CORPORATE OWNERSHIP & CONTROL

Postal Address:

Postal Box 36
Sumy 40014
Ukraine

Tel: +380-542-611025
Fax: +380-542-611025
e-mail: alex_kostyuk@mail.ru
alex_kostyuk@virtusinterpress.org
www.virtusinterpress.org

Journal Corporate Ownership & Control is published four times a year, in September-November, December-February, March-May and June-August, by Publishing House "Virtus Interpress", Kirova Str. 146/1, office 20, Sumy, 40021, Ukraine.

Information for subscribers: New orders requests should be addressed to the Editor by e-mail. See the section "Subscription details".

Back issues: Single issues are available from the Editor. Details, including prices, are available upon request.

Advertising: For details, please, contact the Editor of the journal.

Corporate Ownership & Control

ISSN 1727-9232 (printed version)
1810-0368 (CD version)
1810-3057 (online version)

Certificate № 7881

КОРПОРАТИВНАЯ СОБСТВЕННОСТЬ И КОНТРОЛЬ

Почтовый адрес редакции:

Почтовый ящик 36
г. Сумы, 40014
Украина

Тел.: 38-542-288365
Факс: 38-542-288365
эл. почта: alex_kostyuk@mail.ru
alex_kostyuk@virtusinterpress.org
www.virtusinterpress.org

Журнал "Корпоративная собственность и контроль" издается четыре раза в год в сентябре-ноябре, декабре-феврале, марте-мае, июне-августе издательским домом Виртус Интерпресс, ул. Кирова 146/1, г. Сумы, 40021, Украина.

Информация для подписчиков: заказ на подписку следует адресовать Редактору журнала по электронной почте.

Отдельные номера: заказ на приобретение отдельных номеров следует направлять Редактору журнала.

Размещение рекламы: за информацией обращайтесь к Редактору.

Корпоративная собственность и контроль

ISSN 1727-9232 (печатная версия)
1810-0368 (версия на компакт-диске)
1810-3057 (электронная версия)

Свидетельство КВ 7881 от 11.09.2003 г.

EDITORIAL

Dear readers!

This issue of the journal is devoted to several issues of corporate governance.

Daniel ZÉGHAL, Raef GOUIAA try to evaluate the effect of the board of directors' characteristics on the cost of capital of the French companies. The results of this study, based on a sample of 87 French companies belonging to the French index SBF120 during 2005, show that the majority of the board of directors' characteristics have an important and significant effect on the cost of equity capital, on the cost of debt and on the balanced average cost of capital of the French companies.

M. Victoria Lopez-Perez, M. Carmen Perez-Lopez, Lázaro Rodriguez-Ariza examine whether the adoption of responsibility-oriented policies constitutes a strategic decision that may explain investment in research and development. The sample obtained is made up of data from 95 European corporations examined for the period 1998-2006. We identify a relation between R&D expenditure and practices of CSR.

Bernard Santen, Aloy Soppe examine the relationship between corporate governance characteristics and corporate financial distress. There are two main theoretical factors of interest: the structure of the monitoring process, and the personal characteristics of non-executive directors (NEDs). The first approach is basically *agency-theory* oriented, and emphasises relationships that complicate proper control, such as dependents on the board (Jensen, 1993). The second approach refers to the *resource dependency* theory, which focuses on the quality of the director(s) involved (Hillman and Dalziel (2003). The relevant relationships are tested on a newly built database consisting of 52 listed companies in the Netherlands that became financially distressed in the period from 1993 to 2003 and a control sample of 167 listed companies. We collected data on NEDs such as age, education, dependency, other board positions (and chairmanships), workload, and the number of executive and non-executive board members. A positive relationship with financial distress was found to exist if the average workload of NEDs on the board was high, or if there was a foreigner on the board. If one of the NEDs has inside knowledge, this is negatively related to financial distress. As a final conclusion, the hypothesis originating in resource dependency theory, which is that the human characteristics of NEDs are important in avoiding financial distress, cannot be rejected with regard to the Netherlands as examined in the period from 1993 to 2003.

M Steenkamp, F J Mostert, J H Mostert focuse on the claims handling process of motor vehicle insurance where a number of factors are considered by insurers. Some of the claims handling *factors* may be more important than others when insurers are assessing the claims submitted by the policyholders. The responding insurers also identify important *problem areas* in the claims handling process, and *solutions* that alleviate the different problems should be welcomed by the insurers. The empirical study is based on the perceptions of the *leading South African* short-term insurers, who represent 82.6% of the total gross premiums written for motor vehicle insurance in 2006. The *objective* of this research embodies the improvement of financial decision-making by insurers when occupied in the claims handling process of motor vehicle insurance.

