A Model to Measure the Maturity of Smartphone Security at Software Consultancies

S. Allam and S. Flowerday

Department of Information Systems, University of Fort Hare, South Africa
e-mail: scallam@gmail.com, sflowerday@ufh.ac.za

Abstract

Smartphones are proliferating into the workplace at an ever-increasing rate. Similarly the information security threats that they pose are increasing. In an era of constant connectivity and availability, information is freed up of constraints of time and place. The risks introduced by smartphones are analysed through multiple cases studies, and a maturity measurement model is formulated. This model is based on recommendations from two leading information security frameworks, the COBIT 4.1 framework and ISO27002 code of practice. Ultimately, a combination of Smartphone specific risks are integrated with key control recommendations to provide a set of key measurable security maturity components.

The empirical evidence is gathered using an in-depth questionnaire of 67 question statements adapted from each of the activities recommended by the COBIT 4.1 processes which target risk management as a primary objective. The opinions of 58 respondents are included as key components in the model. The solution addresses the concerns of not only policy makers, but also the employees subjected to security policies. Nurturing security awareness into organisational culture through reinforcement and employee acceptance is highlighted in this research paper. Software consultancies can use this model to mitigate risks, while harnessing the potential strategic advantages of mobile computing through smartphones. In addition, the critical components of a Smartphone security solution are identified. As a result, a model is provided for software consultancies due to the intense reliance on information within these types of organisations. The model is applicable to any information intensive organisation.

Keywords

Smartphones, Mobile Computing, Information Security, Software Consultancies

1. Introduction

"A chain is no stronger than its weakest link; but if you show how admirably the last few are united; half the world will forget to test the security of the parts which are kept out of sight" (Stephen, 1868, p. 295). Stephen suggests that a chain's strongest link often overshadows its greatest vulnerabilities.

These vulnerabilities are the hidden weaker links in the chain. They are the issues in the chain that one prefers not to have to deal with, instead focusing on the more visible ones. The result, as concluded by Stephen, is that one is often under an illusion that the strength of a chain is as strong as the strongest linkages, as these are the ones most visible.

Smartphone security is proving to be one such area of weakness. In order to develop a model capable of measuring the maturity of Smartphone security within software consultancies, the areas of risk need to be identified, and information security must be at the centre of the solution.

Gartner (2009) research group define the Smartphone as a "large-screen, voice-centric handheld device designed to offer complete phone functions while simultaneously functioning as a personal digital assistant (PDA)." Palm (Elgan, 2007) provides the following definition, "a portable device that combines a wireless phone, e-mail and Internet access and an organiser into a single, integrated piece of hardware".

This paper focuses on the requirements for a model to measure the maturity of Smartphone security within software consultancies. The paper will begin by discussing the information security and awareness requirements followed by an analysis of Smartphone security risks and the risks of Smartphones to software consultancies. In the final section of this paper the methodology used to derive the components of the model is explained. The concluding model is then presented and an explanation of its contribution is provided.

2. Information security and Smartphone's in software consultancies.

Organisational information is one of the key assets of any organisation. Smartphone's have introduced another area of potential information security weakness into an organisation's chain of security. More and more organisational information is being stored, processed and transported using these devices. Securing this information is the ultimate goal of Smartphone security. Today, information assets are found to be exposed to an ever increasing number of threats and vulnerabilities.

2.1. Information security

Employees do not tend to take as much care of information assets as they would with a physical asset. Kruger and Kearny (2008) point out that companies will often spend huge amounts of money and time on implementing technical solutions while the human factor in information security receives relatively less attention. From this it becomes apparent that even the most secure information security solution would be futile without the support of the employees with whom it is tasked to protect.

Olzak (2006) states that one of the most important pieces of an effective information security solution is employee awareness; especially new employees who may not be aware of existing policies, or the need for these information security policies. It becomes vitally important that employees are aware of such programs at the initiation of their employment with the organisation. Existing employees require constant reminding, using both direct and indirect means of reinforcing that awareness. This reinforcement eventually leads to information security practices becoming a part of the organisational culture of an organisation. Furnell and

Thomson (2009) state that the culture of an organisation is not formed by what management preaches or publishes, but what it accepts in practice.

