available at www.sciencedirect.com

SCIENCE DIRECT®

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Information Security – The Fourth Wave

*Basie von Solms**

University of Johannesburg, Johannesburg, South Africa

ARTICLE INFO

Article history:
Received 20 February 2006
Revised 9 March 2006
Accepted 9 March 2006

Keywords:
Corporate Governance
Information Security
Information Security Management
Information Security Governance
Risk management
Sarbanes–Oxley
Social engineering

ABSTRACT

In a previous article [von Solms, 2000], the development of Information Security up to the year 2000 was characterized as consisting of three waves:

- the technical wave,
- the management wave, and
- the institutional wave.

This paper continues this development of Information Security by characterizing the Fourth Wave – that of Information Security Governance.

1. Introduction

The First Wave was characterized by Information Security being a technical issue, best left to the technical experts. The Second Wave was driven by the realization that Information Security has a strong management dimension, and that aspects like policies and management involvement are very important. The Third Wave consisted of the need to have some form of standardization of Information Security in a company, and aspects like best practices, certification, an Information Security culture and the measurement and monitoring of Information Security became important.

Since the paper (von Solms, 2000) introducing this development cycle for Information Security appeared in Computers and Security, the development of the next wave of Information Security, the Fourth, became very clear and well defined. This wave relates to the development and crucial role of Information Security Governance.

The drivers behind this Fourth Wave are closely related to developments in fields of Corporate Governance and the related legal and regulatory areas. Top management and Boards of Directors felt the heat as they started to become personally accountable for the health (read Information Security) of their IT systems on which they base their planning and decisions.

This paper will discuss this Fourth Wave, and the drivers behind the wave.

In Section 2 we will briefly investigate the development of Corporate Governance, and highlight the relationship with Information Security. Section 3 will discuss the relationship between Corporate Governance and Information Security in more detail, followed by Section 4 investigating the concept of Information Security Governance. After that, in Section 5 we look at some of the drivers behind the Fourth Wave, followed by Section 6 which presents the discussion about some of the consequences of this wave. We conclude with a summary in Section 7.

* Tel.: +27 11 489 2843; fax: +27 11 489 2138.
E-mail address: basie@rau.ac.za
0167-4048/$ – see front matter © 2006 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2006.03.004

2. Corporate Governance and Information Security

Several documents related to Corporate Governance have appeared during the last five years, and the importance of Corporate Governance in general is now established on an international level. Important examples of such documents are the OECD Principles of Corporate Governance (OECD Principles of Corporate Governance, 2004) and the King 2 Report on Corporate Governance (King 2 Report on Corporate Governance, 2002).

The following two quotes come from the OECD document under the section 'Responsibilities of the Board':

> *'[Responsibilities of the Board include] ensuring the integrity of the corporation's accounting and financial reporting systems, including the independent audit, and that appropriate systems of control are in place, in particular, systems for risk management, financial and operational control, and compliance with the law and relevant standards.'*

> *'In order to fulfill their responsibilities, board members should have access to accurate, relevant and timely information.'*

Therefore, although these documents do not necessarily refer to Information Security per se, they do refer to aspects like reporting systems, systems of control, compliance with relevant standards, risk management, accurate, relevant and timely information, internal controls, etc.

Most companies are totally dependent on their IT systems to capture, store, process and distribute company information. As Information Security is and has always been the discipline to mitigate risks impacting on the confidentiality, integrity and availability of a company's IT resources, Information Security is extremely relevant to what is required in such Corporate Governance documents.

Several legal and regulatory developments related to Corporate Governance have further escalated the role and accountability of senior management as far as their Corporate Governance responsibilities are concerned, reaching the agendas of board and other high level meetings. The leading example here is the Sarbanes–Oxley Act (Sarbanes–Oxley, 2002).

This Act requires top management (and the Board) to sign off on the information contained in annual reports.

> '… in this law (Act) there is a provision mandating that CEOs and CFOs attest to their companies' having proper 'internal controls'. It's hard to sign off on the validity of data if the systems maintaining it are not secure. It's the IT systems that keep the books. If systems are not secure, then internal controls are not going to be too good.' (Hurley, 2003)

From the above discussion, it is clear that, although indirectly mentioned, there is a significant relationship between Corporate Governance and Information Security.

3. The relationship between Corporate Governance and Information Security

The important, and interesting, aspect of the relationship between governance and security is the clarity with which this relationship had been expressed in relevant and recent documentation.

The following type of statements has started to appear more regularly, highlighting the integral role of Information Security in Corporate Governance.

> 'Corporate Governance consists of the set of policies and internal controls by which organizations, irrespective of size or form, are directed and managed. Information security governance is a subset of organizations' overall (corporate) governance program.' (Information Security Governance – a call to action).

