feature

Boardroom Dynamics

Group Support for the Board's Involvement in a Smart Security Decision-making Process

Decision making during business meetings is an elusive phenomenon[1] for a couple of reasons. Business meetings have been defined as "…a gathering where people speak up, say nothing, and then all disagree."[2] In general, the main objectives of meetings are to facilitate and enable decision makers in exchanging knowledge, discussing complex topics and monitoring large projects, and this all happens under pressure and amid uncertainties.[3]

Within the domain of information security, boards become more exposed due to expanded regulations, an escalating external threat environment and the complexity of IT on which organizations increasingly rely. All these factors drive increased focus from boards and executive management and the requirement for information security to integrate more widely into the business. This seems a challenge, since information security is perceived as a complex, IT-only subject and decisions are made in IT silos under pressure.[4] The result is an unbalanced engagement of the relevant participants and, potentially, poor decision making. This poses a risk to organizations.

These pressures and uncertainties often result in:

- Cost to the business in man-hours due to prolonged decision making
- Business risk due to delayed actions as complexity causes paralysis

Yuri Bobbert, CISM, SCF
Is chief information security officer at NN Group. He is associate professor at NOVI University of Applied Sciences, visiting researcher at Antwerp Management School (Belgium) and Radboud University in Nijmegen (The Netherlands). He did his Ph.D. research on improving the maturity of business information security in numerous organizations.

Hans Mulder, Ph.D.
Is The Standish Group European research director and executive professor at the Antwerp Management School (Belgium). As the founder of Viagroep.nl, a company that has investments in IT industry, he is on the management and executive boards of various IT companies. He is regularly engaged as an IT expert when conflicts between companies need to be resolved in or out of court, such as participating in arbitration, mediation and expert reports. He has published more than 100 articles in specialist journals and international magazines and is the author of several books.

- Increased risk of making bad decisions due to complexity

The impact of these three factors on the future of organizations can be dramatic for the organization and its leaders. In contrast, getting these decisions correct and making them in a timely manner can provide a tremendous strategic advantage and secure the future of a business. This can be referred to as business information security (BIS). This article addresses the major takeaways of efficient meeting facilitation and decision making based on practical and academic insights. Focusing on boards and executive management, including the chief information security officer (CISO) and the chief risk officer (CRO), to increase efficiency in meetings and engage important stakeholders at all levels helps gain a mutual level of knowledge and meaning to increase impact and BIS effectiveness.

From IT Security to Business Information Security

Security is still seen as a technology-specific topic, not a wider business issue,[5, 6] undeservedly, because the scope of information security is much broader than just IT.[7, 8] In particular, this can be a challenge for mid-sized organizations.[9, 10, 11] The lack of knowledge on information security can be addressed by adopting an appropriate framework; however, successful adoption requires strong engagement with multiple parties involved in business processes throughout the decision-making process.[12, 13, 14]

The information security and risk management domains are largely managed by professionals who are well educated in IT, security or other related topics. They often receive only limited training in business management principles and, therefore, it can be challenging to find a fruitful balance between content and process.[15] As a result, most meetings are managed based on the content instead of the process and, therefore, are derailed. This can result in meeting outcomes that fall far short of the desired objectives.[16]

Meetings without a steering process may lead to participant disappointment.[17] To avoid this disappointment and increase the effect of collaborating toward predefined targets, meeting software can be employed to help facilitate goals achievement. According to a longitudinal study on 900 meetings, a 56 percent savings in man-hours can be achieved with the use of this technology and an experienced facilitator.[18] Given that the average manager spends 25-80 percent of his/her time in meetings, the companywide savings are easily calculated, and the quality of the decision-making process enhanced.[19]

Thus, information security requires a business-oriented approach that involves multiple parties at all levels.

Introduction of Group Support Systems

Group support systems (GSS) facilitates the effective collection, organization, evaluation, cross-impact analysis and reporting of data[20] with the assistance of a group moderator. GSS can help to resolve subjective dilemmas among participants such as culture, attitudes or hierarchic relations. Because GSS support anonymous participation in meetings, individuals are more willing to be open and transparent. This enables ideas to be judged based on the content rather than origin. It also addresses the differences between introverted and extroverted participants, an issue that is seldom discussed, but is a dominant factor in meeting effectiveness as it impacts both process and content and, therefore, the eventual outcomes. The role of the facilitator is to acknowledge these different participants' characteristics prior to and during the meeting.