The traditional mindset of information security, as being a defence strategy from outside offenses, needs to be updated or redefined to an offensive strategy on internal security weaknesses. This is especially important for smartphone security. Still in its infancy, smartphone security is at a higher risk from both internal and external threats, than more mature computing platforms. Dunn (2007) agrees suggesting that smartphone security is a largely neglected area.

2.2. Smartphone security risk areas

The areas in which smartphone security is at risk differs from traditional areas of risk to fixed computing devices due to various factors which define these devices. Botha, Furnell and Clarke (2009) provide a number of specific mobile computing security risk areas. Seven areas are defined as most significant to smartphone security. These areas are included as measurable items in the model provided by the paper. The seven significant risk areas are provided below.

- Botha, Furnell and Clarke (2009) point out that early generations of cell phones and PDA's had relatively little storage capability. Johnson (2009) indicates that today's generation of devices can be quickly and easily upgraded by adding additional storage cards. Botha, Furnell and Clarke (2009) add that a malicious user would be able to insert unencrypted expansion media from one device into another device in order to easily access that information.
- Because of their mobile characteristics, smartphone devices are also more likely to be exposed to destructive elements such as sand, water or fire than fixed machines.
- One of the key challenges of smartphone security is that these devices can perform both personal and work related tasks. Quite often, the device belongs to the employee personally. However, even where the device is company issued, employees will tend to personalise their device to their preferences. According to Botha, Furnell and Clarke (2009), this has become a significant point of neglect by organisations, who have failed to acknowledge that users are often responsible for configuration of their smartphones, while administrators secure their desktops. Furnell, Josoh and Katsabas (2006) point out, that although some users will actively seek to overcome secure configurations, the most likely scenario is that security configurations will be unused or configured incorrectly.
- Botha, Furnell and Clarke (2009) also found that smartphone users are of the opinion that periodic re-authentication is intolerable on smartphone devices, but widely accepted on desktop machines. Clark and Furnell (2007) add that existing PIN-based techniques are under-utilised, and provide an inadequte level of protection when compared to the sensitivity of data and services accessible through the devices. Jürjens, Schrek and Bartmann (2008) explain that users tend to adopt a short and nomadic usage pattern with smartphones.

- Another unique challenge introduced with the smartphone, is that these devices are no longer limited to communicating over only the public cellular network. The majority of users do not know appropriate security settings, and will connect to the least secure network that requires minimal configuration.
- Mobile applications are rapidly becoming available for smartphone devices. These applications are targeted at providing access to the same information that users access on their desktop machines. While the level of sensitivity of the data remains the same, the security level of smartphone applications is usually much lower than the desktop version of the same application.

2.3. Software consultancy organisations

Software consultancy organisations are perfectly positioned to take advantage of the benefits introduced by smartphone devices. They operate by identifying and implementing software based solutions to business problems and requirements.

Software consultancy employees of all levels deal with vast amounts of information on a daily basis. This information is usually part of a collective effort towards achieving a work task. The work tasks processed by software consultancy organisations produce information deliverables. These information deliverables usually feed into other work tasks, effectively creating a chain of information flowing from customer requirements through to solutions development. Information becomes both an input and output of each process in this type of organisation.

Attempting to define a unique security solution from the ground up would prove overwhelming for almost any software consultancy. Industry recognised and accepted security frameworks already exist. These can be utilised in the development of a smartphone security solution. The following section introduces these frameworks and their role in developing a model to measure the maturity of smartphone security.

3. The COBIT 4.1 Framework and ISO 27002 standards

Karyda, Kiountouzis, and Kokolakis (2005) reason that there is no single security solution or policy that can fit all organisations. Organisations attempting to implement an authoritarian approach to security, risk losing support from end users.

