Association for Information Systems
AIS Electronic Library (AISeL)

ECIS 2011 Proceedings

European Conference on Information Systems (ECIS)

Summer 10-6-2011

EXPERT OPINIONS ON INFORMATION SECURITY GOVERNANCE FACTORS: AN EXPLORATORY STUDY

Waldo Flores

Adnan Farnian

EXPERT OPINIONS ON INFORMATION SECURITY GOVERNANCE FACTORS: AN EXPLORATORY STUDY

Rocha Flores, Waldo, Department of Industrial Information and Control Systems, Royal Institute of Technology, Osquldas väg 10, 100 44 Stockholm, Sweden, waldorf@ics.kth.se

Farnian, Adnan, Department of Industrial Information and Control Systems, Royal Institute of Technology, Osquldas väg 10, 100 44 Stockholm, Sweden, farnia@kth.se

Abstract

Information Security Governance (ISG) is an important discipline that addresses information security at a strategic level providing strategic direction, optimized use of information resources and proper security incident management. ISG and the impact of poor security incident management have attracted much attention in the literature but unfortunately there is little empirical evidence regarding the explicit link between ISG and its effectiveness in terms of reducing negative impacts on business objectives from security incidents. Consequently, little exploration of ISG factors and their impact on the above mentioned measure of effectiveness exists. Further, to direct endeavors the crucial question is if there exist any differences in how effective these factors are in attaining this target. Currently, there is a lack in research considering this question. The research presented in this article explores the ISG domain further by empirically examine 30 ISG factors and their ability of reducing negative impacts on business objectives from security incidents. Data has been collected by surveying ISG experts. Ten factors were identified to have significant different means in relation to other factors according to a one-way ANOVA analysis that was conducted. The results give an indication on what ISG factors that have an effect, providing both support for further academic research and also decision support for implementing ISG.

Keywords: Information security governance, information security governance factors, Expert survey.

1 Introduction

Business information can unquestionably be considered as an extremely important asset to any organization. Therefore, protecting business information is a high priority throughout many industries. A survey conducted in 2006 by the British Government Department of Trade and Industry (DTI) showed that a nine-tenth of the organizations rated information security as important (Calder and Watkins, 2008). A study performed by the Texas AM University showed that 93% of companies that lost their data centre for 10 days or more due to a security incident filed for bankruptcy one year after the incident. 50% of businesses that found themselves without data management for this same time period filed for bankruptcy immediately (Moskal, 2008). As the result of a security incident can severely harm or even destruct an organization, it is imperative that organizations must make every effort to ensure that their business information is protected against the growing range of threats that is arrayed against this information, and if incidents due occur also ensure that corrective actions are taken to reduce negative impacts on business objectives.

However, recovering from a security incident in an effective way is a complex task and requires an effective management of information resources and that everybody in the organization partakes in a comprehensive process of managing the incident (Von Solms and Von Solms, 2006). Indeed, the still ever increasing reports of organizations suffering from fatal consequences from an incident suggest that organizations are still failing to manage security incidents effectively. One reason for this is that in the ever changing and complex IT environment, simply applying technical countermeasure to recover from incidents is no longer adequate (Calder and Watkins, 2008). Another reason is that information security traditionally has been seen as a technical job and best left to the technicians (Entrust, 2004). Fortunately, this image has significantly changed, and nowadays it is well-known that the responsibility for information security starts right at the top, and propagates right down to the operational level (Von Solms 2005a). Information Security Governance (ISG) addresses information security at a strategic level from a top-down approach and provides structure and relational mechanisms to ensure security in a holistic fashion (Johnston and Hale, 2009). ISG is further beneficial to an organization by providing: (i) strategic direction so that objectives are achieved, (ii) proper security incident management, (iii), responsible usage of information resources, and (iv) optimized information security investments. These examples are far from absolute and the list can be made much longer. However, they emphasize the benefits an organization can gain when implementing enterprise ISG (ISACA, 2006; Okhil et al. 2009; Von Solms, 2005a).

