International Journal of Cyber-Security and Digital Forensics (IJCSDF) 2(1): 36-47
The Society of Digital Information and Wireless Communications, 2013 (ISSN: 2305-0012)

A FRAMEWORK FOR GOOD CORPORATE GOVERNANCE AND ORGANISATIONAL LEARNING – AN EMPIRICAL STUDY

WD Kearney, HA Kruger
School of Computer, Statistical and Mathematical Sciences
North-West University, Private Bag X6001, Potchefstroom, 2520
South Africa
Kearneys@iinet.net.au, Hennie.Kruger@nwu.ac.za,

Abstract. The importance of applying good governance principles has grown over the past decade and many studies have been performed to investigate the role and impact of such principles. One of the difficulties in the governance arena is to provide sufficient empirical evidence that good corporate governance and good governance of information technology is beneficial. This paper describes a framework, based on a value-focused approach, which is used to identify unique dimensions for evaluation in a large organisation. Following the evaluation a practical phishing experiment was used to show how a learning process can be initiated through security incidents and how organisational learning can be used to focus on the improvement of specific governance areas.

Keywords: Corporate governance, Governance of Information Technology, Value-focused approach, Phishing, Social engineering, Security awareness, Organisational learning.

1. INTRODUCTION AND BACKGROUND

It is often stated that information and information technology are key assets in many organisations and that it is used to drive business processes [1]. Information technology has become intrinsic to business operations and inadequate systems can hinder the performance and competitiveness of organisations and expose them to the risk of not complying with legislation [2]. It makes therefore sense to have proper governance principles in place that would apply firstly, to corporate governance and, second, to appropriate information technology governance principles which is a subset of corporate governance.

Corporate governance has become a topic that has been researched increasingly in the last decade [3]. Many definitions for corporate governance exist but in its simplest form it refers to the set of processes, customs, policies, laws and institutions affecting the way a corporation is directed, administered or controlled [4]. There are a number of standards and frameworks that define, describe and recommend the application of good corporate governance, all with the same objective of directing and controlling organisations to conduct business in such a way that it is beneficial to all parties involved. A number of common elements that underlie good corporate governance can be found within these frameworks and standards. Examples of such standards are the King III report [5], the Guidelines on Corporate Governance published by the Organisation for Economic Co-operation and Development (OECD) [6] and the Corporate Governance Principles and Recommendations issued by the Australian Securities Exchange (ASX) Corporate Governance Council [7].

There is a general lack of sufficient empirical evidence that good corporate governance pays. The core of this problem lies in the question on what and how to measure the success or impact of applying good corporate governance principles. A number of research studies to address these questions have been completed and some of the studies include the following. Bhagat and Bolton [8] performed a comprehensive study to analyse the relation between corporate governance and performance while Kelton and Yang [9] studied the impact of corporate governance on Internet financial reporting. Other researchers, who have studied the topic, or parts of it, include Plant [10] and Abdo and Fischer [11].

To address the importance of good corporate governance principles and how it may be

evaluated, this paper reports on a project that was initiated at a large geographically dispersed utility to investigate the feasibility of developing a framework to identify key dimensions that are specific to the company. The technique used to identify the dimensions was based on a value-focused approach [12] which allows for participation from stakeholders and helping to align dimensions in accordance with stakeholders' values. As corporate governance for information technology forms an integral part of corporate governance, it was decided to focus on the identification of key dimensions within the corporate governance arena which will then also cover information technology governance. The organisation in question is a large multi-billion dollar entity with over 3500 IT users and supply essential services to over 2 million customers.

In an effort to also respond to those dimensions that are perceived to be on an inadequate level, one of the identified dimensions *Risk Management* was chosen for further analysis. The objective was to show how a security incident such as a phishing scam may lead to organisational learning and ultimately lower some of the risks associated with the *Risk Management* dimension. This evaluation phase is important as it is imperative to ensure that there are proper security metrics and methodologies in place which will eventually lead to the achievement of specific security control objectives [13]. It is also important to try and quantify the measures for information security [14]. The choice of the *Risk Management* dimension can further be justified from the literature. Tamjidyamcholo and Al-Dabbagh [15] argue that the core of information security lies in risk management. According to them there is also a lack of details in the literature on how to reduce risk, especially in instances where uncertainty plays a role.

Van Niekerk and Von Solms [16] stated that organisational learning theories deal with the idea of how organisations learn and adapting their behaviour. One of the definitions for organisational learning is formulated as follows. Organisational learning occurs when individuals within an organisation experience a problematic situation and enquire into it on the organisational behalf [17]. The two main types of learning that generally occur are called single-loop and double-loop learning. Single-loop learning occurs when errors are detected and corrected and organisations continue with the present status quo without modifying present policies and goals while double-loop learning challenges, and possibly makes changes to the status quo and the existing assumptions and conditions [18]. Examples of researchers who performed studies related to information technology and organisational learning include Ahmat *et al* [19] and Van Niekerk and Von Solms [16].