K. Höne, J.H.P. Eloff analyse the requirements from the business community and mapped it against current research outputs. Findings clearly indicate that the two worlds are not entirely aligned and that in some cases minimum effort is being spent on the topics deemed important by the business community. Information Security Governance in general can benefit from an improved alignment between the needs of business and the outputs of the research community.

Ilse Maria Beuren, Elza Terezinha Cordeiro Müler verify how the Controllership institutionalization process takes place in corporate governance companies in Santa Catarina State – Brazil. Research was carried out by means of a multi-case study with a qualitative approach. Five companies were selected, but four answered the questionnaire, all listed in Bovespa's corporate governance. The research found only one company underwent a restructuring process in controllership. In this, the institutionalization process involved the system and sub-systems used in the company, encompassing every task and practice. The institutionalization of controllership assured the implementations, controls, performance, goals and levels of commitment of those involved.

CORPORATE OWNERSHIP & CONTROL

Volume 7, Issue 1, Fall 2009 (Continued - 2)

CONTENTS

INFORMATION SECURITY GOVERNANCE: BUSINESS REQUIREMENTS AND RESEARCH DIRECTIONS

*K. Höne, J.H.P. Eloff**

Abstract

World wide the importance of Information Security Governance is demanding the attention of senior management. This is due to the ever-changing threat landscape requiring that organisations adopt a focussed approach towards the protection of information assets. Any successful approach towards Information Security Governance is dependant on the availability of relevant and timely research outputs. The research community working on Information Security Governance are diverse and appears to be mis-aligned with the needs of the business community. The problem that this paper addresses is twofold. Firstly, it addresses the confusion regarding the meaning of Information Security Governance. Secondly, it assesses the gap between research and business communities from an Information Security Governance perspective. This article analyses the requirements from the business community and mapped it against current research outputs. Findings clearly indicate that the two worlds are not entirely aligned and that in some cases minimum effort is being spent on the topics deemed important by the business community. Information Security Governance in general can benefit from an improved alignment between the needs of business and the outputs of the research community.

Keywords: security governance, information

**Information and Computer Security Architecture Research Group, Department of Computer Science, University of Pretoria, Pretoria, South Africa*
eloff@cs.up.ac.za
SAP Meraka UTD, CSIR, Pretoria, South Africa

1. Introduction

With the blurring and disappearance of organisational boundaries through the proliferation of electronic information channels, the need drastically increased for organisations to acknowledge the importance of Information Security Governance. Organisations are recognising that an effective approach towards Information Security Governance can enable them to make business decisions faster and more accurately enabling them to retain and grow their market share. Yet there are still numerous organisations that cannot claim success in this area. Although organisations presumably deploy appropriate security technologies, they fail to link security technologies to real risks regarding the protection of information assets.

Although the operational aspects of information security such as tools and procedures are a well-established, organisational as well as technological risks and threats are in a continuous state of change. This demanded that organisations have to focus on the management aspects of information security enabling them to address relevant risks in a timely and appropriate manner. The discipline of Information Security Governance concerns itself with this problem domain and in particular ensures that information security activities are executed in an orderly manner commensurate to the risk exposure of an organisation and in support of its business goals.

The purpose of this article is to firstly explore what the business community, i.e. representatives of the corporate world who concern themselves with the discipline of information security but are not linked to an academic or research institution, views as important with regards to Information Security Governance. A list of key topics was compiled through the analysis of various annual global security surveys in which the business community participated. Secondly, the article investigates what the various research communities, i.e. academic and private institutions who focus on understanding the topic of information security through dedicated learning and investigation thereof, are currently focussing on in terms of their Information Security Governance-related work. The "business" view was then mapped to the "research" view to understand whether these two worlds were in fact complementing each other and addressing the same issues.

Both the business and research communities have in the past – and in some cases on an ongoing basis –

investigated the realm of Information Security Governance topics. In 2006 an exercise was conducted by Botha and Gaadingwe (2006) which analysed the research focus areas of the 20 SEC conferences hosted by the IFIP Technical Committee 11 from 1983 to 2005. The study indicated that the amount of Information Security Governance-related research remained fairly constant over the evaluated time period, although a slight decrease was noted in towards the latter part of the said time period. In contrast, the business community, regularly – in most cases on an annual basis – captures the views and perceptions of people responsible for the execution of the Information Security Governance function within organisations to determine the issues faced by them.

2. Definition of Information Security Governance

The concept of Information Security Governance is not well established and there is an absence of formal definitions. A Wikipedia (2008) definition for Information Security

Governance defines it as the discipline of corporate governance with the focus on information security systems and their performance and risk management. Furthermore, current literature indicates that the terms Information Security Governance and Information Security Management are used as synonyms. Because of the lack of formal definitions for Information Security Governance this paper proposes a definition for Information Security Governance that is based on literature references for Information Security Management.