GSS require the establishment of a predefined agenda for the meeting and prompt the facilitator to analyze in advance the topic, the group composition, and differences in participants' issues and interests. This enables the facilitation of the meeting to align to the desired outcomes. The role of the facilitator is to make sure everybody has a voice in the meeting and to stimulate a free-flowing discussion throughout the processes displayed in **figure 1**. The facilitator must help members share their experiences, elicit the views of all participants, keep group members on track and capture responses.[21]

"Because GSS support anonymous participation in meetings, individuals are more willing to be open and transparent."

This calls for the facilitator to possess certain core competencies, including:

- Generating new data from the participants, thus creating awareness and transferring knowledge
- Testing assumptions
- Sharing relevant information (knowledge) with the participants
- Using specific examples and agreeing on the meaning of important terms
- Explaining reasoning and intent
- Focusing on professional, not personal, opinions
- Combining advocacy with inquiries
- Jointly designing next steps and ways to test disagreements
- Discussing "undiscussable" issues (barriers)

- Ranking outcomes (parameters or intervention candidates)
- Comparing outcomes and discussing variables (double-loop learning)[22]

The acceleration of the meeting is achieved by the collective and simultaneous discussion, so the size of the group does not negatively influence the meeting's duration. On the contrary, larger groups can influence the quality of the meeting and decision-making process.[23] The results of the meetings are directly processed and, therefore, visible on the participants' screens, which enables double-loop learning.[24] The data are directly reported in an understandable and attractive format.

> **"The use of GSS software enables complex and knowledge-intensive decision-making processes to be carried out faster and more efficiently."**

Everybody Has a Voice

GSS, which have made a tremendous contribution to knowledge sharing over the last 15 years,[25] are often used to diverge or to converge individual standpoints in the decision-making process. The use of GSS is highly efficient, effective and user friendly.[26, 27] The Dutch Police Academy conducted 45 GSS sessions from 2005 to 2011, in which 763 employees of the Dutch police participated[28] in intelligence gathering for cold cases.[29] This large-scale longitudinal GSS research showed the potential of GSS as a facilitating system and methodology for capturing data and knowledge sharing, and reusing previous collected knowledge that was initially implicit and was made explicit through group discussion and thinking.[30]

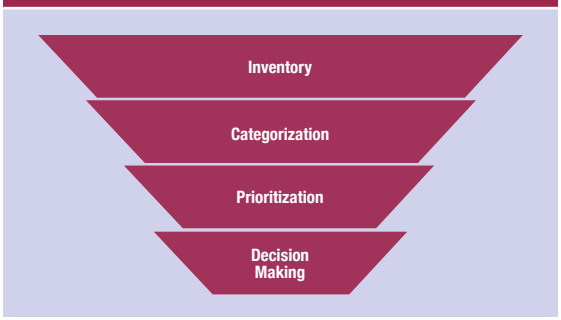
During sessions in which the authors have facilitated, the early engagement of senior management is addressed by the participants as a prerequisite to improve the maturity of BIS.[31] Discussion is targeted to the specific underlying problems with which BIS is coping.

The first is a sense of urgency within the boardroom. The second is *ad hoc* approaches to solving problems. GSS can bridge this gap in two ways:

1. By making the problem explicit based on theoretical constructs and concepts thereby creating a sense of urgency on the magnitude of the problem
2. By establishing awareness and a mutual level of knowledge among those involved with the problem (object and subject) to stimulate group dialog and facilitate socialization,[32] thinking,[33] discussions[34] and using the decision-making process for strategic planning,[35] e.g., improving the maturity of BIS[36]

Figure 1 displays the flow of the GSS process of decision making.

Figure 1—GSS Decision-making Process Flow



Source: Y. Bobbert and J. B. F Mulder. Reprinted with permission.

Thus, technology and proper meeting facilitation can help with common pressures and uncertainties, such as the absence of "evidence trailing." Collecting,

storing and "trailing" during the decision-making process the information about who made which decision based upon what evidence may seem rather complex, but it does not have to be, since contemporary technology can facilitate it. GSS technology can record and store the entire meeting, from brainstorming to the final decisions.

