TABLE OF CONTENTS

EXECUTIVE SUMMARY

"The ultimate security is your understanding of reality." [1]

Organisations are being placed under increased pressure by means of new laws, regulations and standards, to ensure that adequate information security exists within the organisation. The King II report introduced corporate South Africa to the concept of information security in 2002. In the same year the Electronic Communications and Transactions Act 25 of 2002 addressed certain technical information security issues such as digital signatures, authentication, and cryptography. Therefor, South Africa is increasingly focussing its attention on information security. This trend is in line with the approach taken by the rest of the international community, who are giving serious consideration to information security and the governance thereof.

As organisations are waking up to the benefits offered by the digital world, information security governance is emerging as a business issue pivotal within the e-commerce environment. Most organisations make use of electronic communications systems such as e-mail, faxes, and the world-wide-web when performing their day-to-day business activities. However, all electronic transactions and communications inevitably involve information being used in one form or another. It may therefor be observed that information permeates every aspect of the business world. Consequently, the need exists to have information security governance in place to ensure that information security prevails. However, questions relating to: which organisation must deploy information security governance, why the organisation should concern itself with this discipline, how the organisation should go about implementing information security governance, and what consequences will ensue if the organisation fails to comply with this discipline, are

1 Judd "Famous quotes" (last visited 1 October 2003) http://www.great-quotes.com 1.

in dispute. Uncertainty surrounding the answers to these questions contribute to the reluctance and skepticism with which this discipline is approached.

This dissertation evolves around the legal implications of information security governance by establishing who is responsible for ensuring compliance with this discipline, illustrating the value to be derived from information security governance, the methodology of applying information security governance, and liability for non-compliance with this discipline, ultimately providing the reader with certainty and clarity regarding the above mentioned questions, while simultaneously enabling the reader to gain a better understanding and appreciation for the discipline information security governance.

The discussion hereafter provides those who should be concerned with information security governance with practical, pragmatic advice and recommendations on:

(i) The legal obligation to apply information security;

(ii) Liability for failed information security;

(iii) Guidelines on how to implement information security; and

(iv) A due diligence assessment model against which those responsible for the governance and management of the organisation may benchmark their information security efforts.

Guide to Information Security Governance Compliance

In order to fully comprehend and understand, not only the legal implication of information security governance, but also what the discipline information security governance itself entails, due consideration must be given to the following issues:

1. Managing Information Security

Information security should be a critical business concern for all organisations venturing into cyberspace. This topic is however of immediate concern for public and private companies as newly enacted legislation and regulations make the implementation and execution of information security within these two companies mandatory.

Furthermore, it should be borne in mind that within the organisation itself different role-players will be assigned different degrees of responsibility for information security. Therefor, there will be a direct correlation between the position/office a person holds, and his responsibility for information security. Two main categories of role-players may be identified, namely:

(i) Primary role-players:

- Primary role-players will comprise of the board of directors and top management;
- Although it is not expected of these role-players to be involved in the development and implementation of information security on a daily basis, they will be held responsible for failed information security;
- Therefor, ultimate responsibility for information security resides in the board of directors, with top management in turn being answerable to the board on this issue.

(ii) Secondary role-players:

- These role-players are responsible for the development and implementation of information security within the organisation;
- Secondary role-players include, but are not limited to IT Service Manager; Security Coordinator; Department Managers; Network and Application Administrators; IT Service Level Manager; Risk and Security Manager; Business Information

Manager; Procurement Manager; Account Managers; Auditors; and Consultants.

Therefor, information security governance will be concerned with how the board of directors and top management consider, apply and administer information security in their supervision, monitoring, control and direction of the organisation.

2. Legal Obligation to Apply Information Security

Organisations, in the form of public and private companies, are being places under increased pressure by means of new laws, regulations and standards to ensure that the organisation complies with its information security obligations. These obligations may originate from various sources, such as –

(i) Common law:

- The common law places the primary role players, and specifically the board of directors, under a fiduciary duty of care and skill. This duty is the most prevalent within the information security governance domain, as this would be the ground on which a stakeholder will be able to hold a director personally liable should information security fail;
- Within the information security governance domain this duty would require of the board to take reasonable steps to secure the information assets of the organisation.

(ii) Statutory and regulatory obligations:

- The newly-enacted Electronic Communications and Transaction Act 25 of 2002 contains specific provisions pertaining to technical information security;
- The King II report places the ultimate responsibility for information security firmly in the hands of the board of directors. Although the board is allowed to delegate certain activities associated with the development and implementation of information security within the

organisation to designated employees, they are not allowed to abdicate their responsibility therefor;

- Furthermore, the JSE New Listing Requirements require of all listed companies to disclose the extend to which they comply with King II, and for the first time ever makes provision for directors to be held jointly and severally liable for failure to comply with the listing requirements, therefor with King II. A director that contravenes this provision may face a penalty of R1 000 000.

(iii) Contractual obligations;

(iv) Self-imposed obligations; and

(v) International legislation that may impact on information security, having specific regard to e-commerce:

- Because of the fact that cyberspace is a borderless, faceless environment, organisations who wish to do business in this realm will have to give due consideration to internationally accepted standards, regulations and best practices concerning information security. If they fail to do so organisations might find themselves in a situation where a country refuses to do business with them because they have inadequate information security practices and/or procedures in place.
- Organisations will therefor have to investigate, consider, and in certain instances comply with the following:
  - Organisation for Economic Co-operation and Development (OECD) security guidelines;
  - European Union (EU) security directives;
  - Information security standards and best practices (ISO 17799 and COBIT); and
  - Enacted information security legislation and regulations of the specific country with which they want to do business.

