Issues in Information Systems
Volume 16, Issue III, pp. 191-198, 2015

CYBERSECURITY: CHALLENGES FROM A SYSTEMS, COMPLEXITY, KNOWLEDGE MANAGEMENT AND BUSINESS INTELLIGENCE PERSPECTIVE

Susan M. Tisdale, Robert Morris University, smtst173@mail.rmu.edu

ABSTRACT

Information systems continue to be plagued by cybersecurity breaches. These breaches are increasing in number, complexity and severity often affect economic interests, local and national security and intellectual property. Many solutions address the information technologies themselves and how best to secure the system. A systems, holistic, approach considers cybersecurity from a business, social and information technology perspective. It also considers complexity and the organizational dynamics and interrelationships of multiple different stakeholders that exist at the strategic, managerial, and operational levels of the organization. These entities must work together in a timely and efficient manner. Business Intelligence and Analytics provides a set of methodologies and tools to help identify and manage the considerable amounts of knowledge necessary to make appropriate, timely, cybersecurity decisions to prevent or limit these beaches.

Keywords: Cybersecurity, Information Technology, Knowledge Management, Business Intelligence, Business Analytics

INTRODUCTION

In May 201, the Ponemon Institute published their tenth study on the cost of data breaches. The study showed the total cost of data breaches increased from $3.5 million dollars in 2014 to $3.79 million in 2015 [15]. In November of 2014, Sony Pictures' information systems were allegedly hacked by North Korean operatives or possibly by the malicious activities of a company insider, exposing trade secrets and embarrassing personal e-mails. Two retail companies, Home Depot and Target, were victims of two of the largest breaches in customer credit card information in 2014 and 2013, costing them millions of dollars in revenue and consumer confidence. Economic impact is not the only consequence from cyber-attacks.

Problems with cybersecurity are typically examined from the technical, information technology, perspective. More recent research calls for a comprehensive approach that considers business objectives, governance, and risk management along with organizational psychology and other factors such as those described in the Clinger-Cohen Act. Systems and Complexity Theory argue that issues should be addressed from all aspects of an organization and at all levels. Given the amount of data, perishability of data, technology turnover, and the multitude of stakeholders and information involved, cybersecurity is particularly a Knowledge Management problem. Business Intelligence and Analytics offer some methodologies and tools to address these challenges. This paper examines cybersecurity from these perspectives.

BACKGROUND

Arguments for a Comprehensive Approach to Cybersecurity

To address cybersecurity shortfalls, research is emerging to suggest a more holistic approach is needed. Atoum, Otoom, and Abu Ali (2014), found cyber security framewords are fragmented, vary in effectiveness, and a holistic approach is needed. Hughes and Cybenko [11], found most technical cybersecurity solutions failed to consider cost, operational tradeoffs, and the ability of adversaries to adapt to vulnerabilities. Previously established security protocols, like the Orange Book, are difficult to keep pace with system complexity and procurement approaches [11].

Jirasek states, "information security is a part of information risk management, which in turn has a place in business risk management" [12]. The author describes a model that addresses security drivers, security management and stakeholders. The security drivers include the laws and regulations that the organization must comply to; the

business objectives and information that must be protected; and security threats. Stakeholders are the receivers of the information contained in the business objectives and the people protecting that data. Security management is the largest driver and includes policy, cybersecurity control standards and other artefacts such as system architectures. Included in this is an assessment of risk and quantifying exposure to risk and security threats from attackers [12]. Klaus states cybersecurity is inter-disciplinary and should consider "technology, economics, usability, and psychology" (Klaus, 2013, p. 6). Bunker states, "security needs to be taken into account in every IT activity, but it has to match the requirements and needs of the business" [5]. He describes three control groups: "strategic controls, such as business alignment and governance; risk and compliance; operational controls, including physical security; back-up and incident handling and response; and tactical controls, such as secure builds, anti-virus and intrusion prevention" [5].