> '…. boards of directors will increasingly be expected to make information security an intrinsic part of governance, preferably integrated with the processes they have in place to govern IT'. (Information Security Governance: Guidance for Boards of Directors and Executive Management).

What has also emerged is the pivotal role of Information Security as a risk management or risk mitigation discipline. A representative statement in this case is:

> 'An information security programme is a risk mitigation method like other control and governance actions and should therefore clearly fit into overall enterprise governance.' (Information Security Governance: Guidance for Boards of Directors and Executive Management).

This growing realization has established the fact that Information Security Governance has an enterprise wide impact, and that the risks mitigated by an Information Security Governance plan are risks which have an enterprise wide business implication.

Of course, we, as professionals and practitioners in the field of Information Security, had been making these statements for some time, but we never really succeeded in getting the impact we wanted. The wider emphasis on good Corporate Governance has now succeeded to achieve that which we had been preaching for so long.

Let us now have a closer look at precisely what we can understand under the concept of Information Security Governance.

4. Information Security and Information Security Governance

From the previous discussion, and many other references, there can be no doubt that the developments in the field of good Corporate Governance over the last three to four years had escalated the importance of Information Security to higher levels. It is not only the fact that the spotlight was on Information Security which resulted in this, but also the

establishment and growth in maturity of the concept of Information Security Governance.

It became clear that Information Security Governance is more than just Information Security Management. Information Security Governance clearly indicates the significant role of top management and Boards of Directors in the way Information Security is handled in a company.

The following definition tries to reflect this wider meaning of Information Security Governance which flowed from its explicit inclusion as an integral part of good Corporate Governance:

> 'Information Security Governance is an integral part of Corporate Governance, and consists of
>
> - the management and leadership commitment of the Board and Top management towards good information security;
> - the proper organizational structures for enforcing good information security;
> - full user awareness and commitment towards good information security; and
> - the necessary policies, procedures, processes, technologies and compliance enforcement mechanisms
>
> all working together to ensure that the confidentiality, integrity and availability (CIA) of the company's electronic assets (data, information, software, hardware, people etc) are maintained at all times'.

Information Security Governance therefore involves everyone in a company – from the Chairman of the Board right through to the data entry clerk on the shop floor and the driver of the vehicle delivering the products to the customers.

Information Security Governance can be seen as the overall way in which Information Security as a discipline is handled (used) to mitigate IT risks. One of the essential characteristics of Information Security Governance is the fact that it consists of a 'closed' loop.

The loop starts with management's commitment to Information Security by treating it as a strategic aspect pivotal to the existence of the company and being responsible for managing the IT risks of the company. This treatment includes the sanctioning of a Corporate Information Security Policy accepted and signed off by the Board.

This Policy is supported by a suitable organizational structure for Information Security, specifying ownership and responsibilities on all levels. The organizational structure must take the compliance and operational management of Information Security into account (von Solms, 2005). Such ownership and responsibilities are strengthened by the necessary User Awareness programs for all users of IT systems.

The required technology is rolled out and managed, and compliance monitoring is instituted to measure the level of compliance to policies, etc., reflecting the level to which IT risks are managed. The results of such compliance monitoring efforts are then fed back to Top Management to comprehensively inform them about the status of IT risk management. This closes the loop.

Information Security Governance is therefore the implementation of the full well-known Plan–Do–Control–Measure – Report loop.

Let us now investigate some of the drivers behind this Fourth Wave in more detail.

5. Drivers behind the Fourth Wave

As discussed above, some of the major drivers behind this Fourth Wave are definitely the bigger emphasis on good Corporate Governance and the supporting legal and regulatory developments in this area.

Taking one step back, we can again reason that the major drivers for this bigger emphasis on good Corporate Governance and the supporting legal and regulatory developments are the risks of committing fraud and misusing financial resources by manipulating the company's electronic data stored on its IT systems.

Therefore, preventing fraud through manipulating electronic company data seems to be the core of this drive. From this core came the relevant regulatory and legal developments, as well as the pressure for good Corporate Governance.

The total integration of IT into the strategic operation of companies over the last few years, and pervasiveness of the use of IT throughout companies and the services they deliver, opened up many opportunities to commit fraud using the company's IT systems, resulting in serious risks.

One of the most serious of these risks is that of social engineering and its relationship to Information Security.

Senior management realized that the human side of using IT systems, by employees, clients and customers, can cause serious risks, not withstanding the amount of money spent on the technical measures. It became clear to them that the Information Security problem cannot be solved by technical means alone, and that strategic decisions on a high level had to be made to ensure that all users are aware of possible risks, and the impact of social engineering in attacking IT systems.