The ITIL® publication of 1999 on Security Management describes the discipline as "the process of managing a defined level of security on information and IT services." (Cazemier, Overbeek & Peters, 1999) It furthermore alludes to the fact that the appropriate measures must be implemented to ensure that risks to the information assets are reduces reduced to an acceptable level. The Trusted Information Sharing Network of Australia (TSN) defines Information Security Management in its publication *Leading Practices and Guidelines for Enterprise Security Governance* (TSN, 2006) as "a methodical and cyclical approach to managing the protection of information to support the achievement of organisational goals."

Various other publications address the topic of Information Security Governance but do not specifically define the concept. Both the IT Governance Institute's *Information Security Governance: Guidance for Boards of Directors and Executive Management* (ITGI, 2006) and the United States of America's *Federal Information Security Management Act* (2002), allude to the fact that Information Security Management deals with the reduction of the risks faced by an organisation's information assets to an acceptable level through the application of applicable controls, yet do not provide a formal definition to this effect.

The link between information security and risk management is further supported in the *Guidelines for Security of Information Systems and Network* (OECD, 2002) of the

Organisation for Economic Co-operation and Development. These guidelines state that risk assessments covering all key business activities and operations of an organisation should form the basis of Information Security Governance. To complete the activities of the Information Security Governance function, the publication recommends that incident management, reviews, audits, policies, practices, measures and procedures should be integrated into the Information Security Governance discipline to support it.

Based on the definitions published above, for the purposes of this article, Information Security Governance is defined as the guidance and control of the information security activities of an organisation through the establishment of applicable policies, processes and procedures based on the risks faced by the information assets of the organisation. The definition implies that the discipline of Information Security Governance consists of activities aimed at managing the pre-defined level of security, commensurate to the risk appetite of the organisation, of all information assets, regardless of their state. These activities include:

- The identification of the business drivers directing the need for information security within the organisation. This evolves into the definition of the level of security required for the information assets;
- The proactive identification, evaluation and management of threats and vulnerabilities specifically related to the risks associated with the information assets. Both internal and external threats are evaluated;
- The definition of the applicable information security-related governance controls and measures, such as the policies that are required;
- The management and guidance of the stakeholders and role players involved in the information security landscape of the organisation;
- The monitoring of the information security-related controls to ensure that they perform as expected and are adhered to;
- The evaluation of legislation and regulatory requirements and ensuring that the applicable controls are in place to comply with these.

3. A Business Perspective on Information Security Governance Issues

Information security is no longer just a technical issue best left to the information technology staff to address. Over the past years, it has evolved into a discipline that is now seen not only as a necessary function, but as business critical. It requires the active participation of business managers in assessing the risks faced by the information assets in determining the best and most

effective response to them. As the business managers play a larger role in the information security discipline, it is important that their views on the topic are understood and addressed.

Various global Information Security Surveys are conducted annually to understand the business community's perception of information security in general, its effectiveness and the latest trends in terms of how to manage the discipline, e.g. the number of resources deployed in the security team and its budget. The surveys measure the perception at a given point in time. These surveys are aimed at identifying the latest trends with regards to information protection-related threats, risks and issues – both real and perceived. The majority of the surveys are aimed at senior non-technical business people and therefore provide a good indication of a business perspective of information security. Ideally the Information Security Governance research topics should match the issues and trends raised by the business community to ensure that the research is of value and appropriate and addresses the business community's concerns.

The annual global surveys conducted during the past two years by Deloitte (2006, 2007), Ernst & Young (2006, 2007) and PriceWaterhouseCoopers (2006) were analysed to identify the needs of the business community with regards to Information Security Governance. The results of the analysis were combined with the authors' practical experience in this domain. Below is a high-level description of the key Information Security Governance topics being challenged, questioned and worked on in the business community as viewed by the author of this paper. A summarised list of Information Security Governance research topics as perceived to be required by the business community is presented as a conclusion to this section of the article.

Foremost, the attention of information security managers is nowadays shifting more and more towards the people element of information security. As the majority of threats to information involve people, it has become important for organisation's to understand who is accessing their information and what actions the people can perform with or on the information.

Information Security Governance is gradually being more fully integrated into organizational culture through information security policies, roles, responsibilities and other governance structures. These are also more clearly and effectively communicated and therefore generally better understood by the owners of information assets. Yet there are few organisations today that have an information security aware culture, because the awareness activities currently employed do not bring about a change in behaviour. Organisations need to understand what an effective awareness strategy entails and the role of the human psyche is in bringing about lasting changes in the behaviour of employees.

One of the greatest challenges facing good governance for information security is the availability, attraction and retention of experienced Information Security Governance practitioners. Given these restraints, information security managers must be able to build innovative and creative organisational structures that retain the ability to deliver on their mandates. Additionally, information security managers must invest in the career development of their staff to ensure that their knowledge remains current.