In the absence of efficient process facilitation, meetings lack balanced engagement of all participants and the "law of decibel"[37]—in which the person dominating the meeting with his/her opinion can influence the opinion of the group—may quickly take over. Meetings then become subjective and chaotic, and may lead to participants' frustration and impaired decision making. Managing the process of the meeting is as important as the content, if not more so, in avoiding this outcome.[38] This is especially the case with projects that are complex and require a certain level of technical knowledge and a longer time slot.

GSS in Business Information Security

Scientific research at Antwerp University (Belgium) and Radboud University (Nijmegen, The Netherlands) has found that the use of GSS software enables complex and knowledge-intensive decision-making processes to be carried out faster and more efficiently than what is commonly experienced in business. For example, in the areas of risk management and information security, GSS makes it easier and swifter to arrive at an informed decision—a primary desire within the information security industry. A use case performed in the health care industry revealed that GSS and proper facilitation assisted the CISO with engaging management and prioritizing risk and security management activities.

Savings on Man-hours

"For example, IBM has documented, through a cumulative comparison of person-hours expended, a 56 percent savings attributable to GSS use.... However, it is unlikely that a GSS, in and of itself, is sufficient to turn meetings into satisfying, productive events...although the technology has matured to the point where it is very easy to use by almost anyone, our experience continues to confirm that the quality of the group session is predominantly dependent on the facilitator."[39]

Cybersecurity in the Boardroom

It is evident that boardroom involvement in cybersecurity initiatives is essential; this is not a new realization.[40] Involvement is more than just appointing a chief information officer (CIO) or IT department to deal with it. Sincere involvement in and commitment to common business management processes, such as meetings are required, especially since knowledge management becomes the focal point in meetings about information security. Making the right decisions depends on the active generation, capture and sharing of knowledge during meetings at the top levels of the organization, especially during meetings that have the objective of formulating viewpoints on items that justify the entire decision-making process. In boardrooms, this becomes increasingly important because the individual board member needs to form his/her own meaning and opinion on a certain topic in order to make a valuable and justified decision.[41]

The aforementioned university research indicates that using GSS can make meetings about prioritizing information security practices very productive.

> *"This paper describes the application of Group Support Systems (GSS) in the field of Business Information Security Governance (BISG). The focus is on longitudinal small team collaboration—for instance within Boards of Directors (BoD), Management Teams and groups of experts—with large amounts of items…It shows how GSS can play a facilitating role in small team collaboration to process and assess large amounts of data in order to make qualified decisions."*[42]

There is an increasing demand to evaluate, direct and monitor (EDM)[43] cybersecurity initiatives at the board level to create broader understanding of this complex topic. The complexity, as well as the huge number of topics related to the information security domain, increases the necessity to create transparency about the basic level of knowledge that is required within boards and how to maintain and further develop it.[44] This is necessary so board members have a clear level of understanding of what they need to know.

An example of topics on the agenda of a board session on cybersecurity is displayed in **figure 2**. This is a screenshot of the GSS agenda. In this example, the board members participate in a session to assess the asset values and score the vulnerabilities these assets pose. The outcome is a set of critical assets on which they can prioritize their investments in cybersecurity initiatives. This provides the CISO, for one, with clear direction.[45]

