An adaptation of the awareness boundary model towards smartphone security

Sean Allam
Information Systems Department
University of Fort Hare
East London, South Africa
scallam@gmail.com

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

Abstract— **Employees are becoming increasingly aware of the wealth of functionality available using smartphone computing; they fall hopelessly short in the awareness of the associated organisational information security risks associated with smartphone computing. Existing security measures are not adequately adapted for the risks introduced through smartphone usage. Therefore, there exists a need to apply principles of dynamic risk awareness to reduce organisational smartphone security risks. This paper examines the Awareness Boundary Model and its feasibility in reducing organisational risks introduced through increasing employee awareness of the information security risks of smartphone computing.**

Keywords-component; Smartphones, Mobile Computing, Information Security Awareness

I. INTRODUCTION

On the road, at the client, even while on holiday, more and more employees remain connected to their office through one critical piece of technology, the smartphone. Smartphones allow employees to communicate their ideas, decisions, queries and requests anywhere and at any time. While employees are becoming increasingly aware of the wealth of functionality available, they fall hopelessly short in the awareness of the associated organisational information security risks associated with smartphone computing [1].

Regular users of smartphones are generally unwilling to personally invest effort in mastering their devices [2]. The physical characteristics of these devices introduce far more complicated and dynamic organisational risks to those experienced by other fixed and mobile computing devices. Smartphone devices now rival personal computers in both sophistication and computing power [1] [2] [3] [4]. However, security measures of smartphone devices do not rival those of personal computers [1].

The nature of smartphone operations is as follows [1] [5] [6]:

- Smartphones are operated in both internally controlled (by the organisation of the employee) and externally uncontrolled environments (operated by a third party).
- Uncontrolled environments present more dynamic risks within the specific context and circumstances of that environment.
- Both the uncontrolled environment and associated risks present dynamic risk variables, impossible to define and therefore target specifically.
- Employees act in unpredictable ways when faced with various daily decisions.

This paper will focus on addressing the challenges introduced through the advance of smartphone usage within organisations. The dynamic environment of smartphone operation necessitates a holistic view of the problem. A background of the problem will analyse the dynamic operating environment. An in-depth discussion follows analysing the feasibility of adapting and applying Rasmussen's Awareness Boundary Model to the problem area. This presents a unique solution to the problem which conventional security measures have failed to adequately address.

II. BACKGROUND: A DYNAMIC OPERATING ENVRIONMENT

A number of factors combine to elevate the risk of smartphone computing above that of other computing devices. These factors are mostly attributed to the environment in which smartphone devices operate. The external environment is constantly changing. Each day introduces a completely new set of security risks. Smartphone users interact with different data sets or services resulting in changes to the information security threat. Furthermore, the convergence of data services increases the risk of cross contamination should one of these services introduce a security threat.

Even in controlled environments one finds that smartphones are usually connected to external networks communicating to numerous online services [1]. Therefore some element of risk from the external unknown environment still exists at all times.

Smartphone users are accustomed to the notion of anywhere and anytime access. The reliance on information access has become so great that often users will connect to the most convenient connection possible to 'update' their information. The array of different connectivity options available on smartphone devices provides multiple choices in such a situation. It is worth reiterating that the most convenient connection will likely be selected to perform the required connectivity task. Unfortunately, security measures can add an additional overhead to task execution. As a result, the most convenient connection is often the one which requires the least configuration or authentication measures.

Configuration and authentication measures are only as effective as the capability of the device and user. End users are usually inexperienced in configuring adequately secure communications [1] [7]. For example, while operating away from the organisation many smartphone users might find a situation in which they are required to interact with an external service over an external network. Unless they are familiar with the configuration required to maximise their security, they will be unable to perform adequate self-configuration of their devices [1]. Thus an inadequate level of awareness of the threats to smartphone security appears to exist.

A. Smartphone security and awareness

The complexities of the dynamic operational circumstances associated with the use of smartphone devices in many unique environments, presents a new much higher level of information security risk [1]. This is compounded further by the low levels of information security awareness of smartphone users.

Information security standards such as the ISO 27002 cover mobile computing, but refer to technical control measures such as backups, virtual private networking and cryptography [8]. While computing at the organisations' premises, technical support workers are available to implement and monitor such measures. In the case of smartphone computing, users are out on their own, sometimes even out of contact altogether. In this situation, policies, procedures and governance steps are at the mercy of the awareness level of that user. The effect on security is greater when addressing behaviour than any other single measure is [9].