Increasingly the priorities for Information Security Governance point to regulatory compliance, privacy and personal data protection, certification, benchmarking, risk management. The corporate world is urging the Information Security Governance practices to more closely integrate the discipline of information security within the organization through effective organisational structure, clear governance controls such as policies, and understanding the business initiatives and requirements. They are realising the importance of using secure, accurate and available information to proactively integrate into the business processes to maintain market share, deliver quality service and improve operational efficiency.

The requirement for regulatory compliance demanded the integration of the information security organisation into the rest of the organisation, specifically the risk management function, whereas in the past it was seen as a sub-function of the Information Technology division only. This is as a result of functional business groups, e.g. Information Technology, Finance and Corporate Management, relying on input from the information security organisation to strengthen their own internal controls. Organisations' senior executives are therefore demanding that Information Security Governance be in a position to demonstrate real business benefits and performance improvements, as well as addressing the threats to the information assets commensurate to the risk appetite of the organisation. Information security managers must be able to effectively identify risks, determine the likelihood and impact of them materialising and match appropriate countermeasures and controls to them. They need to be in a position where they clearly understand the regulations and legislations.

Additionally, the business expects compliance to regulations to be taken seriously especially where they relate to information and privacy protection. Compliance monitoring is the key activity for demonstrating that the information security controls and processes are functioning as expected and that they are addressing the said legal requirements.

With the disappearance of the traditional organisational boundaries, Information Security Governance is forced to formalise risk management practices to be able to identify threats and risks relating to information assets timeously and proactively. The risk management framework must enable the Information Security Governance function to address risk appropriately through mitigation, acceptance, avoidance or transfer thereof. Business processes must also be subject to regular threat analyses to ensure that there are sufficient Information

Security Governance controls in place to reduce the likelihood of the threats materialising.

Today, Information Security Governance is an important enabler for in organisations towards meeting their business objectives. Simultaneously, information security is an integral part of the business process, specifically aimed at enhancing service delivery. Furthermore, Information Security Governance also manifests itself in the improvement of vendor-related information risk management and the incorporation of information security principles into business relationships. Information security managers require the establishment of practical controls, such as policies, standards and procedures, to be able to underscore its value to the organisation in ensuring that the business processes are secure, yet still functional.

The lack of easy and practical approaches towards assessing the return of investment (ROI) in the information security domain results in inappropriate and insufficient security expenditure.

Furthermore, information security managers have to constantly justify security expenses. Information security managers need practical ways to measure the benefits of information security to the organisation.

In summary (Deloitte 2003, Deloitte 2005, Deloitte 2006, Deloitte 2007, Ernst & Young 2005, Ernst & Young 2006, Ernst & Young 2007, PriceWaterhouseCoopers 2004, PriceWaterhouseCoopers 2006), the business community's requirements in terms of Information Security Governance research can be described as follows:

- The correct and effective staffing of the information security organisation Information Security Organisational Structure);
- The sensitisation of owners and users of information assets through effective awareness initiatives (Information Security Awareness);
- Compliance guidance to assist organisations in understanding the complex requirements of information security-related regulations and legislations (Legal and Regulatory Issues);
- Fast, practical and feasible compliance monitoring, both in terms of being able to measure compliance to internal controls, as well as to external regulations and legislations (Compliance Monitoring);
- Standardisation of Information Security Governance activities, processes and controls through benchmarking against international practices such as ISO/IEC 27001/2, with the possible end-result being fully certified (International Best Practice Guidance);
- Thorough incident management processes that can support subsequent forensic investigations and prosecutions (Security Metrics and Incident Response);
- Quantitative return on investment calculations that can demonstrate the value of information security to senior management (Value of Information Security);
- Risk management practices that assist the Information Security Governance function in selecting the correct countermeasures and keeping abreast of threats and risks (Information Risk Management);
- The easy and efficient integration of Information Security Governance into the business processes (Convergence of Information Security Governance and Business).

This research effort did not attempt to prioritise the above list in order of priority as the quantifiable data was not available from the survey reports.

4. Current Information Security Governance Research

Through the evaluation of various research sources, specifically publications of global nonacademic research institutions with a reputation for focussing at least partly on information security and leading information security-related journals, for the period June 2006 to December 2007, a summary of the current Information Security Governance research trends has been compiled.

4.1 Information Security Governance Research: Non-academic Research Institutions

This article focused on the research initiatives and focus areas of the Information Security Forum (ISF) and the SysAdmin, Audit, Networking and Security (SANS) Institute, as organisations known to be focusing their activities on information security-related research.