Information Security as an Integrated Business Practice

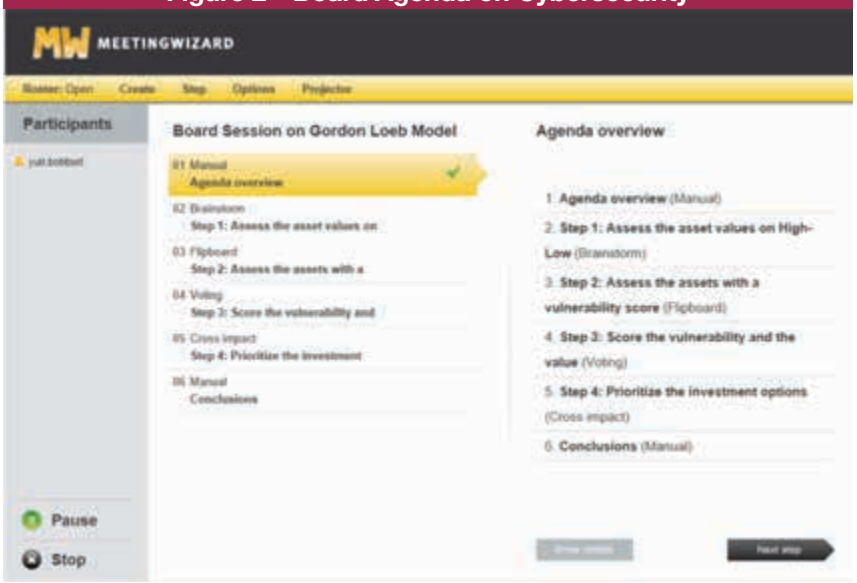
Information security is increasingly becoming an integrated business practice instead of just IT. Information security academic literature emphasizes the necessity to govern information security at the level of the board of directors (BoD) and to execute it (i.e., plan, build, run and monitor) at the management level. GSS is a powerful and novel instrument to discuss and prioritize complex items such as information security practices. The distilled core practices (figure 3) for BoDs, derived via GSS, present a core set of carefully selected and prioritized information security governance practices and thereby reveal the power of GSS in knowledge sharing and decision-making processes. These strategy elements, based upon SPRM, are successfully applied by numerous organizations. These 10 practices function as a frame of reference for BoDs and management teams to gain knowledge consensus and facilitate the decision-making process in order to improve the maturity level of business information security.[46, 47]

In addition to use within academic environments, GSS has proven itself in practice. For example, hundreds of sessions at the Boeing aircraft corporation with 654 participants in 82 GSS sessions, IBM with 441 participants in 55 GSS sessions, Nationale Nederlanden with 414 participants in 41 GSS sessions, where knowledge management and thorough decision making on safety and security are crucial, have successfully used GSS.[48]

From Strategy to Operations

A potential use for GSS in relation to BIS could be for organizations to apply a cyberthreat perspective to the analysis and prioritization of BIS strategy. The strategic forces model appears to be suitable for use in GSS to assess the strategic cybersecurity forces in a group.[49, 50] Examples of forces can be cybercriminals, states and terrorists. Discussing these forces and prioritizing the necessary measurements and investments of improvement[51] can be done via GSS. For example, translating the

Figure 2—Board Agenda on Cybersecurity



Source: Y. Bobbert and J. B. F Mulder. Reprinted with permission.

Figure 3—Top 10 Governance Practices and Critical Success Factors for Business Information Security				
#	Governance Practice and/or Critical Success Factor Description	Score	Level	SPRM
1	**Determine roles.** Accountability and responsibility for BIS at the board and executive management levels, including the role of the stakeholders	11.25	Governance	Structure
2	**Corporate internal communication** on cyber downsides, e.g., cybercrime, fraud, theft, forgery, piracy, bullying. Internal communication channels such as intranet, human resources management (HRM) letters and workshops can be used to educate employees	11.25	Management	Relational mechanism
3	**Awareness** at the board level about business risk, business-critical information, level of IT dependency, and types of threats from outside and inside	11.00	Management	Relational mechanism
4	**Board and senior management leadership**, such as leading by good example, having a clean desk policy, limiting personal web exposure (personal blogging, video), and forbidding software piracy and shredding confidential papers	11.00	Governance	Relational mechanism
5	**Lessons learned.** Lessons are discussed during sessions after security incidents. Incidents are documented and reported, as well as the kind of response made to the stakeholders and how such an event can be prevented. These should be taken into consideration for the formulation of a strategy.	11.00	Governance	Process
6	**Transparency.** The company should also consider the need for a confidential reporting process (whistle-blowing) covering fraud and other risk.	10.75	Governance	Process
7	**Determine risk appetite.** The level of risk and exposure a company is willing to take when it comes to information security risk. It is used to justify decision making on investments/insurance	10.25	Governance	Process
8	**Internal control.** Processes and procedures should be regularly reviewed to ensure the effectiveness of the internal systems of control so that the organization's decision-making capability and the accuracy of its reporting and financial results are maintained at a high level at all times.	10.00	Management	Process
9	**Regular reporting** on security adequacy and effectiveness, including regular reports from management on the program's adequacy and effectiveness	10.00	Management	Process
10	**Ensuring the integrity of the corporation.** The accounting and financial reporting systems, including the independent audit, must be effective. Appropriate systems of control must be in place, in particular, systems for risk management, financial and operational control, and compliance with the law and relevant standards.	9.75	Management	Process