Economics and cyber security has emerged as a new discipline in the 21st Century. Anderson, et al., [1], discuss direct, indirect, and defense costs associated with cybercrimes. This includes direct theft, loss of revenue due to a lack of consumer confidence, and traditional cyber defenses costs such as firewalls and antivirus protection. Thomas, Antkiewicz, Florer, Widup and Woodyard [17] examined frameworks and models that considered the cost of recovery and restoration as well. Anderson and Moore's [2] research on economics and information security further suggests cybersecurity should address: (1) designing systems to remove risky behavior; (2) designing systems that considers human psychology, criminal behavior, and warfare; and (3) determining the type of institutions that can manage complex interconnected systems.

These various viewpoints suggest a holistic approach to cybersecurity management that considers business objectives and alignment; governance; laws and regulations; economics, risk management; technology, psychology and criminology, to name a few. Holistic approaches have its foundation in Systems Theory. The dynamically changing cyber environment in the 21st Century also suggests that Complexity Theory/Complexity Leadership Theory can inform the cybersecurity management process.

Systems and Complexity Leadership Theory

Systems Theory is considered an interdisciplinary, cross-cutting meta-theory. Ludwig von Bertalanffy (1955) and Joseph Litterer (1969) formulated the hallmarks of the theory. These are the "interrelationship and interdependence of objects and their attributes…and holism" [16]. It also includes: (1) interaction between systems to achieve goals; (2) transforming systems to achieve the goal; (3) environmental and other disorderly factors on systems; (4) regulatory impact on systems; (5) system hierarchies and subsystems impact on the system; (6) differentiation among the subsystems; and (7) multiple/alternative ways to achieve system objectives (Skyttner, 2005). Systems Analysis applies to complex organizations and considers the "problems of identifying, reconstructing, optimizing, and controlling an organization, while taking into account multiple objectives, constraints and resources…possible courses of action, together with their risks, costs and benefits" [16].

Complexity Leadership Theory has grown in popularity in the 21st Century and late 20th Century as a way to address the dynamic interactions in a global economy where organizations and management styles need to adapt quickly to meet new challenges. Schneider and Sommers (2006) included non-linear dynamics, adaption, evolutions and the influence of chaos (Chaos Theory) in Complexity Theory. Early leadership and management theories that viewed the exchange of information between a leader and follower as simple will not provide the dynamics needed to optimize organizational performance [4]. "Leadership is not merely the influential act of an individual or individuals but rather is embedded in a complex interplay of numerous interacting forces" [19]. Uhl-Bien, Marion, and McKelvey also studied management within the Complexity Leadership Theory and identified the "entanglement of two roles: (1) creating appropriate organizational conditions (or enabling conditions) to foster effective adaptive leadership in places where innovation and adaptability are needed, and (2) facilitating the flow of knowledge and creativity from adaptive structures into administrative structures. Enabling leadership occurs at all levels of the organization (as well as within the adaptive dynamic), but the nature of this role will vary by hierarchical level and position…" [19]. Clarke [7] adds that the leadership process is autocatalytic and leaders must also consider how they shape cultures, structures and context.

These two theories point toward cybersecurity as a multi-dimensional, multi-disciplinary, issue that is subject to constant, complex, changes. Systems Theory is valuable in identifying the multidisciplinary cybersecurity

stakeholders, functions, and information and Complexity Leadership Theory, the dynamic exchanges needed between and among the stakeholders. However, these approaches are not the only underlying forces to address. The amount and time sensitivity of the data produced by these entities, internal and external to an organization, highlights the importance of Knowledge Management, to gather and distribute the information, and Business Intelligence and Analytics, to organize and understand the contents of the data.

Knowledge Management and Business Intelligence and Analytics

Cybersecurity is typically not considered a Knowledge Management or Business Intelligence issue. However, the role it should play in cybersecurity is significant. Cybersecurity is more than just the technologies. It is the business processes and information, including intellectual property that is the target of the attacker. The attack may also be for financial gain or philosophical embarrassment. Attackers exploit weaknesses in the information technology but also through individuals. This makes all parts of an organization vulnerable. As a result, everyone becomes a stakeholder in cybersecurity. Through Knowledge Management and Business Intelligence and Analytics, an organization can capture and understand their mission threads, information, intellectual property and connect the stakeholders to the information systems and data. Knowledge, however, is more than information.