The role and importance of ISG and the severity of poor incident management have attracted much attention in the literature but unfortunately much of the literature has focused on technical and operational aspects (Sipponen and Kukkonen, 2007). There is further little empirical evidence regarding the explicit link between ISG and its effectiveness in terms of reducing negative impacts on business objectives from a security incident. Consequently, little exploration of ISG factors (e.g. IT security policies are enforced, Security vulnerabilities and incidents are identified, monitored and reported and cost-effective action plans for critical IT risks) and their impact on the above mentioned measure of effectiveness exists. This paper seeks on bridging this gap in the academic literature by empirically examine 30 ISG factors and their effectiveness in terms of reducing negative impacts from incidents. Empirical data has been collected through a survey distributed to experts in the ISG domain in which they report their opinions on the effectiveness of ISG factors. This paper does not aim to reach in-depth regarding each of the investigated factors; it rather aims at gaining an understanding of the relative impact of these factors and thus provides empirical input of potential relationship between factors and their impact open for discussion and other researchers might find interesting hypotheses to test in their work. The paper, further investigate a broad range of ISG factors but only their impact on reducing negative impacts on business objectives and not on proactive effectiveness, i.e. preventing attacks before they lead to incidents which causes impacts on the business. This question is left open for future research.

The rest of the paper is structured as follows. Section 2 presents a review of the literature and the research model of the study. In section 3 the methodology used in the study is presented. Section 4 presents and discusses the results. Section 5 concludes the paper.

2 Literature review and research model

This section aims to present a discussion of the literature with regard to ISG and the consequences of a security incident. The section further presents the research model of the study, which includes ISG factors and the negative consequences of a security incident that these factors aim to reduce.

2.1 Information Security Governance

The term information security governance (ISG) describes the process of how information security is addressed at an executive level (Posthumus and Von Solms, 2004). Von Solms (2005a) defines ISG as "management commitment and leadership, organizational structures, user awareness and commitment, 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".

According to the Corporate Governance Task Force (2004) ISG should be considered to be a facet of an organization's broader corporate governance strategy established by the Board, which is also responsible and accountable to the shareholders of the company and, therefore, they must ensure that their organization produces business value and delivers a suitable return on shareholder investment (King Report, 2001). Good ISG enables an organization to effectively fulfill all the internal and external requirements in terms of protecting business information assets and will most assuredly help to generate this return (Posthumus and Von Solms, 2004).

The academic literature in the area of ISG is far from extensive and established as its related concept corporate governance and IT governance. The literature that exists does in general highlight the importance of ISG and gives normative recommendations on how information security governance should be conducted. For instance, Von Solms (2001) and Moulton and Coles (2003) discusses the direct link between corporate governance and information security. These papers emphasize the importance of information security management as a part of both corporate - and IT governance and further guide directors and business managers in corporations of all sizes on how to ensure that business requirements are met and that their IT strategy is coordinated, coherent, structured, comprehensive, and cost-effective.

Other studies in the area of ISG cover general implementations of ISG programs in organizations and the role of frameworks and methodologies in Information Security Management and governance (Herath et al., 2009) and (Tabor, 2009).

Guidelines that are usually regarded as "pure" information security (e.g. ISO 27000) and "pure" IT governance (e.g. CobiT) frameworks have been discussed for ISG purposes in the literature by Von Solms (2005). The idea is that if these guidelines are followed, the security of the addressed system or organization will be increased. Looking at them from this point of view, they can thus be seen as theory for how to implement, manage and control ISG. A problem with them is however that they do not provide information about dependencies between different promoted features and goals to fulfill. For instance, the question to what degree certain factors impact the fulfillment of the goal to reduce negative impacts from security incidents has not been analyzed. To the author knowledge there is currently a lack of empirical data considering this question. Additionally, research on ISG factors in general and as earlier argued, factors to consider when planning ISG in a top-down approach in particular does not exist to a large extent.

2.2 Consequences of a security incident

Information security measures can be categorized into proactive and reactive measures. Proactive means that preventive measures have been applied to secure data or resources before a security incident can occur. Reactive means that curing measures are being applied to secure data or resources as soon as a security incident is detected (Venter and Eloff, 2003). In this paper the focus lays more on the reactive efforts to secure business information so that negative impacts on business objectives can be avoided, and as earlier argued, these impacts can be devastating for an organization. For an organization loss of business data is devastating as it can be considered to be an extremely important asset to any organization (Posthumus and Von Solms, 2004). (Halliday et al., 1996) goes even further by claiming that an organization's information resources are the lifeblood of that organization

When information technology is managed effectively, business information produced by these technologies can help an organization achieving competitive advantage over others, which produces business value and keeps shareholders and other investors satisfied. The business information can further be used, by top executives, to base the making of the numerous critical business decisions. It is therefore critical that this information has been kept confidential, accurate and timely. If any of these characteristics of information has been compromised due to a security incident there is a risk that the management team makes ill-advised decisions which could have a significantly devastating impact on the overall well-being of the organization. This could lead to huge negative impacts such as financial loss and even the tarnishing of an organization's corporate reputation (Entrust, 2004).