Source: Y. Bobbert and J. B. F Mulder. Reprinted with permission.

threat actors (which can be perceived as forces) identified by the National Cyber Security Centre in The Netherlands (**figure 4**) to effective measures that protect critical assets no longer comes from theoretical books but from the collective brain of the group.[52]

Figure 4—Threat Actors

- Professional cybercriminals
- States
- Terrorists
- Cybervandals
- Hacktivists
- Internal actors
- Cyber researchers
- Private organizations

Source: National Cyber Security Centre, The Netherlands, 2015. Reprinted with permission.

Conclusion

By making use of knowledge facilitation technologies such as GSS, in combination with an experienced facilitator, board members can prioritize more effectively and meetings can become more pleasant and efficient. The list of 10 core practices noted in **figure 3** enables boards to set strategic directives and collect viewpoints and voices of all parties within the business, in addition to IT. GSS can support bringing more insights into these viewpoints, eliciting the right level of urgency and collecting the evidence during the meeting. This substantiates a smart decision-making process.[53]

By achieving a mutual level of knowledge, directors and managers are able to strip away the jargon of the security professionals and focus on the essence. This better prepares them to take the heat once they are exposed to an escalated threat. Proven technology and theory such as double-loop learning provide managers with more understanding so they can fully take responsibility and ownership and, as a result, perceive information security as an integrated business practice instead of an *ad hoc* practice.

“By achieving a mutual level of knowledge, directors and managers are able to strip away the jargon of the security professionals and focus on the essence.”

References

Gordon, L.; M. Loeb; “The Economics of Information Security Investment,” *ACM Transactions on Information and System Security*, vol. 5, no. 4, 2002, p. 438-457.

Gordon L. L. M.; T. Sohail; “Market Value of Voluntary Disclosures Concerning Information Security,” *MIS Quarterly*, vol. 34, no. 3, 2010

Solms, B.; “Corporate Governance and Information Security,” *Computers and Security*, vol. 20, 2001, p. 215-218

Gordon, L.; M. Loeb; “The Economics of Information Security Investments,” *ACM Transactions on Information and System Security*, vol. 5, no. 4. 2002, p. 438-457

Day, G.; "Cybersecurity for Small Businesses," 23 October 2009, *small business.uk.reuters.com*.

Calder, A.; Implementing Information Security Based on ISO 27001/ISO 27002, Zaltbommel: Van Haren Publishing, 2009

ITGI, "Aligning COBIT 4.1, ITIL V3, ISO/IEC 27002 for Business Benefit," IT Governance Institute and OGC, United Kingdom, 2008

Von Solms, B.; R. Von Solms; "The 10 Deadly Sins of Information Security Management," *Computers & Security*, South Africa, 2004.

Sveena, F.; J. Torresa; J. Sarriegia; "Blind Information Security Strategy," *International Journal of Critical Infrastructure Protection*, vol. 2, 2009, p. 95-109

Pfeffer, J. S. R.; *The Knowing Doing Gap: How Smart Companies Turn Knowledge into Action*, Harvard Business School Press, USA, 2001

Meyer, B.; R. De Wit; *Strategy Synthesis: Resolving Strategy Paradoxes to Create Competitive Advantage*, Thomson, UK, 2005

De Haes, S.; W. Van Grembergen; "Practices in IT Governance and Business/IT Alignment," *ISACA® Journal*, vol. 2, 2008

De Haes, S.; W. Van Grembergen; *Enterprise Governance of IT: Achieving Strategic Alignment and Value*, Springer, USA, 2009

ISACA, *COBIT® 5 for Information Security*, ISACA, USA, 2012

ISACA, *Controls and Assurance in the Cloud: Using COBIT® 5*, ISACA, USA, 2014

Endnotes

1 Elsayed-Elkhouly, S.; H. Lazarus; "Why Is a Third of Your Time Wasted in Meetings?" *Journal of Management Development*, vol. 16, no. 9, 1997, p. 672

2 Kayser, T.; *Mining Group Gold, Third Edition: How to Cash in on the Collaborative Brain Power of a Team for Innovation and Results*, McGraw-Hill Education, USA, 2010