In order to create an opportunity for organisational learning a practical phishing exercise was conducted. The basic idea of phishing is when someone attempts to fraudulently acquire sensitive information from a victim by impersonating a trustworthy entity [20]. The use of practical tests seems to be a popular and effective way of making people aware of the dangers of phishing. Examples of such studies include Dodge *et al* [21] who performed a practical phishing experiment involving students from the United States Military Academy, Jagatic *et al* [20] performed a study at the Indiana University, Steyn *et al* [22] conducted a practical experiment in South Africa and Hasle *et al* [23] a study in Norway.

The remainder of this paper is organised as follows. Section 2 describes the methodology used for the different phases of the exercise while Section 3 presents the results. Section 4 concludes the paper with some general comments.

2. METHODOLOGY

The study comprises of three main steps. First, a value-focused approach was followed to identify the different dimensions of corporate governance; secondly, a survey was conducted to evaluate the identified dimensions; and finally, a practical phishing exercise was conducted to show how organisational learning can take place from security incidents which may improve specific corporate governance dimensions.

2.1 Value-focused Approach

Value-focused thinking is a three step decision technique suggested by Keeney [12]. The approach is concerned with what is important and how to achieve it [24]. The first step involves in-depth interviews with stakeholders with the objective of eliciting values that these persons or groups of persons might have within the decision context. The result is then a list of individual wishes or values. In step two, the values are converted into a common format which is termed an objective. According to Keeney [12] an objective is characterised by an object and a direction of preference. In the third and last step a means-ends network of objectives is established. Objectives are first classified as either a fundamental or means objective and then interrelationships and possible cause-effect relationships are generated. To classify an objective as a fundamental or means objective, Keeney suggested the use of a "why is this important" test. Each objective is tested against this question and if the answer suggests another objective, then it is classified as a means objective. Fundamental objectives are essential reasons for the problem and are not used to achieve any other objectives. The complete process and steps are schematically summarised in figure 1.

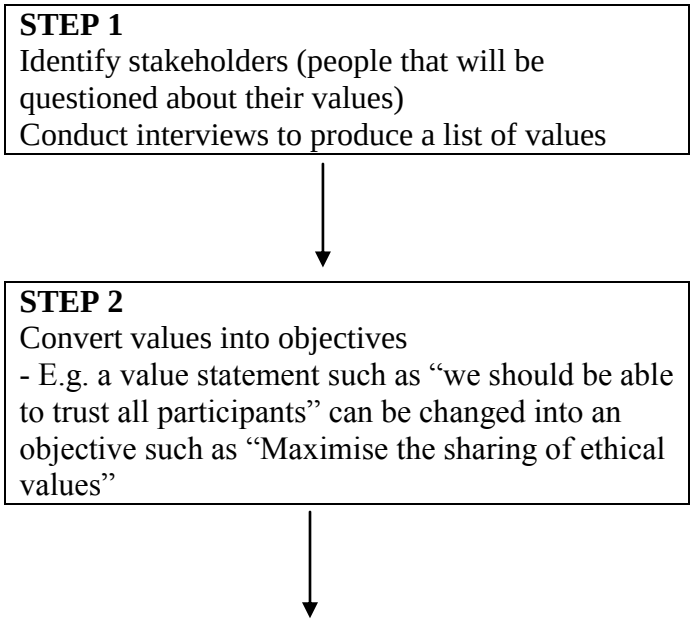

Figure 1 – Value-focused thinking process

To ensure that meaningful interviews (step 1) are conducted and that the wishes, concerns, problems and values of stakeholders are identified, a discussion document was prepared that was used during the interviews. The document contained four broad and open questions that was compiled according to the techniques for the identification of objectives suggested by Keeney. The four questions, used as discussion points, were the following.

1. What would you regard as important aspects in good corporate governance?

The purpose of this question was to encourage stakeholders to discuss their goals and to determine strategic and generic objectives. Examples of some of the answers received include building trust with partners, risks that are well managed, proper structures and systems in place etc.

2. What would you do or implement to ensure that the application of corporate governance principles is effective?

The second discussion point assisted mainly with the development of a wish list and the identification of alternatives. The wish list included answers such as proper contracts and documentation, monitoring systems, capacity to respond to changes etc.

3. What are your current concerns regarding the effective application of good corporate governance principles?

It is often useful to identify shortcomings and problems when trying to determine and describe objectives. The goal of this discussion point was to

assist with this identification, for example, a concern such as "a mismatch between our requirements and what our business partners can provide" may indicate that appropriate structures are essential to ensure that business objectives are achieved.

4. If you have to evaluate the effectiveness of the application of corporate governance principles, how would you do it and how would you know that it is acceptable?

The aim of this point was to try and quantify objectives. Answers ranged from the use of audit reports to measuring against contractual obligations to monitoring financial indicators.