This was combined with an investigation of the publications produced by the Information Systems Audit and Control Association (ISACA). In addition, the publically available abstracts from the Gartner and Forrester reports were reviewed to identify the focus of their Information Security Governance-related research. These organisations were selected based on their prominence in the global environment, as well as the fact that they all supported ongoing information security research programmes in one form or another, whether from individuals or from commissioned studies.

The Information Security Forum (ISF) consists of a membership of leading global organisations, generally large organisations. The main focus of its activities is on providing relevant research and practical guidance to its members on topics determined by its membership community. These topics are investigated due to a large proportion of information security-related activities being linked to them or them being perceived as being a problem area with which the majority of their membership is struggling with. The forum reevaluates its current project list on an annual basis by soliciting input from its members on the key topics and issues they would like the research efforts to be focussed on. The representatives of the member organisations generally include Chief

Information Security Officers, Information Security Managers and Chief Information Officers. The research is available to its membership community only, but as it is directed by its membership, it gives a good indication of the current most important information security topics. In addition, the forum has made it's Standard of Good Practice publically available to assist any interested party in identifying appropriate information security controls.

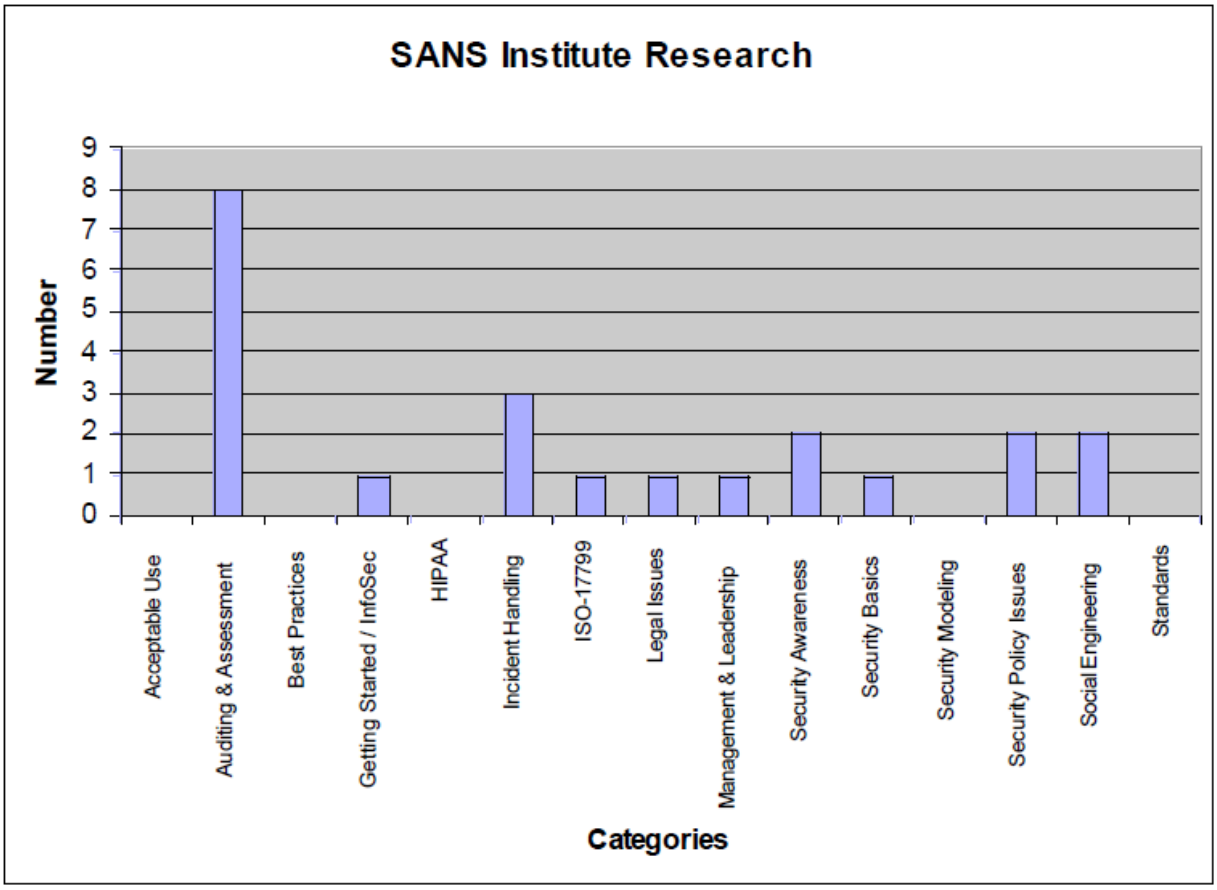
For each publication issued by the ISF, it provides a brief topic description. A study was performed on the ISF's website (2008) to identify the publications released within the specified timeframe. The associated topics of the publications were then captured to compile the list below. As the list indicates, a fair proportion of topics relates to the discipline of Information Security Governance or includes Information Security Management components, specifically governance and policy aspects, per the available abstracts (marked as "Partly" in the table below). The complete list is as follows:

Topic	Information Security Governance Related?
Compliance	Yes
Endpoint Security	No
Information Classification	Partly
Information Security Architecture	Yes
Management and securing of critical infrastructure, including governance and policy aspects	Partly
Risk Management (specifically Information Risk Management methodologies)	Yes
Secure System Development, including governance and policy aspects	Partly
Security Event Logging, including governance and policy aspects	Partly
Strategy and Policy	Yes
User Access Management, including governance and policy aspects	Partly
Windows Vista	No

The SANS Institute focuses on providing information security practitioners with the opportunity to share their knowledge and experience with fellow practitioners. The topics covered by the institute cover all aspects of information security, and are not only limited to Information Security Governance. The research papers on the various topics are submitted by information security practitioners. The information submitted generally includes challenges being faced by a range of individuals varying from auditors, network administrators to Chief Information Security Officers. It also address lessons learnt in solving and overcoming these challenges. The recently submitted research papers therefore provide a good indication of the current information security-related research topics as determined by individuals who deal with information security on a daily basis.

The SANS Institute (2008) research papers have been categorised into 67 categories by SANS itself, the majority of which are of a technical nature. The Information Security Governancerelated topics were identified out of these categories and the number of research papers submitted for each of these during the period under review for this article was determined.

The figure below indicates the distribution of these and represents the actual number of articles applicable to each topic. It clearly indicates that the most important research topic currently, as per the SANS Institute, is Information Security Governance auditing and assessment. A closer look at the articles classified under this topic indicates that articles on risk management were included in this topic. Some of the categories were identified as being Information Security Governance-related but have no value assigned to them due to the fact that no articles were published for them during the timeframe under review.



The Information Systems Audit and Control Association's (ISACA) membership consists of certified individuals involved in the audit of information technology controls. In recent years it has increased its focus area to also incorporate information security controls. It additionally offers career path certification in a program called Certified Information Security Manager (CISM).

The nature and primary focus of ISACA (2008) is towards research on Information Security Governance, with the majority of the research published during the past 18 months addressing this specific topic. In the past ISACA also conducted research on international Information Security Standards, the organisational structure of an Information Security Governance function, as well as user awareness. However, no publications appeared in these areas during the period under review.

Gartner and Forrester are leading global information technology-related research institutions. Although their main focus is not information security, their research efforts related to Information Security Governance were also evaluated due to their reputation for quality research aimed at the business community. Both these research institutions publish their research results on a restricted basis being only available to their membership community.

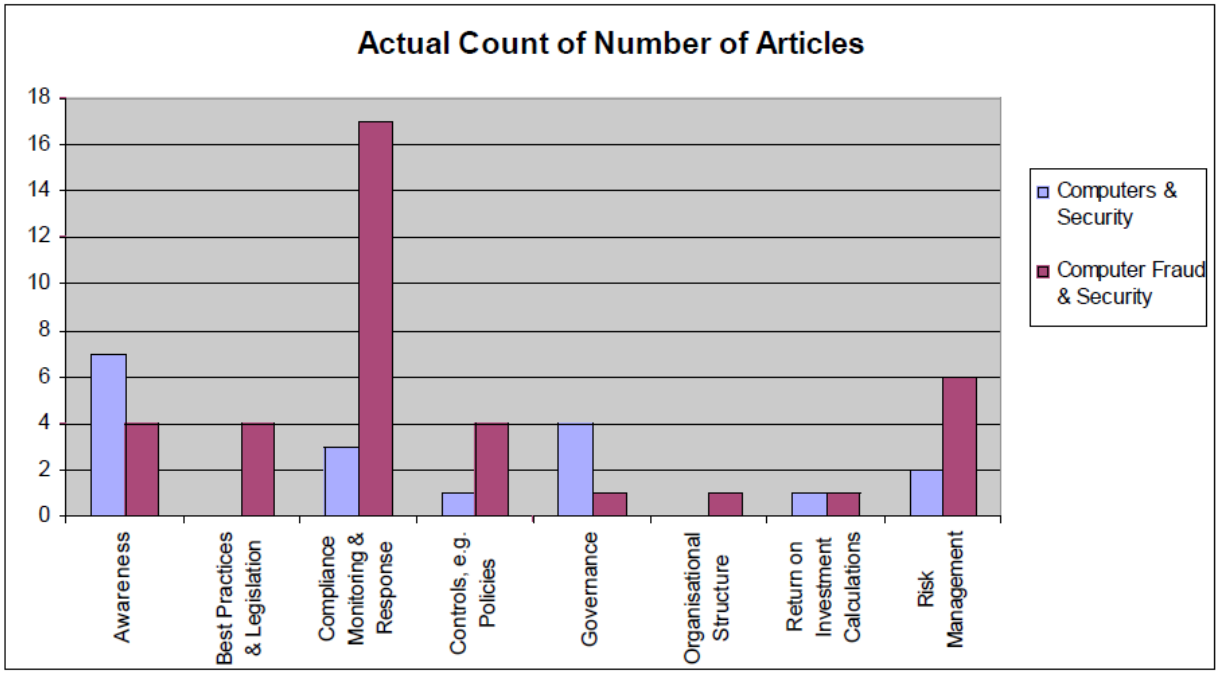
They do, however, provide abstracts of their research papers which were used by the authors of this paper to analyse Information Security Governance-related research outputs. In summary, Gartner (2008) addressed amongst others the following Information Security Governance topics: policies, charters and program maturity. In addition, Gartner conducted research into: the concept of an Information Security Management report card; the trends of Information Security Governance in Japan; the relationship between Information Security Governance and physical security; regulatory aspects and the Information Security Governance process.