These consequences indicate how important it is for an organization to have an effective process of managing incidents to avoid fatal consequences on business objectives. In order to protect sensitive business information from the various incidents that potentially affect it, it is important to understand from what sources these incidents may arise. In general, a security incident arises from an agent seeking to exploit one or several vulnerabilities in an organization's information assets using a tool (e.g. physical attack, Dsniff). The agent further performs an attack, and if the attack is successful, a security incident (e.g. Denial of service, Social Engineering, Remote Execution) is caused (Santos Moreira, et. al., 2008). The security incident implies to a negative impact on business objectives (e.g. loss of business, reputational damage, operational disruption, privacy breach in the assets affecting the business).

To avoid these negative impacts it is critical for organizations to establish clear procedures for assessing the current and potential business impact of incidents, and implement effective methods of collecting, analyzing, and reporting data (NIST, 2004)(ISACA, 2006). Further, building relationships and establishing suitable means of communication with other internal groups (e.g., human resources, legal) and with external groups (e.g., other incident response teams, law enforcement) are also vital. Information security governance can support the achievement of building these capabilities in an organization. This paper therefore bases its research model on ISG factors and how these reduce negative impacts on business objectives.

2.3 Research model

For the purpose of studying if there exist any differences in how effective ISG factors are in attaining the goal of reducing negative impacts from security incidents; this study proposes to investigate the research model presented in figure 1. 30 factors are studied to assess their relative strength in reducing negative impacts from an incident. The general idea is that if these factors are implemented effectively, it is likely that an effective ISG program is in place to reduce negative impacts on the business. To achieve a sufficient degree of content validity the studied factors were retrieved from well-established best-practice literature (Von Solms, 2005b)(Brown and Nasuti, 2005). These are presented in the document "Information Security Governance: Guidance for Board of directors and Executive management 2nd Edition". In table 1, the studied factors are outlined. Each factor is also given a unique identification number.

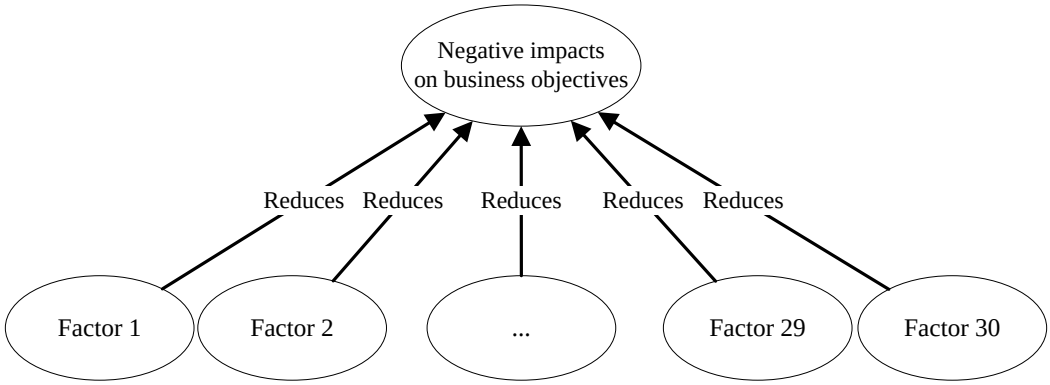

Figure 1. The research model of the study

Factor
1 IT security costs, benefits, strategy, policies and service levels are transparent and made understandable.
2 A common and comprehensive set of IT security policies are developed.
3 The IT strategy, policies and control framework are communicated
4 IT security policies are enforced
5 Security incidents in business impact terms are defined
6 The business impact of risks to IT objectives and resources is made clear.
7 An IT continuity plan that supports business continuity plans is established
8 The likelihood and impact of IT security risks are established and reduced
9 Regular risk assessments with senior managers and key staff are performed
10 Only authorized users are permitted to access critical and sensitive data
11 Critical and confidential information are withheld from those who should not have access to it
12 Security vulnerabilities and incidents are identified, monitored and reported
13 IT continuity plans that can be executed, tested and maintained are developed
14 The integrity of information and processing infrastructure is maintained
15 Making sure that IT services and infrastructure can resist and recover from failures due to error, deliberate attack or disaster
16 Making sure of proper use and performance of the applications and technology solutions
17 The number of incidents damaging reputation with the public is measured
18 The number of systems where security requirements are not met is measured
19 The number and type of suspected and actual access violations is measured
20 The number and type of malicious code prevented is measured
21 The number and type of security incidents is measured
22 The number and type of obsolete accounts is measured
23 The number of unauthorized IP addresses, ports and traffic types denied is measured
24 The number of access rights authorized, revoked, reset or changed is measured
25 Making sure that automated business transactions and information exchanges can be trusted
26 Making sure that IT services are available as required
27 Minimizing the probability of IT service interruption
28 Minimizing the impact of security vulnerabilities and incidents
29 Making sure of minimum business impact in the event of an IT service disruption or change
30 Establish cost-effective action plans for critical IT risks