Some researchers prefer to make use of questionnaires to gather information but in this study it was decided to follow a similar interview process as the one used by Dhillon and Torkzadeh [25] and Sheng, *et al* [24] who evaluated the strategic implications of mobile technology using a value-focused approach. Seven senior staff members (ranging from managers to directors) were interviewed using the four discussion points as a basis. This sample size was determined by a "saturation point" which is a standard stopping rule for qualitative research. Glaser and Strauss [26] used the term "theoretical saturation" which means that no additional data is found by the researcher for a specific category in a study. It is off course true that one would never know if the next interviewee would be able to provide new information (which is also true in the case of questionnaires). Statistically speaking it might also be argued that the sample size is not sufficient. It was however decided to keep to the generally accepted qualitative procedure utilizing the saturation point stopping rule. The interviews lasted for approximately 30-60 minutes and were recorded together with notes taken during the interviews.

2.2 Survey To Evaluate Dimensions

Following the identification of the different dimensions, a survey was conducted to determine the level of compliance. A questionnaire, based on the different means objectives, was developed to obtain respondents' views. A total of 20 questions were formulated in the form of statements that had to be evaluated on a scale of 1 to 10. Some of the statements were formulated in a subjective manner to gauge perceptions while others were more of an objective nature to determine whether certain matters have been implemented or exist.

One of the main objectives identified (see section 3.1 for details) was *Risk Management*. Figure 2 presents two example questions in the form of statements for this objective. The first question is an example of an objective question to determine if something has been implemented while the second question has a subjective nature intended to measure a perception.

The application of the questionnaire was structured in such a way that a number of opportunities to benefit from the process were possible, for example measuring and reporting in a drilled down fashion, the use of importance weights, sensitivity analysis etc. Questionnaire results were processed in a spreadsheet application and output was presented in the form of various graphs (see section 3.2) and tables describing the different evaluations.

1. The company has a fully effective documented risk register for its operations and projects
2. The company has effectively manage risks that may have an impact on its objectives and operations

Figure 2 – Example survey questions

2.3 The Phishing Exercise

The successful implementation of an e-mail phishing exercise is dependent on how well certain issues, associated with the exercise, are considered. In this study general as well as specific considerations had to be taken into account. The general considerations are concerned with those issues that may have an impact on the exercise as a whole and include a range of issues such as the determination and definition of an objective; getting ethical clearance and top management

approval; the timing of the exercise; maintaining the privacy of respondents; the selection of a random and representative sample of respondents; measurements to ensure that no information was disclosed prior to the exercise; and, a debriefing exercise following the test.

The specific considerations deal with aspects specific to the enterprise where the study was conducted. Some of the aspects included no reference to any specific IT, security or internal audit staff as this may compromise the trust between users and staff. Steps also had to be taken to ensure that the enterprise's anti-phishing tools and spam filters do not identify the message as spam or a phishing scam, and the Service Centre had to be provided with a predetermined response should there be any queries from users. Provision was also made for respondents who reply directly to the phishing e-mail. Some of the technical considerations include the deletion of duplicate records (if a user responds more than once) and also a check to see whether the correct usernames were supplied (password were requested but not recorded). The key issue was the construction of an appropriate e-mail message. The message had to be concise, credible and at the same time be enticing in order for participants to react.

To ensure that the phishing e-mail message complies with all the necessary requirements, it was decided to make use of certain emotional exploits [27]. The emotional exploits include legitimacy (when a user is made to believe that the source of the e-mail message is legitimate), authority (people tend to comply with instructions or requests issued by someone with authority), scarcity (when users believe that the time to react is limited) and conformity (users who believe that other fellow-employees have already reacted to a request are inclined to also comply with the request).

Figure 3 shows how the e-mail was constructed and the clues provided to alert users that the message was likely not to be legitimate. The real name of the organisation has been changed in figure 3.