Forrester (2008) focussed primarily on the commercial aspects of Information Security Governance; compliance to regulatory requirements and international best practices.

4.2 Information Security Governance Research: Information Security Publications

The research project at hand focuses on the papers published in two internationally leading journals: Computers & Security and Computer Fraud & Security Journals. The research outputs for the period June 2006 to December 2007 were considered. The objective was to determine which Information Security Governance topics were covered and to which extend.

The review consisted of an evaluation of the abstracts of all articles. Only research related articles were considered for the evaluation. Articles of a short news-related nature for the Computer Fraud & Security journal were disregarded. The graphs below illustrate a synopsis of the findings.



In summary, the following were identified as the most important topics:

- Compliance monitoring, with special focus on digital forensics and the appropriate incident management and investigation processes;
- Information Security Governance, such as aligning policies with strategy;
- Understanding legislation, specifically related to electronic information retention and privacy requirements;
- Information security awareness and education;
- Information security investments;
- Risk management models appropriate for information security;

Few research outputs were found on international best practice guidelines, such as ISO/IEC 2700127001, and their impact on the Information Security Governance discipline. This may be attributed to the fact that the guidelines have been available for a while and no longer warrant intensive research efforts. Organisational structures and Information Security Governance controls also received virtually no attention in the publications under investigation.

4.3 Information Security Governance Research: Summary

The research community by far primarily focussed their efforts on compliance monitoring and the associated procedures. The non-academic research institutions also focussed effort on the elements required to build and govern an Information Security Governance framework, such as the governance aspects, strategy and policies. The information security publications, in addition to the focus on compliance monitoring, have also reflected considerably on governance, awareness and risk management.

The research community's research efforts are summarised below:

- Awareness, including social engineering;
- Best practices and legislation;
- Compliance monitoring and response;
- Information risk management;
- Information security management controls, e.g. policies;
- Information security governance, including strategy;
- Organisational structure, including management and leadership;
- Return on Investment calculations.

The reader should note that the analysis of research efforts conducted for the article at hand did not evaluate the specific content related contributions made by the different efforts as only abstracts of the publications were considered. The article at hand thus rather concludes on coverage and effort.

5. GAP Analysis: Shortfall between Current Research and Business Expectations

The table below presents a mapping between the needs (topics) of businesses and the topics as covered by the various research communities.

Topic	Coverage By	Comments
Compliance Monitoring, including Security Metrics and Incident Response	• Computer Fraud & Security • Computers & Security • Gartner • ISF • SANS	Although not addressed by all research community role players under review, the highest total number of articles was produced on this topic.
Convergence of Information Security Governance and Business	• Forrester • Gartner	No research on this topic, except by the business community-aligned research institutes.
Information Security Governance, including Strategy, Policy, Architecture and Frameworks	• Computer Fraud & Security • Computers & Security • Gartner • ISACA • ISF • SANS	Addressed by the most research community role players under review.
International Best Practice Guidance	• Computer Fraud & Security • Forrester • SANS	Few research outputs on this topic; covered by a minority of research community role players.
Legal and Regulatory Issues, such as HIPAA	• Computer Fraud & Security • Forrester • Gartner • SANS	Very little research on this topic; covered by a minority of research community role players.
Organisational Structure	• Computer Fraud & Security	Very limited research conducted in this area.
Risk Management	• Computer Fraud & Security • Computers & Security • ISF • SANS	In-depth research performed by the ISF (includes a series of deliverables); good coverage by the research community role players.
Security Awareness, including Social Engineering	• Computer Fraud & Security • Computers & Security • SANS	Good coverage by the research community.
Value of Information Security	• Computer Fraud & Security • Computers & Security • Forrester	Limited coverage by the research community.