Knowledge "is a fluid mix of framed experience, values, contextual information, and expert insight that provides a framework for evaluating and incorporating new experiences and information…In organizations, it often becomes embedded not only in documents or repositories but also in organizational routines, processes, practices, and norms" [8] Further, it includes information technology capabilities, artifacts, its usage, impact and methodological, managerial and operational processes [20].

These processes and information exist at an organization's strategic, tactical and technical/operational levels [20].. Likewise, every organization possesses various cultural layers and each person brings those different perspectives to the organization [10]. Knowledge is best achieved when embedded in an organization's culture, individual behavior and daily operations that, in turn, is linked to the work processes [8] It considers cross-functional knowledge between business groups and divisions with working groups and operational knowledge (USAID, 2013). Finally, it exists in "a social-technical context that cannot be separated from the involved information technology" (vom Brocke et al., 2011, p. 394). To manage knowledge, the organization needs a set of rules (roles and skills) to capture, distribute and manage the information. The tools and techniques that capture and analyze this data constitutes Business Intelligence and Analytics.

Business Intelligence "is an umbrella term that combines architectures, tools, databases, analytical tools, applications and methodologies"…with the objective "to enable interactive access (sometimes in real time) to data, to enable manipulation of data, and to give business managers and analysts the ability to conduct appropriate analysis" [18]. It helps a business to understand its market and to make timely business decisions [6]. However, it is becoming increasing difficult to process and analyze the vast amount of cybersecurity and threat data and there is no consistent framework to analyze the data [6]. This makes the development of cybersecurity business intelligence and analytic processes and procedures time critical.

Before Knowledge Management and Business Intelligence and Analytics can mature in the cybersecurity management field, an understanding of what constitutes a comprehensive view of cybersecurity management is needed. Then, these functions can be mapped in a Business Intelligence and Analytic framework. This is the next focus of the paper.

DISCUSSION

So far, this paper has highlighted the severity and growing concern with cybersecurity breaches; the necessity to examine cybersecurity from a holistic and complex perspective; and that tools and techniques are needed to organize, analyze and share the vast amount of information needed to manage cybersecurity among the stakeholders. But who are the organizational stakeholders and the factors? The Clinger-Cohen Act of 1996 is one of the first system approaches to information technology management.

As a result of The Clinger-Cohen Act of 1996, the US Government Federal Chief Information Officer's Council [9], developed a set of best practices based on requirements stated in the 2012 Clinger-Cohen Core Competencies and Learning Objectives. Theses competencies include: (1) policy and organization; (2) leadership and human capital management; (3) organizational development; (4) information resources strategy and planning; (5) information technology performance assessment models and methods; (6) project scope and requirements management; (7) Capital Planning and Investment Control; (8) acquisition; (9) information and knowledge management; (10) cybersecurity/information assurance; (11) enterprise architecture; and, (12) technology management and assessment. Although these competences address information technology management, the interdependent nature of Systems Theory suggests cybersecurity can also be viewed at from all these perspectives.

By applying the concepts discussed above, a taxonomy begins to emerge that shows the stakeholders and factors. Figure 1, below, represents this taxonomy. Note that there are two way arrows to show how each informs the other and in a synergistic way.