3 Riabacke, A.; "Managerial Decision Making Under Risk and Uncertainty," *IAENG International Journal of Computer Science*, vol. 32-4, 2012

4 Hu, Q.; T. Dinev; P. Hart; D. Cooke; "Managing Employee Compliance With Information Security Policies: The Critical Role of Top Management and Organizational Culture," *Decision Science*, vol. 43, no. 4, 2012, p. 615-660

5 Solms, V.; "From Information Security to Business Security," *Computer and Security,* Elsevier, South Africa, 2005

6 ISACA, *An Introduction to the Business Model for Information Security*, USA, 2009

7 *Op cit*, Solms

8 Bobbert, Y.; *Maturing Business Information Security,* Utrecht: IBISA, 2010

9 Kluge, D.; S. Sambasivam; "Formal Information Security Standards in German Medium Enterprises," *Conisar*, 2008

10 Sanchez, L.; A. Santos-Olmo; E. Fernandez-Medina; M. Piattine; "Security Culture in Small and Medium-Size Enterprises," *Communications in Computer and Information Science*, vol. 110, 2010, p. 315-324

11 W. Flores, W.; E. Antonsen; M. Ekstedt; "Information Security Knowledge Sharing in Organizations: Investigating the Effect of Behavioral Information Security Governance and National Culture," *Computers and Security*, vol. 43, 2014, p. 90-110

12 Siponen, M.; R. Willison; "Information Security Management Standards: Problems and Solutions," *Information and Management,* vol. 46, 2009, p. 267-270

13 da Veiga, A.; N. Martins; "Improving the Information Security Culture Through Monitoring and Implementation Actions Illustrated Through a Case Study," *Computers and Security*, vol. 49, 2014, p. 162-176

14 Straub, D.; R. Welke; "Coping With Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly,* vol. 22, no. 4, 1998, p. 441-469

15 Miranda S.; R. Bostrom; "Meeting Facilitation: Process Versus Content Interventions," *Proceedings of 30th Hawaii International Conference on System Sciences*, Institute of Electrical and Electronics Engineers, 1997

16 Pai, J.; "An Empirical Study of the Relationship Between Knowledge Sharing and IS/IT Strategic Planning (ISSP)," *Management Decision*, vol. 44, 2006, p. 105-22
17 Romano, N.; J. F. Nunamaker; "Meeting Analysis: Findings From Research and Practice," *Proceedings of 34th Hawaii International Conference on System Sciences*, Institute of Electrical and Electronics Engineers, 2001
18 *Ibid*.
19 *Op cit,* Elsayed-Elkhouly and Lazarus
20 Vreede, G.; J. Boonstra; F. Niederman; "What Is Effective GSS Facilitation? A Qualitative Inquiry Into Participants' Perceptions," *Proceedings of 35th Hawaii International Conference on System Sciences*, Institute of Electrical and Electronics Engineers, 2002
21 Newby, R.; G. Soutbar; J. Watson; "Comparing Traditional Focus Groups With a Group Support Systems (GSS) Approach for Use in SME Research," *International Small Business Journal,* vol. 21, no. 4, 2003, p. 421-433
22 Hengst, M.; M. Adkins; S. van Keeken; A. Lim; "Which Facilitation Functions are Most Challenging: A Global Survey of Facilitators," *Proceedings of the Group Decision and Negotiation Conference,* 2005
23 Dennis, A. R.; J. S. Valacich; J. F. Nunamaker; "An Experimental Investigation of the Effects of Group Size in an Electronic Meeting Environment," *IEEE Transactions on Systems, Man, and Cybernetics,* vol. 20, no. 5, 1990, p. 1049-1057
24 Double-loop learning entails the modification of goals or decision-making rules in light of experience. The first loop uses the goals or decision-making rules, the second loop enables their modification, hence double loop. Double-loop learning recognizes that the way a problem is defined and solved can be a source of the problem.
25 Kolfschoten, G.; J. Nunamaker; "Collaboration Support Technology: Patterns of Successful Collaboration Support Based on Three Decades of GSS Research," *Collaboration Science, Technologies, Processes and Applications, Advances In Management Information Systems*, no. 3, 2014
26 Kolfschoten, G; J. B. F. Mulder; H. Proper; "De fata morgana van Group Support Systemen," *Informatie*, vol. 4, no. 5, 2016, p. 10-14
27 Fjermestad, J.; S. Hiltz; "Group Support Systems: A Descriptive Evaluation of Case and Field Studies," *Journal of Management Information Systems,* vol. 17, no. 3, 2001, p. 115-159
28 Snel, A.; J. B. F. Mulder; A. Van der Niet; "Group Support System," *Opsporing Belicht, Politieacademie*, Vols. Lectoraat Criminaliteitsbeheersing & Recherchekunde, 2011
29 Mulder, J. B. F.; *et al*, "New Applications of Group Support Systems, Group Decision and Negotiation," University of Vienna, Austria, 2005
30 *Op cit*, Sanchez, Santos-Olmo, Fernandez-Medina, Piattine
31 Bobbert, Y.; J. B. F. Mulder; "Governance Practices and Critical Success Factors Suitable for Business Information Security," *Proceedings of International Conference on Computational Intelligence, Communication Systems and Networks*, Institute of Electrical and Electronics Engineers, 2015
32 Nonaka, I.; "A Dynamic Theory of Organizational Knowledge Creation," *Organization Science*, vol. 5, no. 1, 1994, p. 14-37
33 Lebek, B.; J. Uffen; M. Neumann; B. Hohler; M. Breitner; "Information Security Awareness and Behavior: A Theory-based Literature Review," *Management Research Review*, vol. 12, no. 37, 2014, p. 1049–1092
34 Rutkowski, A.; B. van de Walle; G. van den Eede; "The Effect of Group Support Systems on the Emergence of Unique Information in a Risk Management Process: A Field Study," *Proceedings of 39th Hawaii International Conference on System Sciences*, Institute of Electrical and Electronics Engineers, 2006
35 *Op cit,* Pai
36 *Op cit,* Solms
37 Murray Turoff refers to this "decibel law" as the Asch Effect. Solomon Asch studied if and how individuals yielded to or defied a majority group and the effect of such influences on beliefs and opinions.