Table 1. The studied information security governance factors

In order to assess the relative impact of these factors, IT experts were surveyed. The next section describes the methodology used for this purpose

3 Method

This study utilizes a survey as a measurement tool, this due to the obvious strengths in terms of statistical analysis and cost efficiency. The aim of the study is not to reach in-depth information regarding the control objectives; it is simply to gain an understanding of the relative importance of each objective and can thus be categorized as an exploratory study. The following subsections describe the sample of the study, the survey and how the data were analyzed.

3.1 Selection of experts

Expertise can describe skills, knowledge or talent, in tasks, activities, jobs, sport and games (Farrington-Darby. T., 2006). Expertise is developed over time through experience, working with specific practices, where the experts often are questioning, striving and hardworking individuals who seldom work in isolation. A thorough selection of experts based on expert criteria is important in order to achieve reliability and high quality of the performance of the study. In the present study the survey participants were strategically chosen to assure that they possessed the competence needed for the objectives of the study. Recommendations by Weiss and Shanteau (2003) and Shanteau (1988) on how to identify experts were followed.

The experts were identified from scientific articles from searches in professional societies databases such as the IEEE and in pure indexing databases such as SCOPUS. The search criteria involved combinations of topic-words such as ”information security governance”, “information security”, and ”information security management” with research area delimitations such as ”IT governance” and ”corporate governance”. 194 IT experts in the IT governance/Information security governance/information security domain were identified.

3.2 The survey

As the experts consulted in this study were widely geographically spread, a mail survey was used Mangione (1995). Invitations to respond to an electronic survey were sent in the spring 2010 to a sample of 194 IT experts. The internet-based application Relationwise hosted the survey, which was open for 30 days in the spring 2010. As recommended in Baxter et al. (2006) a reminder was sent to non-responding participants in order to increase the response rate.

The survey consisted of eight pages of which the first according to recommendation by Blair (2005) gave an introduction to the survey, and a description of how to answer the questions. Furthermore, the first page also included questions used to assess background information of respondents. The following pages of the survey consisted of 30 questions utilized in order to gain information regarding the significance of the factors in terms of reducing negative impacts on business objective from an incident. All of the 30 questions included in the survey were taken directly from ISACA (2006) without any manipulation.

For each of the 30 factors the respondents were asked to assess their degree of agreement with a statement concerning an ISG factor and its impact on the desired outcome. As the states varied from 1-5, a five point’s likert scale was used. For each factor and its corresponding outcome respondents were asked to answer on a quantitative scale from 1 to 5, were 1 = strongly disagree, 2 = disagree, 3 = partly agree, 4 = agree and 5 = strongly agree

3.3 Analysis method

As the purpose of the research is to assess the relative importance of three or more different factors and identify significant difference between them, descriptive statistics combined with one-way

ANOVA analysis is the preferred statistical analysis appropriate for the type of data Warner (2008) and Field (2009). The ANOVA analysis tests the null hypothesis that there doesn´t exist any significant differences between means of the assessed factors. ANOVA is also to be preferred in order to avoid type 1 errors and mass significance which is a risk using pair wise t-test Warner (2008). In the present study the statistical tool SPPS (Statistical Package for the Social Sciences) was used for the statistical analysis. In order to identify significant differences between the assessed ISG factors the steps outlined in Warner (2008) and Field (2009) and interpreted by the author, are followed:

1) Display descriptive statistics
2) Run test for homogeneity of variances
3) Run the Anova test
4) Run multiple comparisons
5) Interpret and report the results

In the following, how each of these steps was carried out in the present study is detailed.

1) Display descriptive statistics: As a first step factor means, standard deviation, standard errors, confidence interval, maximum and minimum values are displayed. These are also pictured in a bar chart with error bars indicating 95 % confidence interval around the mean. Due to this the highest mean value and were the variability is the lowest can be detected.

2) Run test for homogeneity of variances: Before running the one-way ANOVA, one first needs to see if there exists any difference of variances between the assessed factors. For this purpose, Levene´s test is employed. This test is used to test the null hypothesis that the variances between the groups are equal (i.e. the differences between the variance is zero). If the Levene´s test is significant at then one can conclude that the null hypothesis is incorrect and that the variances are significantly different - therefore, the assumption of homogeneity of variances has been violated.