6. Conclusion

The research environment has embraced the requirement for research in the compliance monitoring and response area. This area incorporates the topics of traditional compliance monitoring, digital investigations, forensics and incident handling. This may be attributed to the fact that legislation enabling organisations to prosecute offenders and violators of secure information handling practices is maturing and therefore requires these processes. Most organisations also generate huge amounts of monitoring, logging and audit data on a daily basis that potentially takes up volumes of storage space and can even impact the performance of a system. The requirement to understand this data, process it and utilise it to improve

the information security environment has been clearly stated and may be a second factor contributing factor to the research outputs in this area.

People-related aspects of information security, and specifically the awareness and cultural aspects thereof, also received the attention of the research community. This is perhaps an indication of the realisation that information security is not only a technology problem but also a people problem. The organisational structure of the Information Security Governance function, however, received insufficient attention in the research community. Governance will always remain an important area of focus as it shapes and defines the Information Security Governance landscape.

There is almost a complete absence of research outputs in determining the value of Information Security also referred to as the return on information security investment. Senior management expects that the Information Security Governance function is in a position to demonstrate real value. New approaches to assess this value-added perspective on information security should be a priority in the future for the research community. In addition, once funding for the Information Security Governance function is secured, it requires to be applied in an intelligent manner so as to affect the greatest impact, value and benefit from a business perspective. Further research is also required in this area.

This analysis of information security related research efforts as conducted for this project indicates that there is a misalignment between business expectations and the issues currently being addressed by the research community. Current research efforts focus primarily on the operational aspects of information security, rather than the traditional business aspects such as the cost and value of information security. This may be an indication that researchers are not comfortable with the business aspects of the discipline or that there is not sufficient dialogue between the business and research communities.

7. References

1. Botha, R.A., Gaadingwe, T.G, 2006, 'Reflecting on 20 SEC Conferences', Computers & Security, vol. 25, no. 4, pp 247 – 256.
2. Cazemier, J.A., Overbeek, P.L. & Peters, L.M.C, 1999, *Security Management*, TSO, London.
3. Deloitte. 2003. *2003 Global Information Security Survey*. [online] [cited February 2008] http://www.deloitte.com
4. Deloitte. 2005. *2005 Global Information Security Survey*. [online] [cited February 2008] http://www.deloitte.com
5. Deloitte. 2006. *2006 Global Information Security Survey*. [online] [cited February 2008] http://www.deloitte.com
6. Deloitte. 2007. *2007 Global Information Security Survey: The shifting security paradigm*. [online] [cited February 2008] http://www.deloitte.com
7. Ernst & Young. 2005. *Global Information Security Survey 2005: Report on the Widening Gap*. [online] [cited February 2008] http://www.ey.com
8. Ernst & Young. 2006. *Achieving Success in a Globalized World: Is Your Way Secure?* [online] [cited February 2008] http://www.ey.com
9. Ernst & Young. 2007. *10th Annual Global Security Survey: Achieving a Balance of Risk and Performance*. [online] [cited February 2008] http://www.ey.com
10. *Federal Information Security Management Act*. 2002. [online] [cited February 2008] http://frwebgate.access.gpo.gov/cgibin/ getdoc.cgi?dbname=107_cong_public_laws&docid=f: publ347.107.pdf
11. Forrester. 2008. http://www.forrester.com [cited April 2008]
12. Gartner. 2008. http://www.gartner.com [cited April 2008]
13. Information Security Forum (ISF). 2008. [cited February 2008] http://www.securityforum.org
14. Information Systems Audit and Control Association (ISACA). 2005. *Critical Element of*
15. *Information Security Program Success.* United States of America.
16. Information Systems Audit and Control Association (ISACA). 2008. [cited February 2008] http://www.isaca.org
17. IT Governance Institute (ITGI). 2006. *Information Security Governance: Guidance for*
18. *Boards of Directors and Executive Management, 2nd Edition*. United States of America.
19. Organisation for Economic Co-operation and Development (OECD). 2002. *OECD*
20. *Guidelines for the Security of Information Systems and Networks. Towards a Culture of Security.* [online] [cited February 2008] http://www.oecd.org
21. PriceWaterhouseCoopers (PwC). 2004. *DTI Information Security Breaches Survey 2004*. [online] [cited February 2008] http://www.pwc.com
22. PriceWaterhouseCoopers (PwC). 2006. *DTI Information Security Breaches Survey 2006*. [online] [cited February 2008] http://www.pwc.com
23. SANS Institute. 2008. [cited February 2008] http://www.sans.org
24. Trusted Information Sharing Network (TISN). 2006. *Leading Practices and Guidelines for Enterprise Security Governance.* Australia.
25. Wikipedia.2008 [online] [cited September 2008] http://en.wikipedia.org/wiki/Special:Search?search=information+security+governance &fulltext=Search