For this reason it is crucial that one understands the cognitive steps undertaken in assessing situational threats in dynamically changing environments. The loss of such situational awareness could result in slower processing of problems and slower reactions [10]. Once understood, the steps to increasing awareness can appeal to such reasoning by adapting policies such that they form a fundamental component of the resulting behaviour of a user within such a situation. Layers of legislation, governance and policies will achieve very little unless they incorporate elements of raising the awareness levels of users [11] [12]. Awareness is detailed further in the following section which introduces the Awareness Boundary Model.

III. Theoretical Milieu: The Awareness Boundary Model

Rasmussen [13] points out that human behaviour in any work system is shaped by objectives and constraints which must be respected by the actors in order for work performance to be successful. Under this context, employees are increasingly performing task related objectives utilising their smartphone devices. However, daily advances in smartphone applications are enabling more and more tasks to be performed anywhere and at any time using a smartphone. Rasmussen [13] warns that aiming at productive targets leaves a wide degree of freedom open which must be closed by each individual actor. This is done through an adaptive search guided by process criteria such as work, load, cost effectiveness, risk of failure, joy of exploration, etc.

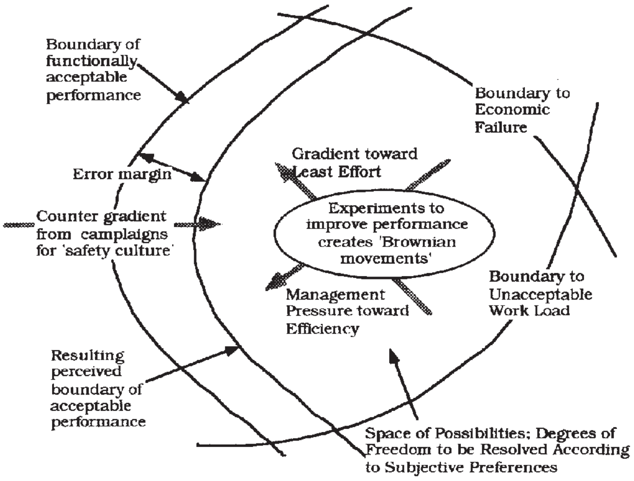
Boundary of functionally acceptable performance
Boundary to Economic Failure
Gradient toward Least Effort
Error margin
Counter gradient from campaigns for 'safety culture'
Experiments to improve performance creates 'Brownian movements'
Boundary to Unacceptable Work Load
Management Pressure toward Efficiency
Resulting perceived boundary of acceptable performance
Space of Possibilities; Degrees of Freedom to be Resolved According to Subjective Preferences

Fig. 1 - The Awareness Boundary Model [13]

The Awareness Boundary Model was established as a response to general accident mitigation in dynamic societal contexts. The model is a functionally abstract overview of the dynamic context of the working environment. Functional abstraction provides an excellent platform to model the awareness level of unpredictable tasks performed by uniquely configured smartphones.

Rasmussen [13] points to the existence of three boundaries within which human actors are free to navigate: administrative, functional and safety related constraints. He adds that during the adaptive search the actors will have ample opportunity to identify an effort gradient, whilst management will normally supply an effective cost gradient. These two gradients form two of the three gradients contained within the Awareness Boundary Model.

The effort gradient moves in a direction away from the boundary of unacceptable workload. At this boundary employees are expected to perform an unacceptable amount of tasks in order to perform their primary work objective. This is an inherently undesirable situation for human workers. Employees through this gradient seek to perform their task with the minimum amount of effort required. Therefore any component of a task that an employee might perceive to be unrelated to the objective of that task is at risk of being gradually "phased out" as a result of pressure along the gradient away from unacceptable workloads [14].

In a similar way the effective cost gradient moves in a direction away from the boundary of economic failure. At this boundary productivity is inadequate to ensure the financial stability of the organisation. This is an inherently undesirable situation for management and senior workers.

Together the two gradients will continue to move unabated away from their respective boundaries. This movement is likened to that of the Brownian movement of the molecules of gas [13]. As each of the gradients adjusts to pressures from that of the other, the operating position of the organisation will move randomly in between the two boundaries of economic failure and unacceptable workload. The result will be a systematic migration towards the boundary of functionally acceptable performance (see Fig. 2) [13].