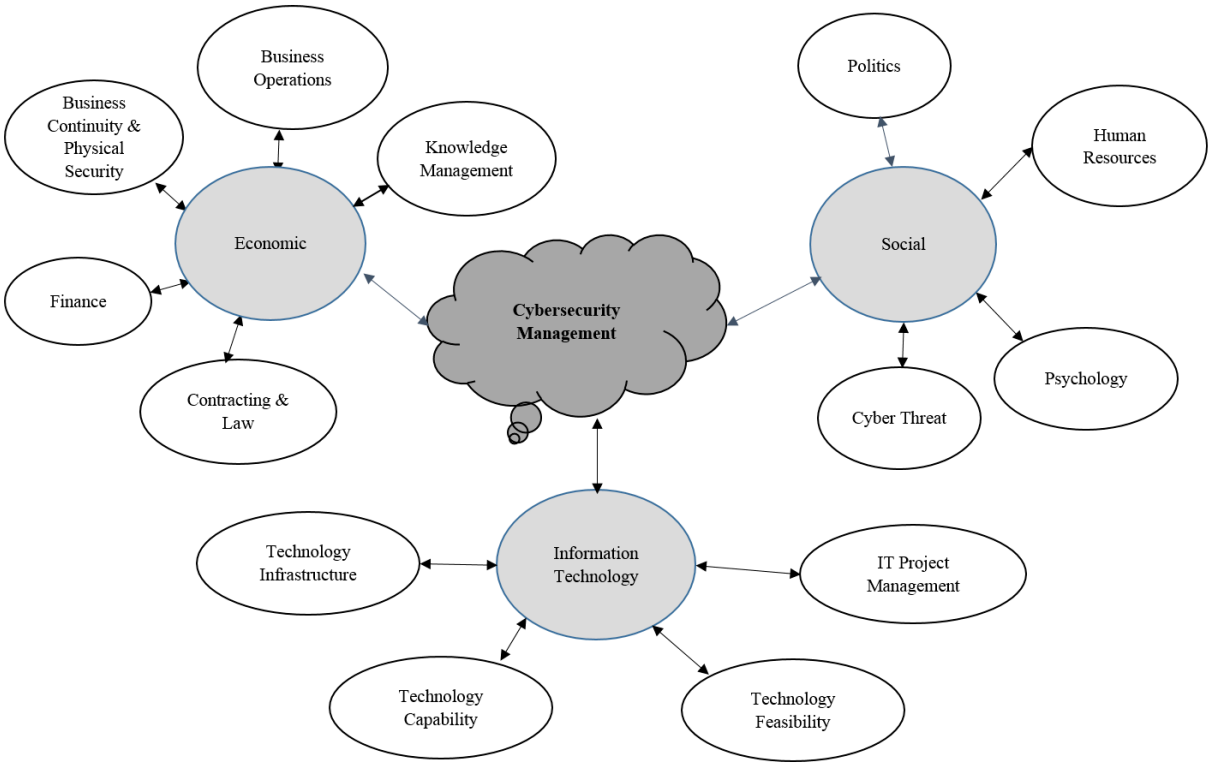

Figure 1. Cybersecurity Management Taxonomy

Policy and organization includes a department or agencies' mission; function; organization; policies; procedures; governing laws; decision making processes; organizational interrelationships; and, intergovernmental programs, processes and policies. Leadership and human capital management include leadership attributes; career development and planning; performance and personnel management; and, retaining a competent information technology workforce.

Process and change management includes organization development; process management; quality improvement; business process reengineering; and, cross-boundary collaboration. Information resource planning and strategy includes a baseline assessment; interdependency analysis; information technology planning; contingency planning; and evaluation techniques and monitoring. Information technology performance assessment models and methods

looks specifically at Government Performance and Results Act compliance, decision making, and measuring information technology success.

Information technology program and project management looks at requirements management; integration; time, cost and performance; quality, risk and lifecycle management; software development and testing; vendor management; and program management leadership. Capital Planning and Investment Control examines cost, benefit, and risk analysis and methods; business case analysis; and, portfolio management.

Acquisition covers strategies, methodologies, contract management, supply chain management and best practices. Information and knowledge management includes privacy and personal data protection; information accessibility; records and information management; knowledge management; social media, web strategy and maintenance; information collection; and, open government initiatives.

Cybersecurity and information assurance addresses roles and responsibilities; governance; strategies and plans; threats and vulnerabilities; security control planning and management; risk management; enterprise management; incident reporting; and, disaster recovery and critical infrastructure protection. Enterprise architecture incorporates governing frameworks, functions and concepts; development and maintenance; use of architectures in investment decision making; data management; and performance measurement.

Lastly, technology management and assessment considers network and telecommunications, including mobile devices; spectrum management; computer systems; web technology; data management and software development technology; cloud computing; and special use and emerging technology. This also includes the outsourcing of technologies and the aspects that must be managed in these circumstances.

Stakeholders include business leaders, business continuity, contract and finance managers, attorneys, human resource and knowledge management professionals, law enforcement, organizational psychologists, and information technology professionals, etc… both internal and external to the organization. Each of these individuals and groups come with their unique professional and personal languages, cultures and experiences. Political dynamics also make cybersecurity a local, national and global problem.