3. Defining the Value of Information Security

Various benefits may be derived from information security governance. These range from enhanced economic performance, substantially boosted productivity growth, to adequately protecting the information assets of the organisation, and ensuring the continued viability and prosperity of the organisation.

Notwithstanding this, arguably the most important benefit derived from effective information security governance is to be found in this discipline's ability to provide the organisation, as well as those responsible for the governance and management of the organisation, with a mechanism to escape legal liability for failed information security. Therefor, if a director can show the existence and execution of an effective information security governance discipline within his organisation, he would have gone a long way in convincing the court that he has fulfilled his duty of due diligence. This would hold true irrespective of the type or nature of the security breach/incident that may occur or has occurred in the past.

4. Liability for Failed Information Security

The organisation, as well as those people entrusted with the governance and management of the organisation, have a legal duty to secure the organisation's information assets. This duty is owed to stakeholders. Stakeholders include –

(i) Shareholders;

(ii) Parties who contract with the company; and

(iii) Parties who have a non-contractual nexus with the company (eg, the state).

The burden of proof will rest on the stakeholder (plaintiff) to proof that a director (defendant) did not fulfill his duty of care and skill, by indicating:

(i) That the director did in fact owe a duty of care to the stakeholder;

(ii) That the director breached this duty;

(iii) That the stakeholder suffered a legally recognizable injury; and

(iv) That the director's breach caused the stakeholder's injury (causation).

The only defense to such an allegation would be to show that the director took reasonable steps to prevent the information security incident/breach from occurring, and that he acted honestly and in the circumstances ought to be excused.

5. Information Security Due Diligence Assessment

Legal compliance with information security

The legal aspects of information security evolves around the following issues: (i) the way in which information is created, processed, stored, transmitted, used and communicated; (ii) who has access to it; (iii) what they will be able to do with it; (iv) how long they will be able to have access; and (v) who has the authority to change access and how.

Consequently, a framework for information security governance has to be established that will satisfy the applicable legal requirements. The following four-pillar framework will allow the board to address key elements of their duty of due diligence. In order to evaluate if a director fulfilled this duty, information security governance due diligence assessment may be performed. Fulfillment of this duty will result in a tick in every box at the end of each pillar:

(a) Ownership:

Information security governance is a critical board task.

- Ownership of information security governance resides in the board. Although they are allowed to delegate activities associated with the development and implementation of information security governance to designated employees, they are unable to abdicate their ultimate responsibility therefor;

- Establish ownership by allowing the board to nominate a senior individual who must-
    - Stay abreast of obligations and responsibilities; and
    - Provide advice on how to comply with legislation and best practices.

☑ Information security governance is the responsibility of the board of directors.

(b) Organisation:

Structure the organisation such that –

- Information security governance is woven into the very fabric of the organisation;
- Collaboration is encouraged between information security specialists and business managers; and
- Information security mission, goals and objectives are aligned with the overall organisational mission, goals and objectives.

  A strong impetus to the business value of information security governance is found in strategic alignment that creates heretofore unheard of synergies between information security, technology and the business. If information security mission, goals and objectives are moving in the same direction as the overall organisational mission, goals and objectives, the true value of information security will be brought to light, namely its inherent function to act as a business supporter, enabler and ultimately transformer.

☑ Information security governance forms an integral part of the overall organisational structure;

☑ A balanced approach between all three components of information security, namely physical, technological and procedural security, is adopted; and

- ☑ Alignment of information security mission, goals and objectives with organisational mission, goals and objectives.

(c) People:

Support appropriate –

- Employee awareness of information security issues through an effective information security awareness and training program. This program must educating employees on why the need for information security exist, what is expected of them, and what sanctions will ensue because of non-compliance;
- Incentive schemes; and
- Performance measurement to develop best practice in information security. Before resources will be allocated to information security efforts, the board of directors will first have to be convinced of the business value thereof. Consequently, the illusive value of information security must be captured by a performance measurement tool such as the balanced scorecard. The value of information security may furthermore be defined by asking the right questions, challenging the answers and measuring the results.

- ☑ Results in a consistent, integrated view across the organisation of the importance of information security;
- ☑ Direct and control information security investments, opportunities, benefits and risks; and
- ☑ Provides a clear view of how much is spend, on what, and measure the return on investment.

(d) Process:

Establish and oversee information security risk management -

- Determining the radius of risk to information security in a specific organisation by following a cyclical risk management process which would encompass both risk assessment and risk mitigation. Risk management must evolve and adapt to the continuous changes experienced in the fields of business and technology;
- Determine acceptable level of information risk;
- Agree and implement appropriate safeguards and control measures; and
- Monitor and maintain information security governance within the organisation. The maintenance and monitoring of information security is just as important as implementing it in the first place, it might even be harder to achieve as it requires renewed commitment to information security efforts on a daily basis.

☑ Information security governance ensures that risks are quantified, understood and managed.

From the preceding it should be clear that there exist a plethora of legal implications and considerations directors and top management will have to give regard to when carving out a presence on the Internet. Organisations wishing to do business in the information age do not have the luxury of asking themselves whether or not to deploy on the Internet. The only question that should be asked is how to deploy. Information security now more than ever, permeates every aspect of the business environment, demanding of directors to become knowledgeable and involved in this discipline. Never has the saying “knowledge is power” been truer, as “ultimate security is your understanding of reality”.[2]

The development and implementation of this discipline may be a humbling experience for some, stripping them of all pretence, by requiring of the organisations, as well as those entrusted with the governance of the organisation, to acknowledge and admit that they are vulnerable, and susceptible to attacks. By knowing and acknowledging that you are vulnerable, therein lies the key to effective information security governance.

“Evolve. Connect. Thrive.”

[2] Judd “Famous quotes” (last visited 1 October 2003) http://www.great-quotes.com 1.