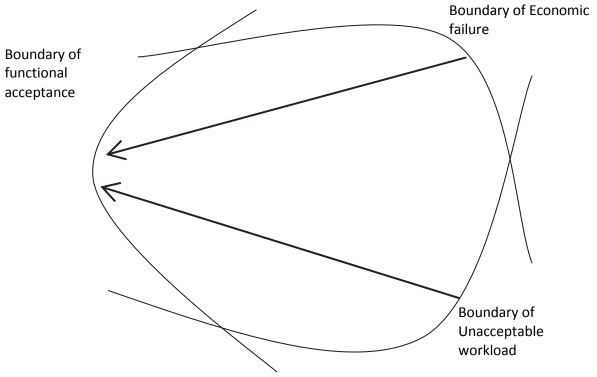
Boundary of Economic failure
Boundary of functional acceptance
Boundary of Unacceptable workload

Fig. 2 – Unabated Migration towards functional acceptance (adapted)

Without counter pressure, the efforts from each of these gradients will eventually result in a breach or crossing of the boundary of functional acceptance. It is at this point that accidents or errors are likely to occur [13] [15].

In the context of smartphone operations, this might result in a loss of organisational information. Rasmussen [13] describes the need for a set of counter gradient measures such as awareness campaigns. These serve to counter the gradient pressures from the boundaries of economic failure and unacceptable workload.

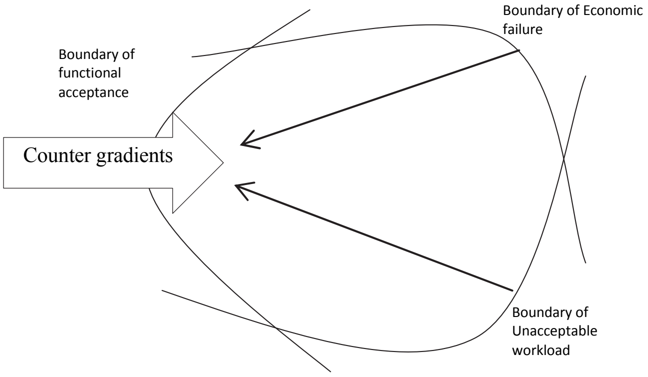
Boundary of Economic failure
Boundary of functional acceptance
Counter gradients
Boundary of Unacceptable workload

Fig. 3 - Counter gradients (adapted)

The gradient movements are dynamic in nature. A constant pressure exists to reduce cost and increase efficiency. Similarly, a natural resistance to unacceptable workload exists. Actors will continue to adjust efforts to maximise the pressure away from their respective gradients through experimental changes. As the pressure from these gradients adjusts systematically towards the boundary of functional acceptance, the counter gradient effort must be able to adapt to counteract these changes. This juggling act between the gradient pressures and the counter gradient pressure is what presents itself as a plausible model from which the dynamic information security environment of smartphone computing can be analysed.

Maintaining a balanced or steady state in which the pressures from the boundary can be safely countered is critical to ensuring a reduction in security incidents. Counter efforts should also not be so intense that the organisation is at risk of breaching either the boundary of economic failure or unacceptable workload.

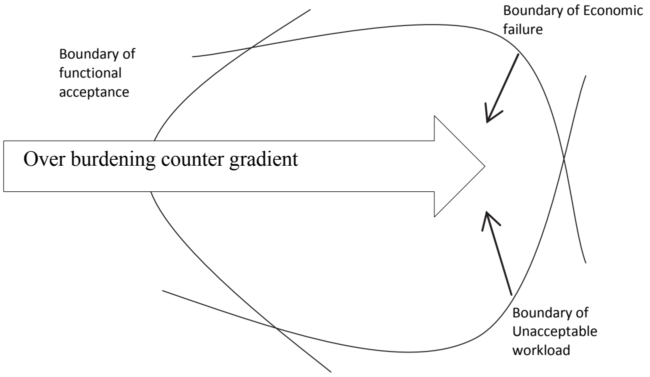
Boundary of Economic failure
Boundary of functional acceptance
Over burdening counter gradient
Boundary of Unacceptable workload

Fig. 4 - An overburdening counter gradient (adapted)

In Fig. 4 the counter gradient is so intense that the pressure away from the boundaries of economic failure and unacceptable workload are overpowered. This scenario is realised where extreme policies or campaigning hampers efforts to lower costs, increase efficiency and reduce workload. It would likely result in much resistance from both managers and employees as they seek to move instead in the direction of functional acceptance. The stronger the pressure on each of the gradients, the higher the level of resistance each gradient will exert from its boundary.