3) *Run the ANOVA test*: The ANOVA analysis can now be employed. ANOVA tests the null hypothesis that the factor means are the same, and is represented by the F-ratio for the combined between group effect. The F-ratio in particular stands for the variance of the group means (mean of the within group variances). The null hypothesis is rejected if the F ratio is large. However, if the significance value for the test is , the null hypothesis can be rejected (there exists a significant difference between mean values in the dataset) and there is a probability lower that 5% that the size of an F-ratio occurred by chance.

4) Pair wise multiple comparisons: If it is determined that differences exist among the means, i.e. the null hypothesis is incorrect, thus the variances are significantly different, multiple comparison are to be employed. Multiple comparisons gives the differences of means for all possible pair of means and identifies means that differentiate from others with a *p* value at the 0.05 level. From these tests factors with significant higher or lower mean value according to expert opinions can de identified.

5) Interpret and report the results: Questions to be answered to interpret the results are the following*:* What factor means differ from each other? Which factors scores the highest and lowest mean values? The test for homogeneity of variances, the results from the ANOVA analysis, with the details on the F-ratio and the degree of freedom from which it was calculated from are and the results from the multiple comparisons to identify significant higher and lower means are to be reported.

4 Results and discussions

Out of 194 respondents (experts from academia) that were invited to the survey, 46 respondents began it, and 22 completed it. Thus the response rate for this study is 11.34 %. Since now study of this kind has yet been performed in the ISG domain it is difficult to see how this response rate stands compared

to previous similar studied. However, according to a previous study by were email invitation were used, a response rate of 15% is considered to be relatively high (Ali and Green ,2009). With this in mind, and the fact that the ISG domain isn't as established as the ITG domain, the author finds the response rate to be satisfactory.

4.1 Expert opinions on ISG factors

Descriptive statistics was used to display the relative importance of ISG factors. Figure 2 pictures factor mean values using bar charts with error bars with 95% confidence interval. Table 2 displays the mean value, Std. Deviation, Std. Error, 95% confidence interval for the mean value, minimum value, and maximum value. By analyzing the bar chart and the table the highest mean value and were the variability is the lowest was detected.

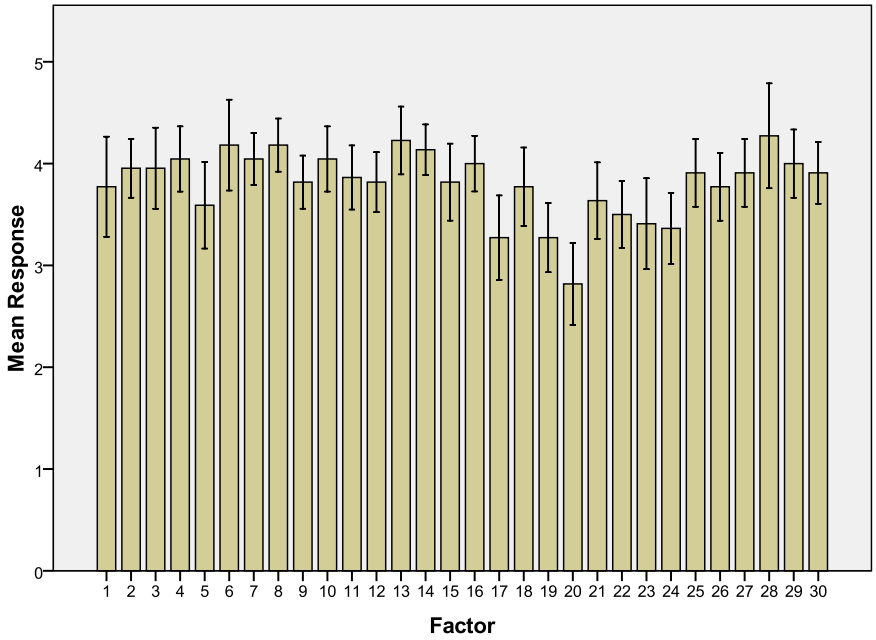

Figure 2. Respondent data on factors reducing negative consequences from security incidents

Levene´s test was employed to test if there significant difference among the variances existed. Levene´s tests the null hypothesis that the variances of the factors are the same. In this case, Levene´s test tested whether the variances of the 30 factors were significantly different. If Levene´s test is significant (i.e. the value of significance is less than 0.05) then we can say that the variances are significantly different. In this study Levene's test gave a significance value for homogeneity of variances of, , the variances of the factors are therfore significantly different.