Attempts to use social engineering to commit fraud seem to be rising. It is essential to realize that good Information Security Governance, in the sense discussed above, is essential to addressing this risk.

Again, this has been stated over and over by Information Security practitioners over many years, but the pressure caused by good Corporate Governance allowed the penny to drop on the level we targeted for such a long time.

An important question is, of course, whether this Fourth Wave will be sustainable.

6. Some consequences of the Fourth Wave

As discussed above, the major drivers behind this Fourth Wave are definitely the emphasis on good Corporate Governance and the supporting legal and regulatory developments in this area. For this reason it can be accepted that the Fourth Wave will be sustainable, in the sense that top management will not lose interest – they cannot afford to, because their heads are on the block.

This will give more exposure to Information Security in general, which is what we have hoped for anyway. We will probably find that audit committees become much more sensitive towards Information Security, and we will even see a person or persons on the Board assigned specific

Information Security Governance responsibilities. In many instances, these steps have started already.

The following quote supports the realization mentioned above:

> 'According to the 2005 Global Information Security Workforce Study, sponsored by the International Information Systems Security Certification Consortium, IT security professionals are gaining increased access to corporate boardrooms. More than 70% of those surveyed said they felt they had increased influence on executives in 2005, and even more expect that influence to keep growing.' (Security Log, 2006).

It is, however, crucial to realize that Information Security Governance as introduced by this Fourth Wave, is NOT a technical issue. Although it contains technical issues, other (non-technical) issues like awareness and compliance management – ensuring that the stakeholders conform to all relevant policies, procedures and standards – are core to good Information Security Governance.

As such compliance and risk reporting is core to Information Security Governance, we will therefore see that the Fourth Wave requires more formal reporting tools and mechanisms – ways and means to give Top Management an easily understandable overview of precisely what the IT risks are, and how these risks are being managed over time.

7. Summary

Based on the three waves in the development of Information Security as introduced in other articles (von Solms, 2000), Information Security development is presently in its Fourth Wave.

This wave reflects the development of Information Security Governance as a result of the emphasis on good Corporate Governance.

The Fourth Wave of Information Security can therefore be defined as the process of the explicit inclusion of Information Security as an integral part of good Corporate Governance, and the maturing of the concept of Information Security Governance.

We as Information Security practitioners must use this development to its optimum to ensure the security of IT systems.

REFERENCES

OECD Principles of Corporate Governance, http://www.oecd.org/dataoecd/32/18/31557724.pdf; 2004 [accessed 13.01.2006].

King 2 Report on Corporate Governance, http://www.iodsa.co.za/corporate.htm; 2002 [accessed 13.01.2006].

Sarbanes–Oxley, http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf; 2002.

Hurley E, http://searchsecurity.techtarget.com/originalContent/0, 289142,sid14_gci929451, 00.html; 2003.

Information Security Governance – a call to action, National Cyber Security Summit Task Force, www.cyberpartnership.org/InfoSecGov_04.pdf; 2003.

Information Security Governance: guidance for Boards of Directors and Executive Management. USA: IT Governance Institute, ISBN 1-893209-28-8, www.itgovernance.org.

Security Log. Computerworld, http://www.computerworld.com/securitytopics/security/story/0, 10801, 107706, 00.html?source=NLT_SEC&nid=107706; 2006 [accessed 18.01.2006].

von Solms B. Information security governance. Computers and Security 2005;24:443–7.

von Solms B. Information Security – The Third Wave? Computers and Security 2000;19:615–20.

Prof SH (Basie) von Solms holds a PhD in Computer Science, and is the Head of Department of the Academy for Information Technology at the University of Johannesburg in Johannesburg, South Africa. He has been lecturing in Computer Science and IT related fields since 1970. Prof von Solms specializes in research and consultancy in the area of Information Security. He has written more than 90 papers on this aspect, most of which were published internationally. Prof. S. H. von Solms also supervised more than 15 PhD, students and more than 45 Master students. Prof von Solms is the present Vice-President of IFIP, the International Federation for Information Processing, and the immediate past Chairman of Technical Committee 11 (Information Security), of the IFIP. He is also a member of the General Assembly of IFIP. He has given numerous papers, related to Information Security, at International conferences and is regularly invited to be a member of the Program Committees for international conferences. Prof von Solms has been a consultant to industry on the subject of Information Security for the last 10 years, and received the 2005 ICT Leadership Award from the ICT Industry in SA. He is a Member of the British Computer Society, a Fellow of the Computer Society of South Africa, and a SAATCA Certificated Auditor for ISO 17799, the international Code of Practice for Information Security Management.