Fig. 4 illustrates the devastating effect an excessive smartphone security programme would have on the gradients. Smartphone users would resist or disable the security measures to avoid being pressured across the boundary of unacceptable workload. Managers might resist smartphone usage altogether as too burdensome for economically feasible operation. It becomes important to find a manner in which a perfect balance can be achieved and maintained. The next section investigates general systems theory as a means to achieve such a level.

A. Application of General Systems theory

The unpredictable nature of security threats in a dynamic environment increases the complexity in establishing effective mitigation measures and controls. The reality is that security measures cannot be implemented for security threats which are not understood and are constantly evolving. General systems theory can provide an effective measure of the feasibility of the Awareness Boundary Model in handling a dynamic environment.

When applied to general systems theory the Awareness Boundary Model appears to be a perfect fit. The sociological undertone of the model is evident in the criteria at the gradient boundaries. Excessive workload and economic failure are both social concerns.

Von Bertalanffy [16] provides general systems theory in order for theory from sociological realms to be understood by physicists. General systems theory was established as a way to define a new scientific doctrine of the concept of wholeness [16]. It is to this concept that the Awareness Boundary Model is being applied so that it can encompass the whole the decision system for smartphone security.

The relationship between a system and its environment is important within general systems theory [16] [17]. This is the reason that the boundaries form such an important part of this model. The Awareness Boundary Model introduces a set of boundaries within which organisational decisions continuously move around according to pressure from both of the gradients. Further to this, the components of that system are continuously changing. New devices are introduced with new security configurations, and new organisational information is being added to these devices continuously. Economic conditions change, as do the threats to smartphone security. Von Bertalanffy [16] describes a similar movement in the characteristics of every organic system in that it maintains itself in a state of perpetual change of its components. Under the definition of systems theory the Awareness Boundary Model can be classified as an open system. This is attributed to the inflow and outflow of materials into and out of the system.

In understanding how the inflows and outflows affect the whole system, one should be able to establish the counter-measures which will maintain a balance as close to the boundary of functional acceptance as possible. Von Bertalanffy [16] states that in an open system a steady state will be maintained, irrespective of the initial content, because it is only determined by the constants of reaction and of inflow and outflow, as opposed to closed systems which arrive at their final state depending on the components at the beginning of the process [16].

Enhanced self-regulatory systems rely on a portion of their output to be returned as input in the form of feedback [16]. Feedback can form a very important part of a system in achieving an enhanced steady state. Feedback forms an important consideration towards maximising the effectiveness of balancing the counter gradient measures within the Awareness Boundary Model. The interrelation of the gradient pressures and counter acting control measures maintain the system in a steady state in which risk can be minimised.

As all threats cannot be reliably preconceived, it becomes impossible to measure system effectiveness. Feedback only acts to relay the current state of the system. Feedback cannot determine the future state of the system. There exists a greater meaning for which the system itself must exist. This is the emergent property of the system [17] [18]. One in which the individual parts act together to produce a quantity greater than their individual sum.

Increased smartphone security is the ideal emergent property from the adapted Awareness Boundary Model. Increased smartphone security is not a destination in time. It exists as a purpose over time for which the system is constantly self-regulating itself to achieve. In order to achieve such an emergent property from the system, a system of control should be established to manage interactions rather than actions [17].

In the next section methods of controlling system performance, as provided by [13], are discussed.

B. Controlling system performance

In this section methods of controlling the performance of the system are considered with a view to minimising breaches of the boundary of functional acceptance.

Rasmussen [13] indicates that instead of striving to control behaviour by fighting deviation from a particular pre-planned path, there should be a focus to control the behaviour by making the boundaries explicit and known and through provision of coping skills at boundaries. This can be achieved through the following methods:

- Increasing the margin between normal operation and the point at which control will be lost
- Increasing awareness of the boundary
- Implementing a combination of the above

1) Increasing the control margin

Increasing the margin between normal operation and the point at which control will be lost creates a compensation factor to accidents. Should an incident occur the distance to the point of control loss acts as a protective "defence in depth" strategy. The resulting level of safety consequently depends on the recovery characteristics of the system [13]. Any efforts to redesign the system for efficiency may decrease this margin resulting in a deterioration of the level of safety [13].