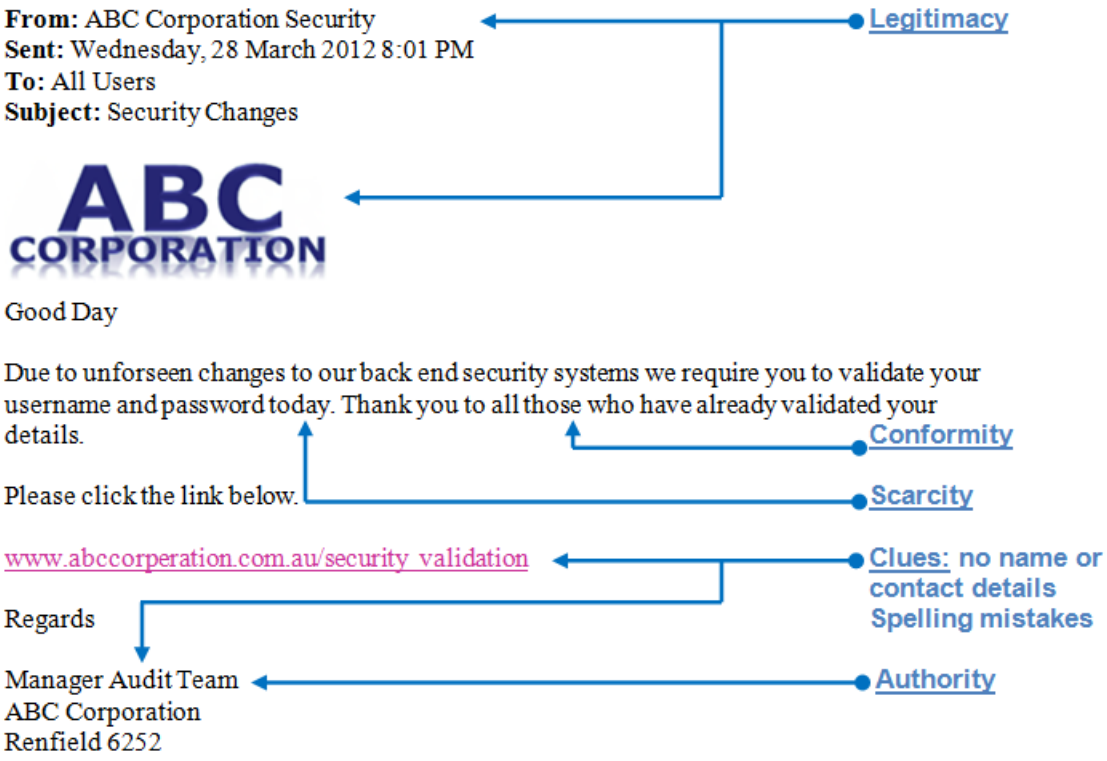

Figure 3 – Phishing e-mail message

The e-mail message (figure 3) was first sent to a small group of 10 employees to test whether all technical aspects are functioning correctly and also to get feedback on possible improvements. After

some minor changes were made it was decided to go ahead and implement the phishing test.

The phishing e-mail message was sent to all employees at 8:00pm on a weekday night. The organisation is a 24-hour operation with activities taking place on a continuous basis. This was done to ensure that night workers are included in the test and also to guarantee that day workers receive the message first thing in the morning. As soon as the message was sent out, security personnel were involved and concern was expressed regarding the possibility of an external attack aimed at disrupting essential services. Due to this and the reaction of senior managers, it was decided at 8:30am the next morning to remove the phishing message and to officially end the test. The reasons for withdrawing the phishing e-mail relatively early the next morning were firstly, to prevent large-scale disruptions and secondly, because enough data has been recorded at that stage to draw meaningful conclusions. The data and the experience were sufficient and interesting results were obtained.

3. RESULTS

This section presents the results for the value-focused process, the survey to evaluate the identified dimensions and the phishing exercise used to demonstrate how organisational learning can take place to address the *Risk Management* dimension.

3.1 Results Of The Value-focused Process

Following the value-focused thinking approach as described in section 2.1, a network of objectives was constructed which is presented in figure 4 (on the next page). On the left hand side (in figure 4) are the means objectives that show the concerns, wishes and values of interviewees while the right hand side shows the fundamental objectives.

The fundamental and means objectives on which the means-ends network is based are listed in tables 1 and 2. Table 1 shows the fundamental objectives and the factors describing them while table 2 shows an extract of the aspects that influence some of the means objectives according to the interviewees. A detailed description of these results can also be found in [28].

Table 1 - Fundamental Objectives

1. **Appropriate Board and Management structures are in place**
   - An appropriate alliance structure is in place
   - All arrangements are formalized
2. **Maximize the use of appropriate business practices and ethics**
   - Build trust with partners; have trusted people; openness
3. **Maximize performance management**
   - Strategic risk
   - Project outcomes must be good
4. **Maximize disclosure and transparency**
   - Continuous improvement; standardized frameworks
5. **Maximize risk management**
   - Robust risk management principles
6. **Appropriate legal, regulatory and social environment exists**
   - Regular reviews
   - Policies and procedures to manage compliance

Table 2 - Means Objectives

1. **Maximize understanding of roles, right and obligations**
   - Protect the interest of the organization; define what needs to be achieved
   - Roles and responsibilities must be understood
2. **The most appropriate structure is used to achieve objectives**
   - Number of parties involved should be appropriate; appropriate resources
   - Structure must be accepted and operates well; value for money

.
.