The main ANOVA of the dataset displays whether the group means are the same. The ANOVA result is represented by the F-ratio for the combined between group effect. In our analysis the F-value was 3,730. Further, there is a probability of 0.000 that an F-ratio of this size would have occurred by chance. The significance value comparing the factors was . So, the null hypothesis could be rejected (there is no difference in the mean scores with the 30 factors). As the null hypothesis could be rejected there exists a significant difference between mean values in the dataset.

Std. Deviation	Std. Error	95% Confidence interval for Mean		Minimum	Maximum
		Lower bound	Upper bound		
1,110	,237	3,28	4,26	1	5
,653	,139	3,67	4,24	3	5
,899	,192	3,56	4,35	2	5
,722	,154	3,73	4,37	3	5
,959	,204	3,17	4,02	1	5
1,006	,215	3,74	4,63	1	5
,575	,123	3,79	4,30	3	5
,588	,125	3,92	4,44	3	5
,588	,125	3,56	4,08	2	5
,722	,154	3,73	4,37	3	5
,710	,151	3,55	4,18	3	5
,664	,142	3,52	4,11	3	5
,752	,160	3,89	4,56	3	5
,560	,119	3,89	4,38	3	5
,853	,182	3,44	4,20	3	5
,617	,132	3,73	4,27	3	5
,935	,199	2,86	3,69	1	5
,869	,185	3,39	4,16	2	5
,767	,164	2,93	3,61	2	5
,907	,193	2,42	3,22	1	4
,848	,181	3,26	4,01	1	5
,740	,158	3,17	3,83	2	5
1,008	,215	2,96	3,86	1	5
,790	,168	3,01	3,71	1	4
,750	,160	3,58	4,24	2	5
,752	,160	3,44	4,11	2	5
,750	,160	3,58	4,24	2	5
1,162	,248	3,76	4,79	3	6
,756	,161	3,66	4,34	2	5
,684	,146	3,61	4,21	3	5
,852	,033	3,74	3,87	1	6

Table 2. Respondent data on factors reducing negative consequences from security incidents

Pair wise multiple comparisons test the difference between each pair of means to determine which factors are responsible for the difference, and yield a matrix consisting of comparisons. Based on these comparisons five factors were identified have significantly different means at a significance level of 0.05. These are displayed in Table 2. The value of the cell in the table represents the difference of means between the factors that are compared. The values with an asterisk depict the difference of means between the compared factors (see Table 2).

Factor	13	17	19	20	28
1	0,455	-0,5	-0,5	-,955*	0,5
2	0,273	-0,682	-0,682	-1,136*	0,318
3	0,273	-0,682	-0,682	-1,136*	0,318
4	0,182	-0,773	-0,773	-1,227*	0,227
5	0,636	-0,318	-0,318	-0,773	0,682
6	0,045	-0,909	-0,909	-1,364*	0,091
7	0,182	-0,773	-0,773	-1,227*	0,227
8	0,045	-0,909	-0,909	-1,364*	0,091
9	0,409	-0,545	-0,545	-1,000*	0,455
10	0,182	-0,773	-0,773	-1,227*	0,227
11	0,364	-0,591	-0,591	-1,045*	0,409
12	0,409	-0,545	-0,545	-1,000*	0,455
13		-,955*	-,955*	-1,409*	0,045
14	0,091	-0,864	-0,864	-1,318*	0,136
15	0,409	-0,545	-0,545	-1,000*	0,455
16	0,227	-0,727	-0,727	-1,182*	0,273
17	,955*		0	-0,455	1,000*
18	0,455	-0,5	-0,5	-,955*	0,5
19	,955*	0		-0,455	1,000*
20	1,409*	0,455	0,455		1,455*
21	0,591	-0,364	-0,364	-0,818	0,636
22	0,727	-0,227	-0,227	-0,682	0,773
23	0,818	-0,136	-0,136	-0,591	0,864
24	0,864	-0,091	-0,091	-0,545	0,909
25	0,318	-0,636	-0,636	-1,091*	0,364
26	0,455	-0,5	-0,5	-,955*	0,5
27	0,318	-0,636	-0,636	-1,091*	0,364
28	-0,045	-1,000*	-1,000*	-1,455*	
29	0,227	-0,727	-0,727	-1,182*	0,273
30	0,318	-0,636	-0,636	-1,091*	0,364

