting Theory states that for goals to be achieved there must be a commitment to those goals (Robbins et al, 2003; Layton, 2005).

As discussed previously, there are various environments in an organisation. The effects of rewards, in the Utilitarian Environment, and consequences, in the Coercive Environment, on goal-setting are indirect at best. This is because the evaluations are of past behaviour and does not necessarily mean that the behaviour will be replicated in future (Locke, 1968). Therefore, in terms of goal-setting and achieving the commitment to these goals, the Goal Consensus Environment is best.

The ideal information security environment would be one where all employees are actively working towards the same information security goals to protect information assets. The commitment to these goals would be displayed through *prosocial* behaviour. In other words, a Goal Consensus Environment where every employee is working towards the goals of information security. According to Griffin *et al* (2004), research has shown that organisational change is often the result of employees, who are self-managing, initiating change at a local level.

However, the Theory of Cognitive Development states that logical people are not persuaded by direct orders without appropriate justification. Further, simply lecturing employees through exhortation on what they should do has little or no effect on *prosocial* behaviour (Kabay,2002; Layton, 2005). According to Goal-setting Theory, instructions or orders will only influence behaviour if they are consciously accepted by each employee and then translated into specific goals. Employees, however, will only translate instructions into goals, if they perceive that they are capable of executing the instructions and achieving these goals. When a person perceives that the achievement of a goal is not possible, commitment diminishes considerably (Layton, 2005). Therefore, it must be ensured that information security goals are perceived as attainable to ensure commitment.

Therefore, it is vital that the 'how' to achieve information security goals is communicated to employees through information security training as it has the goal of building knowledge and the necessary skills for employees to successfully protect information assets (Locke, 1968; National Institute of Science and Technology Special Publication 800-16, 1998).

6. Goal-setting to encourage *Prosocial* Behaviour

Management should, of course, be concerned with the behaviour and actions of employees as it relates to information security. Further, there is a strong relationship between goal-setting and actions. It has been found that specific or difficult goals produce better performance levels compared with vague or easy goals. These specific or difficult goals act as a compelling motivating force (Robbins et al, 2003; Layton, 2005).

Therefore, it is important that management set specific information security goals that should translate into the information security goals of employees. The *Prosocial* Behaviour Process is shown in Figure 3. As can be seen, the start of the process is management's articulation of the information security goals for the organisation. These information security management goals should be outlined in the corporate information security policy, which is the set of instructions for protecting information security assets. However, as mentioned previously, instructions will only translate into goals when employees consciously accept them and perceive these goals as being achievable. Therefore, the corporate information security policy, and related procedures, will only become part of the goals of employees when they consciously accept the policy. The first step towards employee acceptance of the policy or instructions will be to communicate the policy to employees through information security awareness and training. This will also assist in incorporating the information security goals of the organisation into the organisational *identity*. An organisation's *identity* provides coherence amongst management and employees and helps employees to accept certain roles because it forms part of "who we are" (Santos & Eisenhardt, 2005).