Technical measures such as solely those of traditional security policies and procedures provide such a margin between normal operation and the point of loss of control. Measures such as backup and recovery, encryption and authentication each provide a reasonable level of security from the point at which control is lost. Unfortunately these measures are usually ignored by smartphone users who are unaware of the purpose of such measures. The result of this is that over time, efforts along each gradient away from the respective boundary will see the overall margin begin to shrink. This is as users experiment with different techniques to maximise efficiency and minimise workload. Effectively users will challenge the security margin in their efforts to resist their respective boundaries. As there is no clear awareness of the boundary of functional acceptance users will be unable to resist penetrating the functional acceptance boundary and avoid the errors and accidents which are then likely to follow.

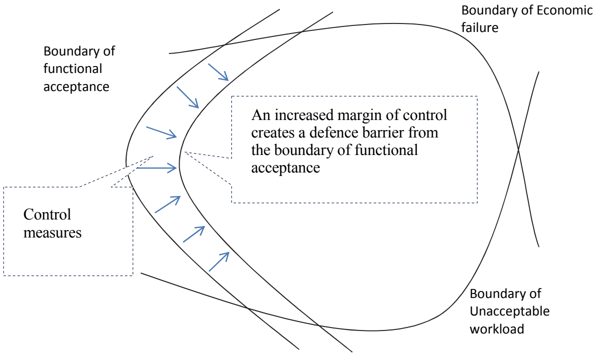
Boundary of functional acceptance
Boundary of Economic failure
An increased margin of control creates a defence barrier from the boundary of functional acceptance
Control measures
Boundary of Unacceptable workload

Fig. 5 - Increasing the margin of resistance to accidents (adapted)

2) *Increasing awareness levels*

The second option of increasing awareness at the boundaries benefits the security of the whole system through efforts to actively counteract each of the respective gradients. Rasmussen [13] points out that this is achieved through instruction and motivation campaigns. This natural counter gradient acts to preserve the margin between operation and the point at which control is lost. It however becomes important to ensure that there is continuous pressure against the gradients. Without a constant counter gradient the gradient pressures would eventually manage to penetrate the functional acceptance boundary with undesirable effect.

Increased awareness should be installed for both the boundary of functional acceptance and the control measures in place to maintain such a boundary.

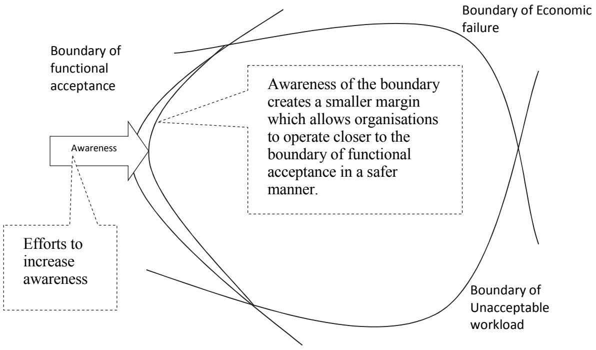
Boundary of functional acceptance
Boundary of Economic failure
Awareness
Awareness of the boundary creates a smaller margin which allows organisations to operate closer to the boundary of functional acceptance in a safer manner.
Efforts to increase awareness
Boundary of Unacceptable workload

Fig. 6 - Awareness of the boundary (adapted)

The goal of such campaigns is to provide an awareness of the boundary of functional acceptance. This ensures that employees understand at which point there is a possibility of a loss of control. It also allows organisations to operate at the furthermost position from each of the two boundaries of economic failure and unacceptable workload. At this point gradient resistance from these boundaries is at its weakest. From this analysis it becomes clear that the second option of providing a continuous awareness strategy most effectively allows for operation as close as possible to the boundary of functional acceptance, reducing the resistance from each of the gradients away from their respective boundaries. Elements of the first option would certainly still play a role as a minimum amount of policy and procedure is essential.

IV. An Adaptation for Smartphone Security Awareness

The purpose of adapting the existing model is to better ensure that the model is positioned to respond to the dynamic risks associated with smartphone computing. The adaptation is intended to be specifically performed to address the unique concerns of smartphone computing, without reducing the generic application of the model to a dynamically changing risk environment. Furthermore, the model can be enhanced by incorporating additional general systems theory concepts to provide a more credible and complete solution, which is grounded on reputable theory.