Both employees and managers should subscribe to a common set of security requirements and policies. These policies are required in order to maintain a balance between employee, management and security requirements. This balance requires security experimentation to discover an optimum level of security and efficiency. This should be achievable through adaption of existing best practices, to the context of smartphone security in software consultancy organisations.

In order to achieve this, best practice approaches must be indentified from existing security frameworks. Two such frameworks are the COBIT 4.1 framework and ISO27002. These security frameworks are both widely accepted and utilised in the

information technology industry. Independent global groups manage them both, through continuous revision.

3.1. The COBIT 4.1 Framework

The COBIT 4.1 framework provides good practices across a domain and process framework, and presents activities in a manageable and logical structure (IT Governance Institute, 2007a, p. 4).

COBIT 4.1 provides recommended control objectives, to assist in choreographing this effort. COBIT 4.1 also ensures that all stakeholder responsibilities are clear and adequate measurement devices available. Ongoing measurement is a key part of monitoring the control objectives. The COBIT 4.1 framework provides a complete set of high-level requirements to be considered by management, for effective control of each IT process (IT Governance Institute, 2007a). Due to the sheer number of different types of smartphones, operating systems and potential uses, management would not be able to provide a specific set of instructions for each. Instead, management must ensure that an adequate set of high-level controls are provided, in such a way that they generically cover as many possible security requirements as possible.

The COBIT 4.1 framework covers five specific IT governance domains:

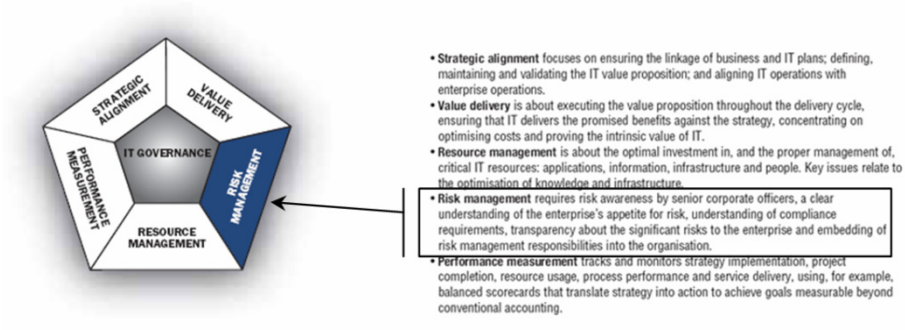

Figure 1 - IT Governance focus areas (IT Governance Institute, 2007a)

Of these five domains, this research project focuses on COBIT 4.1 domain processes of which the area of "risk management" is the primary focus. This ensures that the solution focuses on providing a model that satisfies solely the requirements of measuring smartphone security readiness. Risk management is the most relevant governance area in relation to information security management. Risk management seeks to embed the responsibilities of security into the organisation.

By basing the questionnaire on activities recommended by these domains, the risk management controls form a core part of a smartphone security readiness model. Three of the four domains are represented (Plan and Organise, Deliver and Support and Monitor and Evaluate), as only these three contain processes that target risk management as a primary objective.

3.2. ISO 27002 code of practice

The purpose of the ISO27002 code of practice is to establish guidelines and general principles for initiating, implementing, maintaining and improving information security management in an organisation organisation (Standards South Africa, 2005). The guide provides direction on the commonly accepted goals of information security. The IT Governance institute provides a mapping document, which maps the components of the COBIT 4.1 framework, to that of the ISO27002 code of practice. Using this document, the components of the COBIT 4.1 framework selected as targeting risk management, can be mapped to the objectives of the ISO27002 code of practice.

4. Research Methodology and Findings

The research methodology selected was based on a qualitative approach. Myers (1997) states that the motivation for doing qualitative research comes from the observation that humans possess the ability to communicate. Myers indicates that humans have the ability to form both social and cultural constructs based on their interactions with each other.