18. **Maximize use of appropriate policies and procedures to manage compliance**
    - Systems and frameworks in place; monitoring – internally e.g. internal audit department
    - Measure against objectives
19. **Maximize internal audit process**
    - Internal mechanisms such as quality control, compliance verification etc.
    - Formal internal audit department exists; regular audit reports

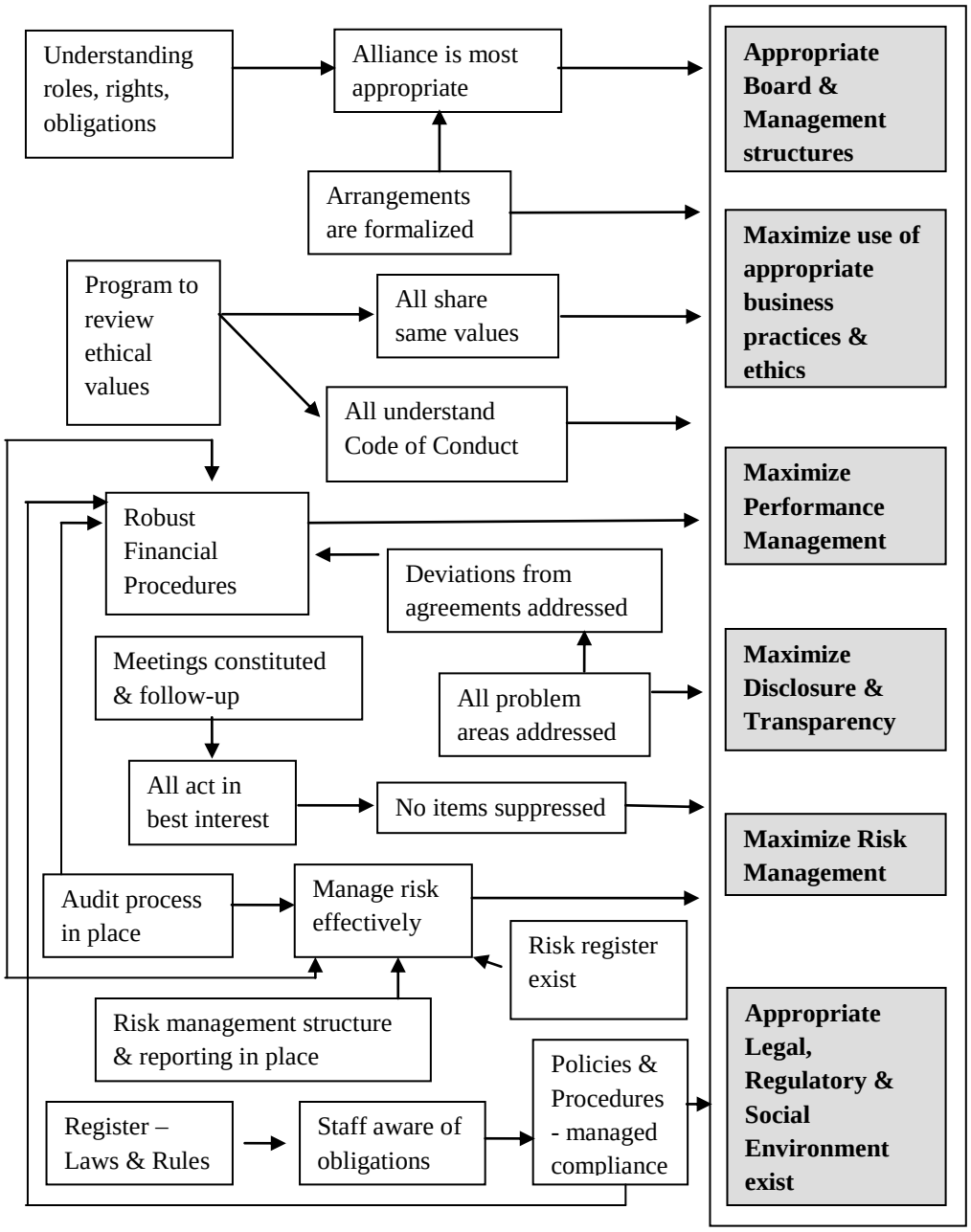

Figure 4 – Means-ends objectives for corporate governance

An analysis of the different means and fundamental objectives resulted in the six different dimensions as indicated in table 1 and figure 4. These six dimensions are:

- Appropriate board and management structures;
- Maximize the use of appropriate business practices and ethics;
- Maximize performance management;
- Maximize disclosure and transparency;
- Maximize risk management; and
- Appropriate legal, regulatory and social environment exist.

To verify whether the six fundamental objectives (or dimensions) identified are in line with generally accepted corporate governance principles, it was decided to compare them to two sets of published principles namely the Corporate

Governance Principles and Recommendations issued by the Australian Securities Exchange (ASX) Corporate Governance Council [7], and the AS8015-2005: Australian Standard for Corporate Governance of Information and Communication Technology [29].

The ASX Corporate Governance Council listed eight corporate governance principles as being necessary to ensure good corporate governance in enterprises while the AS8015 standard provides six principles for good governance of ICT. These principles are briefly presented in table 3 along with an indication of how the identified fundamental objectives may be linked to them.