Table 2. Pair wise multiple comparisons

4.2 Discussions of the statistical analysis

A one-way ANOVA was conducted to compare the mean scores of ISG factors assessed by experts in the ISG domain, on a lickert scale (1 = strongly disagree, 2 = disagree, 3 = partly agree, 4 = agree and 5 = strongly agree). Examination of a histogram of ISG factor scores indicated that the scores were approximately normally distributed and no extreme outliers were found. Prior to the ANOVA analysis, Levene´s test for homogeneity of variances was used to examine whether there were serious violations of the assumption of variance across the factors. No significant violations were found at the degrees of freedom which it was calculated: .The overall F-ratio for the one-way ANOVA was significant at an significance level: . Thus, conclusion that there exist significant differences of means in the data set could be drawn. To identify which means that differ, all possible pairwise comparisons were made using the Tukey's HSD (Honestly Significant Difference) test. Based on this test conclusions on which's ISG factors that experts assess have significant higher value than others could be drawn. This is summarized in table 3.

Factor	
28	Factor 28 has significant higher mean value than factor 20, 19 and 17
13	Factor 13 has significant higher mean value than factor 20, 19 and 17
20	Factor 20 has significant lower mean value than all factors except factor 5, 17, 19, 20, 21, 22, 23, and 24

Table 3. Significant stronger factors

Below, the factors that scored the highest/lowest mean values and were identified to be significant different are discussed.

Factors scoring the highest mean value: Factor 28 Minimizing the impact of security vulnerabilities and incidents
Factor 28 "Minimizing the impact of security vulnerabilities and incidents" scored the highest mean value of all factors and significantly higher than factor 20 "The number and type of malicious code prevented is measured", factor 19 "The number and type of suspected and actual access violations is measured", and factor 17 "The number of incidents damaging reputation with the public is measured". An explanation to this could be that this factor can be categorized as a reactive countermeasure and it is extremely difficult to have a successful ISG in place if the impact from security vulnerabilities and incidents isn't handled effectively. Another explanation could be that the questions of the survey explicitly asked for expert opinions on factors reducing negative consequence from security incidents.

Factors scoring the next highest mean value: Factor 13 IT continuity plans that can be executed, tested and maintained are developed
Factor 13 "IT continuity plans that can be executed, tested and maintained are developed" scored the next highest mean value of all factors and significantly higher than factor 20 "The number and type of malicious code prevented is measured", factor 19 "The number and type of suspected and actual access violations is measured", and factor 17 "The number of incidents damaging reputation with the public is measured". An explanation to this could be that an IT continuity plan is one of the most important documents to keep the IT running to support different business functions. A possible other explanation is related the goal of the study, i.e. assess factor that reduces negative consequences from security incidents. In this sense, IT contingency is the most important factor to keep the IT running to avoid any severe impacts on the business.

Factors scoring the lowest mean value: Factor 20 The number and type of malicious code prevented is measured
Factor 20 "The number and type of malicious code prevented is measured" scored the lowest mean value of all factors and significantly lower than all factors except factor 5 "Security incidents in business impact terms are defined", factor 17 "The number of incidents damaging reputation with the public is measured", factor 19 "The number and type of suspected and actual access violations is measured", factor 20 "The number and type of malicious code prevented is measured", factor 21 "The number and type of security incidents is measured", factor 22 "The number and type of obsolete accounts is measured", factor 23 "The number of unauthorized IP addresses, ports and traffic types denied is measured", and factor 24 "The number of access rights authorized, revoked, reset or changed is measured". An explanation to this could be that measuring security incidents doesn't directly affect how an organization reduces negative consequences from security incidents. When measuring, any severe incident has by then already made an impact on the business. This is can further be seen when analyzing the mean values of factors concerning measurements.

5 Conclusions and further work

This article has further explored the ISG domain and the importance of ISG factors in particular. The relative impact of information security governance factors on the goal related to ISG of reducing negative impacts from security incidents has been examined. Factors were extracted from best-practice literature and data was collected trough surveying experts in the ISG domain. Ten factors were identified to have significant different means in relation to other factors according to an ANOVA analysis that was conducted. The factors "Minimizing the impact of security vulnerabilities and incidents" and "IT continuity plans that can be executed, tested and maintained are developed" had the highest mean value and score significantly higher than "The number and type of malicious code prevented is measured", "The number and type of suspected and actual access violations is measured", and "The number of incidents damaging reputation with the public is measured. The factors "The number and type of malicious code prevented is measured" scored the lowest mean value of all factors and significantly lower than all factors except eight factors (cf. table 3).

Although that the study doesn't draw any general conclusion from the results, from a practitioner's point of view the results gives some indications that a manager responsible for the ISG program can concentrate the efforts to the factors that experts assess have the most impact on the goal of reduces negative impacts from security incidents. From an academic point of view, the results can be used to further analyze how factors included in an ISG program can be prioritized not only when acting reactive in the work of ensuring security, but also for preventive and detective purposes.