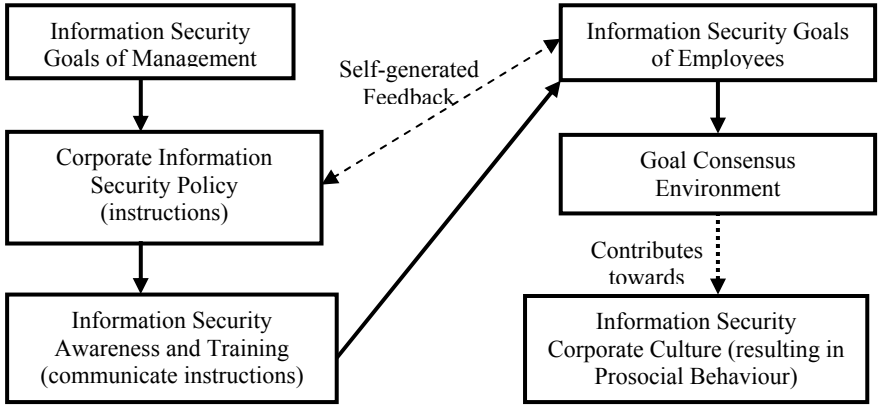

Figure 3: *Prosocial* Behaviour Process

The information security goals of employees should consistently be compared with the information security goals of management, expressed in the information security policy, to identify discrepancies. This could take the form of self-generated feedback where employees will compare their actions and behaviour to the information security policy. As indicated previously, self-generated feedback is an essential and effective component of Goal-setting Theory. As can be seen in Figure 3, once employees accept the information security goals as their own, the entire organisation will be working towards the same goals, in other words a Goal Consensus Environment will exist. As a corporate culture cannot be created overnight, this Goal Consensus Environment should, over time, evolve into an information security corporate culture where *prosocial* behaviour will be evident. Further, commitment to these goals should be demonstrated through *prosocial* behaviour. In other words, if there is any threat to information assets or a breach in security, the employees of an organisation will voluntarily react to protect the information assets.

7. Conclusion

It is often said that one of the weakest links in the information security chain is the employees of an organisation. Frequently, employees are apathetic to the protection of information assets and do not react to security threats. *Prosocial* organisational behaviour is generally the opposite of apathetic behaviour. In terms of information security, *prosocial* organisational behaviour should result in employees protecting information assets, without consequences or expectations of rewards, because they have accepted the organisational goals of information security.

Once employees have accepted and are committed to achieving information security goals, a Goal Consensus Environment has been created and employees see this environment as part of the corporate identity. Over time, an information security corporate culture will begin to emerge, which would ensure that employee actions and behaviour would reflect the information security goals of management outlined in the Corporate Information Security Policy.

8. References

Accel-Team (2000). *Change Management. Achieving Goal Congruence - Integration of Goals and Effectiveness.* (online). (cited 18 June 2005) Available from Internet: URL http://www.accel-team.com/techniques/goal_congruence.html

Brief, A.P. & Motowidlo, S.J. (1986). *Prosocial organisational behaviours.* Academy of Management Review, Vol 11, No 4, pp. 710-725.

Drennan, D. (1992). *Transforming company culture – getting your company from where you are now to where you want to be.* Berkshire, England : MacGraw-Hill, ISBN: 0-077-07660-5.

Griffin, M.A., Rafferty, A.E. & Mason, C.M. (2004). Who started this? Investigating different sources of organizational change. *Journal of business and psychology,* Vol 18, No 4, pp 555-570.

Kabay, M.E. (2002). *Computer security handbook - using social psychology to implement security policies*. John Wiley & Sons, Inc., ISBN: 0-471-41258-9.

Layton, T.P. (2005). *Information security awareness – the psychology behind the technology.* Bloomington, Indiana : AuthorHouse, ISBN: 1-4208-5632-4.

Locke, E.A. (1968). *Towards a theory of task motivation and incentives.* Organizational Behavior and Human Performance, Vol 3, Issue 2, pp. 157-189.

Messer, B.A.E, White, F.A. (2006). Employees' mood, perceptions of fairness and organizational citizenship behaviour. *Journal of business and psychology,* Vol 21, No 1, pp 65-82.

Mitnick, K.D. & Simon, W.L. (2002). *The art of deception – controlling the human element of security.* Indianapolis, Indiana : Wiley Publishing, Inc., ISBN: 0-471-23712-4.

National Institute of Science and Technology Special Publication 800-16 (April, 1998). *Information technology security training requirements: a role- and performance-based model.* Washington D.C. : Superintendent of Documents, U.S. Government Printing Office.

Robbins, S.P., Odendaal, A. & Roodt, G. (2003). *Organisational behaviour – global and South African perspectives.* South Africa : Maskew Miller Longman, ISBN: 1-86891-024-5.

Sathe, V. (1983). *Implications of corporate culture: A manager's guide to action.* Organizational Dynamics, pp. 5-25.

Santos, F. M. & Eisenhardt, K. M. (2005). Organizational Boundaries and Theories of Organization. *Organizational Science*, Vol 16, No 5, pp 491-508.

Schein, E.H. (1999). *The corporate culture survival guide.* San Francisco, California, United States of America : Jossey-Bass Publishers, ISBN: 0-78794-699-0.

Schein, E.H. (1992). *Organisational leadership and culture.* (online). (cited 12 January 2004) Available from Internet: URL http://www.tnellen.com/ted/tc/schein.html.

Srivastava, P. & Frankwick, G.L. (2011). Environment, management attitude and organizational learning in alliances. *Management decision,* Vol 49, No 1, pp 156-166.