Table 3 – Corporate Governance and ICT Principles

ASX Principles [7]	**Corresponding fundamental objectives identified with value-focused assessment**	**AS8015 Principles for ICT Governance [29]**
1. Lay solid foundations for management and oversight (refers to roles and responsibilities of the board and management)	Appropriate board and management structures are in place	Establish clearly understood responsibilities Plan ICT to best support the organisation
2. Structure the board to add value (refers to composition, size and commitment)	No specific fundamental objective can be mapped to this principle, but it is partially addressed by *Appropriate board and management structures are in place*	
3. Promote ethical and responsible decision making	Maximise the use of appropriate business practices and ethics	Ensure ICT respects human factors
4. Safeguard integrity and financial reporting	Maximise performance management	Acquire ICT validly Ensure that ICT performs well whenever required
5. Make timely and balanced disclosure	Maximise disclosure and transparency	Acquire ICT validly Ensure ICT conforms with formal rules
6. Respect the rights of shareholders	No specific fundamental objective can be mapped to this principle, but it is partially addressed by *Maximise the use of appropriate business practices and ethics*	Ensure ICT respects human factors
7. Recognise and manage risk	Maximise risk management	Plan ICT to best support the organisation Ensure that ICT performs well whenever required
8. Remunerate fairly and responsibly	No specific fundamental objective can be mapped to this principle	
Appropriate legal, regulatory and social environment exists. There is no specific principle where this fundamental objective can be linked to. It does however cover certain aspects under the principle *Promote ethical and responsible decision making*.		

It is clear from table 3 that the value-focused assessment produced fundamental objectives that are in line with accepted corporate governance principles. Only one of the principles (Remunerate fairly and responsibly) was not directly covered by the identified objectives while there was also only one fundamental objective that could not directly be linked to any of the eight principles (Appropriate legal, regulatory and social environment exists). This objective, however, covers certain aspects in some of the other principles.

3.2 Results Of The Survey

A total of 31 staff members were identified as respondents to evaluate the identified dimensions. This choice of participants was based on their level of seniority, their knowledge of corporate governance principles, and a request from senior management to include them in the exercise. Figure 5 shows a graph with the overall evaluation of the six dimensions. A formal 5-level scale (not presented here) was constructed to interpret the results on the graph. The scale ranges from no evidence that governance principles are applied at the lower end, to significant investment in time and resources to apply governance principles at the other end.

Applying the scale and from figure 5 it can be seen that the two principles *Disclosure and Transparency* and *Performance Management* are, on average, currently performing satisfactorily as evaluated by the participants. The remaining four governance principles were all, on average, evaluated as principles that are applied to a certain degree but with some room for improvement. The *Risk Management* dimension was chosen for further investigation to see if a practical security incident can initiate an organisational learning process that can contribute to the risk management process.

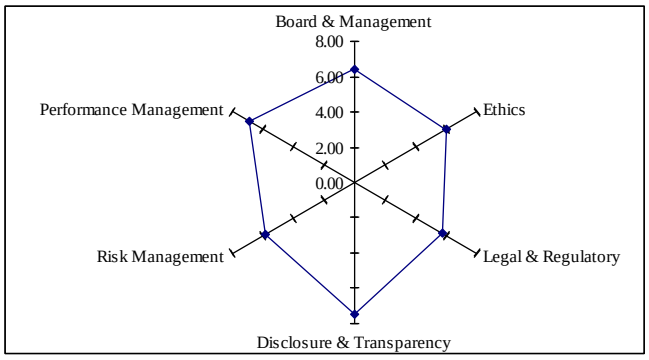

Figure 5 – Overall evaluation of principles

3.3 Organisational Learning Results

The data recorded from the phishing exercise include the employee name, department where the person is working and the username. Passwords were also requested but not recorded due to privacy considerations. As part of the exercise, passwords were validated but only the result was recorded in a simple yes/no format. Appropriate safeguards to ensure privacy were put in place. The recorded employee names were purely recorded for statistical purposes and nowhere during reporting were specific names linked to responses.

During the test 280 users responded to the phishing message of whom 231 (83%) entered their usernames and passwords on the webpage. Although there were approximately 1700 active users logged on during the test, it would be incorrect to assume that all of those who did not respond acted in a positive way. Reasons for this may be the fact that many people do not respond immediately to e-mail messages, some users may have left their workstations logged on during the night while not there, some users may have been engaged in other tasks and simply did not check their mail inboxes, etc. A much more significant analysis was to link the 280 users who responded, to an information security course that all staff members are required to complete and which would have provided them with basic security information on how to react to possible phishing scams. An unexpected 69% of those users who entered their passwords did complete the security training in the past. This also implies that almost one third (31%) never completed the security training course. These basic results indicate that there are at least two points of concern. Firstly, the high number of users who responded in a negative way despite their security training and secondly, the relatively high number of users that never completed the information security course.

An analysis of responses (percentages) per experience (years of service) category for those who entered their usernames and passwords shows that those employees with less experience at the organisation - and therefore less exposure to its security practices and policies - are more inclined to give away personal details. More than a third (35%) of those who entered their usernames and passwords have less than 5 years experience with more than half (52%) less than 10 years. This analysis is shown graphically in figure 6.