1) *Feedback as a self-regulatory measure*

The first adaptation is the inclusion of feedback into the model. The importance of feedback as covered earlier is to ensure that an enhanced level of self-regulation is achieved. Therefore, when there is a need to exert extra pressure away from one of the boundaries this can be achieved at a higher level of safety. An example might be where an organisation places increased pressure on employees close to the deadline of a major client deliverable. With feedback, the organisation could be warned before a major accident is likely to occur (through breach of the boundary of functional acceptance).

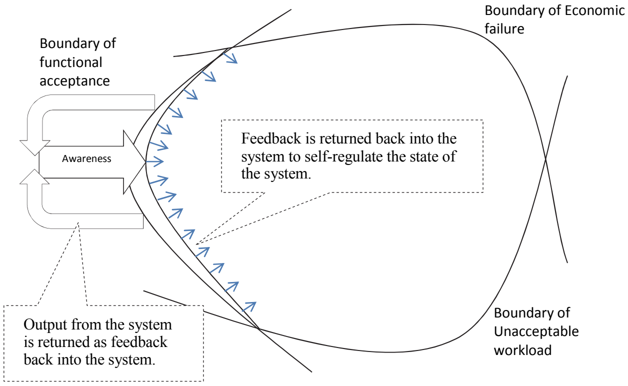
Boundary of functional acceptance
Boundary of Economic failure
Awareness
Feedback is returned back into the system to self-regulate the state of the system.
Output from the system is returned as feedback back into the system.
Boundary of Unacceptable workload

Fig. 7 - Introduction of feedback (adapted)

2) *Readapting the boundaries*

The next adaptation focuses specifically on the boundaries of unacceptable workload and economic failure. Unacceptable workload and economic failure are very broad concerns more farther reaching than through only smartphone operation. In order to ensure that pressures unrelated to smartphone operation do not influence the gradient pressures, each of the boundaries will be redefined specifically. Both boundaries must be redefined to reflect only the smartphone operational concerns within the broader concern of each respective boundary.

The boundary of unacceptable workload represents the point at which performance of work tasks in achieving organisational objectives requires an unacceptable amount of effort. Using a smartphone for a task becomes unacceptable if achieving the task objective outweighs the advantages of performing the task using a smartphone. The unacceptable workflow boundary is adapted as the boundary of unacceptable smartphone operation. This retains the broad scope of the boundary while simultaneously restricting it to only smartphone operational gradient pressures.

For the boundary of economic failure, a similar adaptation is required. The boundary represents a point at which the economic feasibility of the organisation is irreversibly terminated. Smartphone operations are unlikely to cause complete economic failure, except in massive security breaches. Instead, as it relates to smartphone usage, management is more likely to be concerned with the economic benefit. A constant pressure from the direction of management is to implement smartphones to reduce costs or increase productivity (and therefore profit). The economic failure boundary is adapted as the boundary of economic feasibility of smartphone usage. Again the broad scope of the boundary is retained while simultaneously restricting the gradient pressures for maximising the economic feasibility of smartphone devices.

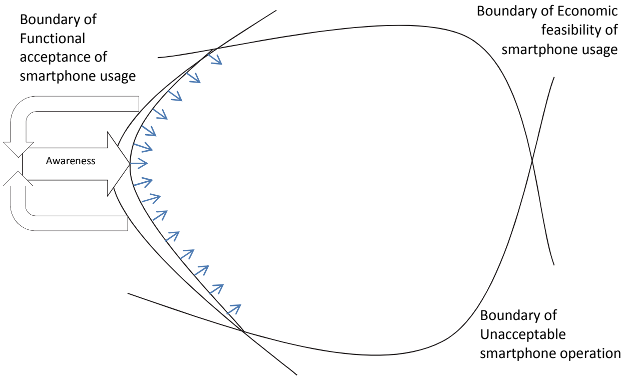
Boundary of Functional acceptance of smartphone usage
Boundary of Economic feasibility of smartphone usage
Awareness
Boundary of Unacceptable smartphone operation

Fig. 8 - Adaptation of awareness boundaries (adapted)

Finally, the boundary of functional acceptance is adapted to simply express the boundary of functional acceptance of smartphone usage. Fig. 8 illustrates the adapted boundaries and feedback components.