38 Altier, W. J.; "Process Expertise—A Critical Managing Fundamental," *Business Horizons*, vol. 36, 1993, p. 10-15
39 *Op cit,* Pai
40 *Op cit,* Hu, Dinev, Hart and Cooke
41 *Op cit,* Miranda and Bostrom
42 Bobbert, Y.; J. B. F. Mulder; "Group Support Systems Research in the Field of Business Information Security: A Practitioners View," *Proceedings of 46th Hawaii International Conference on System Science*, Institute of Electrical and Electronics Engineers, 2013
43 EDM refers to the *COBIT® 5 for Information Security Governance Process*, Evaluate, Direct and Monitor.
44 *Op cit,* Miranda and Bostrom
45 Gordon, L.; M. Loeb; "You May Be Fighting the Wrong Security Battles," *The Wall Street Journal,* 26 September 2011
46 SPRM refers to the strategic elements, to establish a competative advantage, from De Wit and Meyer. This distinction is applied by numerous studies at Antwerp Management school by Steven De Haes and Wim van Grembergen and later on integrated into *COBIT 5 for Information Security* and its derivatives for assurance and cloud.
47 *Op cit,* Bobbert and Mulder
48 de Vreede, G.; D. Vogel; G. Kolfschoten; J. Wien; "Fifteen Years of GSS in the Field: A Comparison Across Time and National Boundaries," *Proceedings of the 36th Hawaii International Conference on System Sciences*, Institute of Electrical and Electronics Engineers, 2002
49 Porter, M.; "How Competitive Forces Shape Strategy," *Harvard Business Review*, March 1979
50 Bobbert, Y.; "Porter's Elements for a Business Information Security Strategy," *ISACA® Journal*, vol. 1, 2015, *www.isaca.org/Journal/archives*
51 Bobbert, Y; A. Niet; "Cybersecurity in the Boardroom," *Oracle Innovation in Government Day*, Erasmus University, Rotterdam, The Netherlands, 2015
52 Turoff, M.; S. Hiltz; H. Cho; Z. Li; Y. Wang; "Social Decision Support Systems," *Proceedings of 35th Hawaii International Conference on System Sciences*, Institute of Electrical and Electronics Engineers, 2002
53 Pfeffer, J. S. R.; R. I. Sutton; "Evidence-based Management," *Harvard Business Review*, January 2006