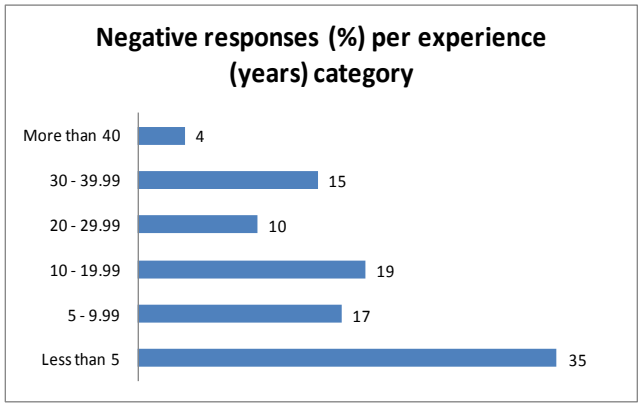

Figure 6 – Responses per experience category

Apart from these results the focus was more directed at possible organisational learning opportunities that may contribute to the Risk Management corporate governance principle. As explained earlier, organisational learning involves the adjustment of actions based on an experience. These adjustments, or learning, can then be categorised as single or double-loop learning. The results from this study have shown that the phishing experiment offers the ideal opportunity for learning and that both single and double-loop learning has taken place.

Single-loop learning took place in the form of small changes in making staff aware of the risks and consequences of phishing scams. Instructions concerning basic acceptable behaviour related to suspicious e-mail messages were issued in the form of e-mail messages and the company's weekly in-house bulletin.

In addition, a corporate blog was employed to assist in making staff aware of risks involved in social engineering activities. There has been a high growth in the use of corporate blogs over the last few years and at the corporation where the testing was done, this is no different. The CEO makes use of a blog to communicate a variety of messages into the organisation. Whilst email communication is more direct, the blog is often seen to offer a more open and personable medium of communication. These corporate blogging initiatives are interactive and cheap to deploy which does make them a very attractive form of communication.

In ongoing discussions regarding the learning from the exercise, the CEO has indicated that this medium will be used to educate and make staff members aware of the dangers of "phishing" and other social engineering scenarios. As the initial email phishing exercise created a level of angst amongst certain elements within the organisation, care will need to be taken on the content and timing of the message. The level of interaction and any feedback received will be monitored and evaluated. This evaluation, which may eventually become a double-loop learning activity, will form part of the broader study and is not a part of this paper.

The single-loop learning activities mentioned above did not change the status quo of any process but were quick and effective corrective measures to address a specific problem area. There were, however, other issues that needed a more comprehensive investigation that may lead to a change in policies and procedures. These double-loop learning issues include the following.

- All staff members are required to complete an information security course which will equip them with basic security knowledge for different security situations including phishing scams. An analysis of the phishing results showed that not all staff has completed the course. More importantly, a relatively large number of those who have completed the course had given their passwords away. An assessment of the course content and possible controls to ensure that everybody completes the course is planned. This may lead to a change in the current security policy on issues pertaining to basic security training.

- Another issue, planned for the future, which was highlighted during the phishing exercise relates to the gap between the different security views and expectations of managers and users. This gap is sometimes referred to as the information security digital divide between managers and users [30] and may lead to unrealistic security assumptions and management strategies that are not aligned with the dynamics of the user environment.

Basic problems were immediately corrected through an easy and uncomplicated single-loop learning approach while double-loop learning issues provided an opportunity for the organisation to adapt and adjust some of their information strategies. To adapt and improve information security strategies implies a definite contribution to the important corporate governance principle concerned with risk management and it therefore seems permissible to draw the conclusion that the practical security exercise has created opportunities for organisational learning which in turn will contribute to the management of risk in general.

4. CONCLUSION

Interest in corporate and information technology governance has grown tremendously in the past decade. It has become increasingly important to ensure that businesses align their information technology leadership, direction and strategies with the rest of their business objectives. One of the challenges in the field of corporate governance is to provide empirical evidence that the application of good corporate governance is beneficial. This paper reported on the development and application of a process to evaluate good corporate governance principles. A value-focused approach was followed to determine important factors specific to the company reviewed. This resulted in six different factors that were in line with those suggested in the literature on corporate governance and governance for information technology. The framework was tested and results have shown that certain areas, e.g. risk management, in the company under review, can be improved. A successful phishing exercise was then conducted to show how a security incident can create opportunities for organisational learning which will benefit the risk management dimension of information technology governance.