V. ADAPTATION FEASIBILITY ASSESSMENT

Feedback mechanisms underpin many of the controls found on the COBIT 4.1 (COBIT) Framework [19] and the ISO 27002 security standard. Although each of these documents is focused at difference levels of organisational security, both contain control objectives with corresponding controls. The breadth and depth of control objectives and controls listed in each document are extensive and likely to be in excess of what is possible to achieve in all but the very largest organisations. For this reason the adapted Awareness Boundary Model provides an excellent basis from which an adapted set of control objectives can be established to increase organisational smartphone security levels.

Organisations can utilise the model to establish security awareness controls for each of the processes which apply to smartphone computing. Each process will reveal an organisational position based on the result of analysing the influence of each of the gradients on that task. Relevant control objectives can be selected for their ability to either increase or decrease pressure on one of the gradients (the counter gradient). By reducing the amount of control objectives required, awareness is more likely to lead to obedience, commitment and finally to form culture [14] [20]. Feedback mechanisms must be implemented as an output from each of the related controls for the control objectives provided.

Consider the following example. If an organisation allows employees to access an enterprise resource planning (ERP) system directly from their smartphone devices, this process would be a candidate for assessment with the adapted model. In the event that password complexity rules are not enforced (no counter gradient) the resulting model assessment would appear as follows.

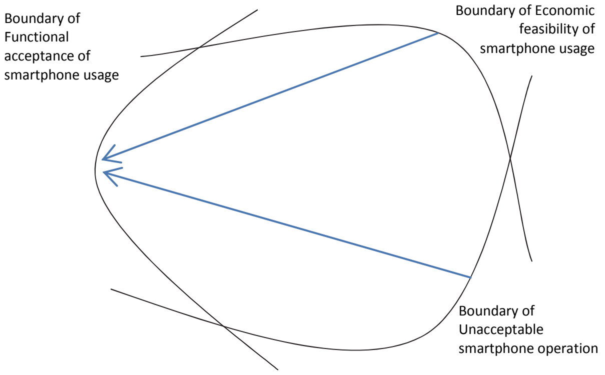
Boundary of Functional acceptance of smartphone usage
Boundary of Economic feasibility of smartphone usage
Boundary of Unacceptable smartphone operation

Fig. 9 - Example awareness model assessment (adapted)

Fig. 9 above illustrates the organisation position as very close to the boundary of functional acceptance. Without the password complexity rules, users are likely to set very insecure or short passwords [21]. As a short password reduces effort in performing the task (minimum required input), this is illustrated as a position far from the unacceptable workload boundary. Similarly, the short password results in maximum productivity (through minimum effort). This is illustrated as a position far from the economic feasibility boundary. As both gradients are extended from their respective boundaries, the organisation is operating dangerously close to the boundary of functional acceptance of smartphone usage. This is a higher level of operational risk.

Implementing a password complexity rule set which provides feedback and an explanation if the user selects a short password, along with an awareness programme, would result in lower risk [21]. As a password complexity rule set forces a user to select a more complex password, there is a small increase in workload required. This results in an equally small decrease in productivity. Fig. 10 illustrates the increased pressure on both of the gradients, which results in the movement of the organisation to a safer operating distance from the boundary of functional acceptance.

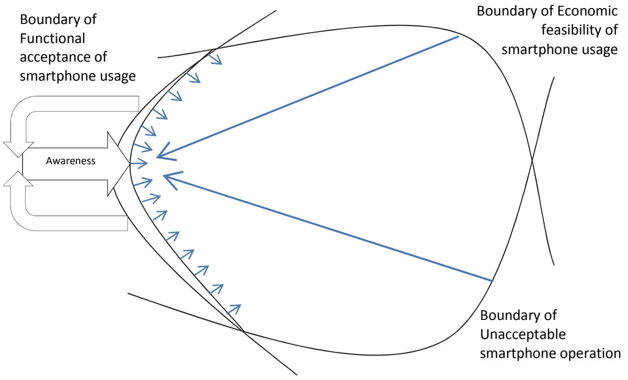

Fig. 10 - Example with counter gradient (adapted)

VI. Conclusion

Smartphones should not be viewed as a risk to organisations, but instead a potential technology to increase operational efficiency and provide strategic advantages. Ensuring that security is maintained is as much a responsibility of the employee as it is the management of the organisation. Without an awareness of the security risks from smartphone operations, users and managers will be unable to make the informed decisions required to maintain adequate levels of security.