A questionnaire was utilised as the research instrument for each case study. The extensive questionnaire of 67 question statements was distributed electronically to randomly selected software consultancies. This resulted in a convenient sample of 58 in-depth responses from multiple randomly selected software consultancies and from various roles within those organisations.

In order to gain insight into the security risks of smartphone devices, this study was performed as a multiple case study. Tellis (1997, p. 1) points out that, "multiple cases strengthen the results by replicating the pattern-matching, thus increasing confidence in the robustness of the theory." The questionnaire was instructed to be answered within the context of the organisation at which the respondent is employed.

A smartphone process framework has been developed.					
Very Unimportant	Unimportant	Neutral	Low Importance	Moderately Important	Very Important

Table 1 - Question example

Respondents were asked to read each statement as part of the question, "how important is it to [their company] that ...", followed by each statement. When read with the previously provided prefix, the statement reads as follows: how important is it to [your company] that a smartphone process framework has been developed. The Linkert Scale requires respondents to provide their opinion as the answer. In order to ensure that the questionnaire provided the highest quality responses, a select number of respondents conducted a pilot study. The pilot study took place two weeks before the questionnaire was scheduled to be released. Pilot study participants were randomly selected. The questionnaire was modified to satisfy any concerns raised by the pilot study group.

In order to enhance the comparative component of the analysis, the results were first considered for all respondents; and then separately based on the respondents' response to the following question: "Are you directly responsible for the definition, implementation OR maintenance of the security requirements of your organisation? ." 19 (or 33%) of the 58 responses were from respondents that indicated that they were responsible for security policies at their organisation.

Separating the users into two groups assists in providing a contrasting analysis between the users implementing and designing security solutions and those who are governed by the security solution. Once the requirements of each population group have been identified, these can be addressed together to ensure that the solution addresses the requirements of both population groups. Once the requirements of both groups are accommodated for it becomes easier to achieve acceptance of the security requirements. Acceptance of security is one of the steps in achieving full awareness of information security.

The results were analysed along the following criteria:

Determination of the question statements that received the highest score ratings.

- Overall
- By respondents who were responsible for security policies.
- By respondents who were not responsible for security policies at their organisation.

Determination of the question statements that received the lowest score ratings.

- Overall
- By respondents who were responsible for security policies.
- By respondents who were not responsible for security policies at their organisation.

Determination of the question statements that yielded the greatest discrepancies between the respondents responsible for security policy, and those not responsible.

- Above standard deviation.
- Below standard deviation.

Determination of the level of importance across each of the represented domains from the COBIT 4.1 framework.

4.1. Empirical study findings

The questionnaire results pointed to the Planning and Organising domain of the COBIT 4.1 framework as having the most significant activities for employees. This was the same for employees who were responsible for security and those who were not responsible.

From the questions, topics dealing with the following ten items received the highest levels of significance from respondents. The level significance was determined from the average level of importance selected by respondents for each question statement.

- System ownership
  - Smartphone system owners have been identified.
- Information ownership
  - Smartphone users are aware of who owns the data processed and stored on their device.
- Restoration and continuity
  - An IT continuity framework has been developed, and this framework includes smartphones.
  - Procedures for smartphone data restoration have been defined, maintained and implemented.
- Backup policy and scheme
  - Smartphone information backup storage and protection has been planned for and implemented.
  - Smartphone data is backed up according to scheme.
- Ownership
  - Smartphone users are aware of who owns the data processed and stored on their device.
- Supplier and service delivery management
  - Smartphone supplier management processes have been defined and documented.
  - Smartphone supplier service delivery is monitored.
  - The long-term goals of the smartphone service relationship for all stakeholders has been evaluated.
- Risk awareness through control framework
  - A smartphone control environment and framework has been established, and is being maintained.
  - Events associated with smartphone objectives have been identified.
  - Smartphone risks associated with events have been assessed.
- Multi-level strategy awareness
  - Smartphone control frameworks, objectives and direction have been communicated to smartphone users.
  - The relative strategic business objectives of smartphones are understood.
  - Relevant smartphone business process objectives are understood.
- Rights and privileges
  - Smartphone user access rights and privileges are periodically reviewed and validated.
- Governance report
  - An IT governance report has been generated and includes feedback on the performance of smartphones.