REFERENCES

1. Von Solms, R., Von Solms, S.H.: Information security governance: Due care. Computers and Security 25, pp. 494--497 (2006).
2. ISO/IEC standard for corporate governance of information technology). http://www.iso.org/iso/ (2008).
3. Gillan, S.L.: Recent developments in Corporate Governance: An overview. Journal of Corporate Finance 12, pp. 381--402 (2006).
4. Wikipedia. http://en.wikipedia.org/wiki/Corporate-Governance (2008).
5. King III Report on Corporate Governance. The Institute of Directors. http://www.iodsa.co.za (2009).
6. Organisation for Economic Co-operation and Development. OECD Guidelines on Corporate Governance of State-owned Enterprises (2005).
7. Australian Securities Exchange (ASX). Corporate governance principles and recommendations. 2nd edition. ASX Corporate Governance Council (2007).
8. Bhagat, S., Bolton, B.: Corporate governance and firm performance. Journal of Computer Finance 14, pp. 257--273 (2008).
9. Kelton, A.S, Yang, Y.: The impact of corporate governance on Internet financial reporting. Journal of Accounting and Public Policy 27, pp. 62--87 (2008).
10. Plant, K.: Towards the development of a framework for ethics audits: an internal auditing perspective. SA Journal of Accountability and Auditing research 8, pp. 15--26 (2008).
11. Abdo, A., Fisher, G.: The impact of reported corporate governance disclosure on financial performance of companies listed on the JSE. Investment Analysts Journal 66, pp. 43--56 (2007).
12. Keeney, R.L.: Creativity in decision-making with value-focused thinking. Sloan Management Review Summer, pp. 33--41 (1994).
13. Azuwa, M.P., Ahmad, R., Sahib, S., Shamsuddin, S.: Technical security metrics in compliance with ISO/IEC 27001 Standard. International journal of Cyber-Security and Digital Forensics (IJCSDF). The Society of Digital Information and Wireless Communications 1(4), pp. 280-288 (2012).
14. Jouini, M., Aissa, A.B., Rabai, L.B.A., Mili, A.: Towards quantitative measures of information security: A cloud computing case study. International journal of Cyber-Security and Digital Forensics (IJCSDF). The Society of Digital Information and Wireless Communications 1(3), pp. 248-262 (2012).
15. Tamjidyamcholo, A., Al-Dabbagh, R.D.: Genetic algorithm approach for risk reduction of information security. International journal of Cyber-Security and Digital Forensics (IJCSDF). The Society of Digital Information and Wireless Communications 1(1), pp. 59-66 (2012).
16. Van Niekerk, J., Von Solms, R.: Organisational learning models for information security. http://icsa.cs.up.za/issa/2004/Proceedings/Full/043.pdf (2004).
17. Argyris, C., Schon, D.: Organisational learning II: Theory, method and practice. Prentice Hall (1996).
18. Kennedy, E.: A critical evaluation of the organisational learning that takes place in a project management

environment. Unpublished M-dissertation, North-West University (2008).
19. Ahmad, A., Hadgkiss, J., Ruighaver, A.B.: Incident response teams – challenges in supporting the organisational security function. Computers and Security 31, pp. 643--652 (2012).
20. Jagatic, T.N., Johnson, N.A., Jakobsson, M., Menezer, F.: Social phishing. Communications of the ACM 50(10), pp. 94--100 (2007).
21. Dodge, R.C., Carver, C., Ferguson, A.J.: Phishing for user security awareness. Computers and Security 26, pp. 73--80 (2007).
22. Steyn, T., Kruger, H.A., Drevin, L.: Identity theft – empirical evidence from a phishing exercise. New approaches for Security, Privacy and Trust in complex environments, IFIP International Federation for Information Processing 232, pp. 193--203 (2007).
23. Hasle, H., Kristiansen, Y., Kintel, K., Snekkenes, E.: Measuring resistance to social engineering. In: Proc. 2005 ISPEC05 first international conference on information security practice and experience, pp. 132--143 (2005).
24. Sheng, H., Fui-Hoon, F., Siau, K.: Strategic implications of mobile technology: A case study using Value-Focused thinking. Journal of Strategic Information Systems 14, pp. 269--290 (2005).
25. Dhillon, G., Torkzadeh, G.: Value-focused assessment of information system security in organisations. In: Proc. 2001, The 22nd international conference on information systems, pp. 561--565 (2001).
26. Glaser, B.G., Strauss, A.L.: The discovery of grounded theory: strategies for qualitative research, New York (1967).
27. Jansson, K.: A model for cultivating resistance to social engineering attacks. Unpublished M-dissertation, Nelson Mandela Metropolitan University (2011).
28. Kruger, H.A., Kearney, W.D.: Effective corporate governance: A case study using a value-focused approach, In: Proc. 2009 SAIMS 21st Conference of the South African Institute for Management Scientists, on CD (2009).
29. AS8015-2005 – Australian Standard for Corporate Governance of Information and Communication Technology (ICT). http://www.ramin.com.au/it-governance/as8015.html (2008).
30. Albrechtsen, E., Hovden, J.: The information security digital divide between information security managers and users. Computers and Security 28, pp. 476--490 (2009).