This paper proposed a model adapted from the Awareness Boundary Model. The adapted model was enhanced by applying principles from the general systems theory. The model was further refined to apply directly to the operational concerns of smartphone computing in dynamic risk environments. The resulting model is one in which organisational control objectives can easily be applied, such that they specifically address the concerns of the gradient pressures.

The result is intended to be a balanced system of information security grounded on awareness and regulated by extensive feedback. This self-regulatory environment should act to maintain the awareness level and reduce breaches of the boundary of functional acceptance of smartphone usage. This translates directly into lower risk for organisations where smartphone computing is in operation.

VII. References

[1] R. Botha, S. Furnell, and N. Clarke, "From desktop to mobile: Examining the security experience," Computers & Security, vol. 28, no. 3-4, pp. 130-137, 2009.

[2] A. Oulasvirta, M. Wahlström, and K. Anders Ericsson, "What does it mean to be good at using a mobile device? An investigation of three levels of experience and skill," International Journal of Human-Computer Studies, vol. 69, no. 3, pp. 155-169, March 2011.

[3] J. Wexler, "The many faces of smartphones," Business Communications Review, January 2005.

[4] L. Pitt, M. Parent, I. Junglas, A. Chan, and S. Spyropoulou, "Integrating the smartphone into a sound envrionmental systems strategy," The Journal of Strategic Information Systems, vol. 20, no. 1, pp. 27-37, March 2011.

[5] J. Jürjens, J. Schrek, and P. Bartmann, "Model-based Security Analysis for Mobile Communications," in International Conference on Software Engineering, Leipzig, Germany, 2008, pp. 683-692.

[6] S. Furnell, "Handheld hazards: The rise of malware on mobile devices," Computer Fraud & Security, vol. 2005, no. 5, pp. 4-8, May 2005.

[7] R. Khokhar, "Smartphones - a call for better safety on the move," Network Security, vol. 2006, no. 4, pp. 6-7, April 2006.

[8] Standards South Africa, "SANS 17799:2005," Pretoria, ISO 17799:2005, 2005.

[9] E. Albrechtsen, "A qualitative study of users' view on information security," Computers and Security, vol. 26, no. 4, pp. 276-289, 2007.

[10] N. A. Stanton, P.R. G. Chambers, and J. Piggott, Situational awareness and safety. Egham: Safety Science, 2001.

[11] H. A. Kruger and W. D. Kearny, "Consensus ranking – An ICT security awareness case study," Computers and Security, vol. 27, no. 7-8, pp. 254-159, 2008.

[12] T. Olzak. (2006, April) Adventuresinsecurity.com. [Online]. http://adventuresinsecurity.com/Papers/Build_a_Security_Awareness_Program.pdf

[13] J. Rasmussen, "Risk management in a dynamic society: a modelling problem," Safety Science, vol. 27, no. 2, pp. 183-213, 1997.

[14] S. Allam and S. Flowerday, "A model to measure the maturity of smartphone security at software consultancies," in Proceedings of the South African Information Security Multi-Conference (SAISMC 2010), Port Elizabeth, 2010, pp. 110 - 121.

[15] R. Cook and J. Rasmussen, "‘‘Going solid’’: a model of system dynamics and consequences for patient safety," Quality Safety Health Care, no. 14, pp. 130 - 134, 2005.

[16] L. Von Bertalanffy, "An Outline of General System Theory," The British Journal for the Philosophy of Science, vol. 1, no. 2, pp. 134-165, August 1950.

[17] J. Gharajedaghi, Systems Thinking, Managing Chaos and Complexity: A Platform for Designing

Business Architechture, 2nd ed. Burlington, MA, United States of America: Butterworth-Heinemann, 2006.

[18] B. G. Hanson, General Systems Theory: Beginning with wholes, 1st ed. London, United Kingdom: Taylor & Francis, 1995.

[19] IT Governance Institute, "COBIT 4.1," Illinois, 2007.

[20] S. Furnell and K. L. Thomson, "Recognising the varying user acceptance of IT security," Computer Fraud & Security, no. 2, pp. 5-10, 2009.

[21] D. Emm, "Creating secure passwords," Infosecurity, p. 36, November / December 2010.