These items were the most significant items across all of the population groups identified previously. This approach satisfies the requirements of employees responsible for security and those who are not. It also addresses items that display

the highest levels of deviation between these groups. As indicated earlier, achieving acceptance from employees is paramount to the success of any security effort.

4.2. Smartphone security model.

The seventeen measurable components for the model are comprised of a combination of the seven smartphone risk items identified in the secondary data collection and ten items from the primary data collected.

In section two, seven smartphone risks identified by Botha, Furnell and Clarke (2009) are listed. These are subsequently mapped to one of the IT resource categories of the COBIT 4.1 framework. These items are included in the model, as they provide a measureable risk component across each of the smartphone security risks areas. However, this does not fully satisfy the IT governance requirements of smartphone security, according to the COBIT 4.1 process requirements.

The model is presented on the following. Along the left are the measurable components in the separate IT categories. The maturity measurement scale to the right is adopted from the COBIT 4.1 framework maturity scale. On the far right a target column appears in which the target maturity can be placed.

In order to ensure the solution satisfies smartphone security governance, the items from the primary data collected, are incorporated into each of the categories. The items added are comprised of responses from the primary data collected. These items were also categorised under one of the IT resource categories of COBIT 4.1. The application category now contains two sub-categories; the other three categories now each contain five sub-categories. This provides a comprehensive smartphone security maturity assessment across each of the IT resource categories of the COBIT 4.1 framework.

Category	Sub-category	Maturity Measurement						
		Non-Existent	Initial / Ad Hoc	Repeatable but Intuitive	Defined Process	Managed and Measurable	Optimised	TARGET
Applications	Mobile application security *Mobile application security policies defined*	0	1	2	3	4	5	
	System ownership *Smartphone application owners identified*	0	1	2	3	4	5	
Applications maturity = (Sum of applications sub-categories) / 2		Maturity level (0 – 5) :						
Information	Authentication *Smartphone authentication policies defined*	0	1	2	3	4	5	
	Removable media *Smartphone removable media security policies defined*	0	1	2	3	4	5	
	Ownership *Smartphone information ownership awareness programmes implemented*	0	1	2	3	4	5	
	Restoration and continuity *Smartphone restoration and continuity plans defined*	0	1	2	3	4	5	
	Backup policy and scheme *Smartphone data backup policy and scheme defined*	0	1	2	3	4	5	
Information maturity = (Sum of information sub-categories) / 5		Maturity level (0 – 5) :						
Infrastructure	Configuration *Smartphone configuration policies defined*	0	1	2	3	4	5	
	Communication *Smartphone recommended communication polices defined*	0	1	2	3	4	5	
	Physical threat *Smartphone physical threat analysis performed*	0	1	2	3	4	5	
	System ownership *Smartphone system ownership (infrastructure) is defined*	0	1	2	3	4	5	
	Supplier & Service delivery management *Smartphone supplier and service delivery polices defined*	0	1	2	3	4	5	
Infrastructure maturity = (Sum of infrastructure sub-categories) / 5		Maturity level (0 – 5) :						
People	Users *User awareness programmes implemented for smartphone security*	0	1	2	3	4	5	
	Risk awareness control framework *Risk awareness is defined through a smartphone security control framework*	0	1	2	3	4	5	
	Multi-level strategy awareness *Business and functional smartphone strategies defined*	0	1	2	3	4	5	
	Rights and Privileges *Smartphone user rights and privileges defined*	0	1	2	3	4	5	
	Governance Report *A periodic governance report provides performance feedback to smartphone users*	0	1	2	3	4	5	
People maturity = (Sum of the people sub-categories) / 5		Maturity level (0 – 5) :						
Overall organisational smartphone security maturity **(Sum of the categories) / 4**		Maturity level (0 – 5) :						

Figure 2 - Smartphone security maturity model

The model is designed for generic use across all types of software consultancies. For each software consultancy, the environment within which they operate is likely to be very different. For this reason, the model allows for a target maturity to be defined according to the specific requirements and priorities of a particular organisation. A committee of senior managers and security officers should be assembled to define the target maturity level for the specific organisation utilising the model.