Another natural continuation of the present line of research is to validate the results with case studies of the effect of factors in actual ISG implementations on reducing negative impacts from security incidents.

References

Ali. S., G. P. (2009). Effective information technology (IT) governance mechanisms: An IT outsourcing. Inf Syst Front .

Blair, C. R. (2005). Designing surveys. Sage Publications Inc.

Blaxter, L. Hughes, C., and Tight, M (2006). How to research. Open University Press.

Brown, W. and Nasuti, F. (2005). Sarbanes Oxley and enterprise security: IT governance what it takes to get the job done. Security Management practices November/December.

Calder, A., and Watkins, S (2008). IT governance A manager´s guide to Data Security and ISO 27001/ISO 27002, 4th edition, Kogan Page.

Corporate Governance Task Force (2004). Information security governance: a call to action. Available from: http://www.cyber.st.dhs.gov

Eijiroh Ohkil, Yonosuke Harada, Shuji Kawaguchi (2009). Information Security Governance Framework. In proceedings of the 1st ACM Workshop on Information Security Governance, WISG'09, Chicago, Illinois, USA.

Entrust. (2004). Information Security Governance (ISG): an essential element of corporate governance. Available from: http://www.entrust.com/governance/

Farrington-Darby. T., W. J. (2006). The nature of expertise: A review. University of Nottingham, UK

Field, A. (2009). Discovering Statistics Using SPSS, third edition, Sage Publications Inc.

Halliday S., Badenhorst K., Von Solms R. (1996) A business approach to effective information technology risk analysis and management. Information Management and Computer Security, 4(1):19-31.

Herath, T., Gupta, M., Rao, R.H. (2009). Forging an Effective Information Security Governance Program A Case Study of a Multinational Organization. In Proceedings of the IFIP TC 8 International Workshop on Information Systems Security Research, Cape Town, South Africa.

ISACA (2006). Information Security Governance: Guidance for Board of directors and Executive management, 2nd edition.

Johnston, A.C. and Hale, R. (2009). Improved Security through Information Security Governance communications of the acm, 52 (1).
King report. (2001). The king report on corporate governance. Available from: http://www.iodsa.co.za
Mangione, T. W.(1995). Mail surveys. Improving the quality. Sage Publications Inc.
Moskal , E. (2006). Business continuity management post 9/11 Disaster report methodology. Disaster Recovery Journal. Vol 19, Issue 2.
Moulton, R. and Coles, R.S. (2003). Applying information security governance, Computers & Security, 22 (7).
NIST. (2004). Special Publication 800-61 Computer Security Incident Handling Guide Recommendations of the National Institute of Standards and Technology.
Posthumus, S. and Von Solms, R. (2004). A framework for the governance of information security Computers & Security, 23, 638-646.
Relationwise. Relationwise survey tool, www.relationwise.se
Shanteau. J. (1988). Psychological Characteristics and Strategies of Expert Decision makers. Manhattan USA: Kansas State University.
Santos Moreira, E., Martimiano, L.A.F., Santos Brandão, A.J., Bernardes, M.C. (2008). Ontologies for information security management and governance", Information Management & Computer Security, Vol. 16(2), pp.150-165.
Siponen, M. and Oinas-Kukkonen, H.(2007). A Review of Information Security Issues and Respective Research Contributions, The Data Base for Advances in Information Systems 38, 60-80.
Tabor, S.W. (2009). Exploring the Role of Frameworks & Methodologies in Information Security Management & Governance - Research in Progress. In Proceedings of the Americas Conference on Information Systems, San Francisco, California, USA.
Venter, H.S. and Eloff, J.H.P. (2003). A taxonomy for information security technologies Computers & Security. Volume 22, Issue 4, pp. 299-307.
Von Solms, B. (2001) Corporate Governance and Information Security, Computers & Security, 20, 215-218.
Von Solms, B. (2005b). Information Security governance: COBIT or ISO 17799 or both? Computers & Security, 24, 99-104.
Von Solms, S.H. (2005a). Information Security Governance – Compliance Management vs Operational Management. Computers & Security 24, 443-447.
Von Solms, R. and Von Solms S.H. (2006). Information Security Governance: A model based on the Direct - Control Cycle. Computers & Security, 25, 408-412.
Weiss. D.J., Shanteau. J. (2003). Empirical Assessment of Expertise. Los Angeles: Department of Psychology, California State University.
Warner, R.M. (2008). Applied statistics, Sage Publications Inc.