5. Conclusion

Ensuring that smartphones are not a weak link in the chain of security in an organisation, is paramount to the protection of the information at that organisation. Regular assessment of all security components is vital in ensuring an ongoing security solution. Using the model provided by this research project, the smartphone component is capable of active ongoing maturity measurement. Finally, employees, management, clients and customers will only benefit by efforts to improve smartphone security.

Future research could be aimed at providing specific instructions for increasing each of the maturity measurement components. Assessing the maturity performance of relatively new technologies ensures that minimal security impact can be felt by an organisation. Through the work of this research paper, the maturity of smartphone security in software consultancies can be both measured and improved. Software consultancies can now embrace this innovative and exciting technological advancement, without fearing it.

6. References

Botha, R., Furnell, S., & Clarke, N. (2009). From desktop to mobile: Examining the security experience. Computers & Security , 28 (3-4), 130-137.

Clarke, N., & Funrell, S. (2007). Advanced user authentication for mobile devices. Computers and Security , 26 (2), 109-119.

Dunn, D. (2007). Mobility: Securing devices on the run. (P. Watson, E. Feretic, & E. Cone, Eds.) Innovations , 2007 (5), pp. 18-19.

Elgan, M. (2007, March 12). It's time we stopped talking about "smartphones". Retrieved May 05, 2009, from techworld.com: http://www.techworld.com/mobility/features/index.cfm?featureid=3204

Furnell, S., & Thomson, K.-L. (2009). Recognising the varying user acceptance of IT security. Computer Fraud & Security (2), 5-10.

Furnell, S., Jusoh, A., & Katsabas, D. (2006). The challenges of understanding and using security: A survey of end-users. Computers and Security , 25 (1), 27-35.

Gartner. (2009). Gartner Glossary. Retrieved December 7, 2009, from Gartner: http://www.gartner.com/6_help/glossary/GlossaryS.jsp

IT Governance Institute. (2007a). COBIT 4.1 Executive Summary. Rolling Meadows, Illinois, USA.

Johnson, J. (2009). Memory Cards for Your PDA; Expand Your PDA's Storage Potential. Retrieved July 21, 2009, from About.com: http://palmtops.about.com/od/accessoriesperipherials/ss/flashcards.htm

Jürjens, J., Schrek, J., & Bartmann, P. (2008). Model-based Security Analysis for Mobile Communications. International Conference on Software Engineering (pp. 683-692). Leipzig, Germany: Association for Computing Machinery (ACM).

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information systems security policies: a contextual perspective. Computers and Security , 24 (3), 246-260.

Kruger, H. A., & Kearny, W. D. (2008). Consensus ranking – An ICT security awareness case study. Computers and Security , 27 (7-8), 254-159.

Myers, M. D. (1997, May 20). Qualitative Research in Information Systems. Retrieved July 22, 2008, from MISQ Discovery: http://www.misq.org/discovery/MISQD_isworld/

Olzak, T. (2006, April). Strengthen Security with an Effective Security Awareness Program. Retrieved February 15, 2009, from Adventuresinsecurity.com: http://adventuresinsecurity.com/Papers/Build_a_Security_Awareness_Program.pdf

Standards South Africa. (2005). SANS 17799:2005. Pretoria: Standards South Africa.

Stephen, L. (1868). Cornhill Magazine (Vol. XVII). London: Smith, Elder & Co.

Tellis, W. (1997). Introduction to case study. The Qualitative Report , 3 (2), 1.