It is a challenge to characterize a cybersecurity management framework that considers stakeholders and factors (Systems Theory), the complex and dynamic interaction that is needed among them (Complexity Theory) and the tools and techniques needed to bring them together (Knowledge Management and Business Intelligence). All this, as well as considering that each layer of an organization plays a role. Figure 2 attempts to show these relationships.

Systems Theory sees the organization from the economic perspective (operations, continuity of operations, finance, legal…), social perspective (human resources, organizational dynamics, politics, threats, etc…) and information technology perspective (the technical infrastructure, technical capabilities, etc…). Complexity Theory adds the multi-layer, strategic, management and operational levels, to the picture. All levels inform each other and to varying degrees depending on the circumstances. As the System and Complexity Theories suggest, the factors and levels are connected and not linear. They can occur in a situation of uncertainty and chaos. With the speed of technology and knowledge sharing, perishability is critical.

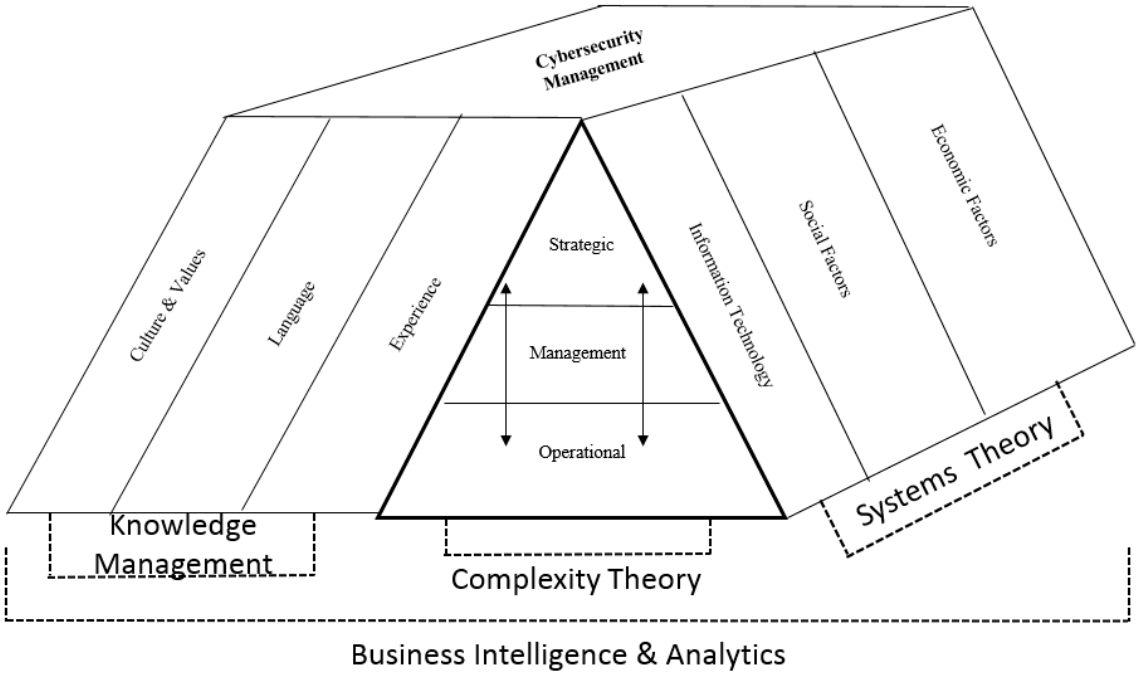

Figure 2. A Cybersecurity Management Framework

To manage the knowledge, leaders need to engage at the appropriate time, with the appropriate information and with the appropriate resources. For example, the budget, contracting, and program management functions can link valuable project and financial information at the appropriate time in the business or operational lifecycle. Databases and incident responses can correlate the threat information and security mitigation strategies to the vulnerable business processes and information systems, also at the appropriate time. Note in Figure 2, that there are two way arrows. This is to emphasize that each layer informs the other and that, at any particular time, one organizational level may become the driving force in a decision. For example, a security breach may result in operational considerations taking precedence over day-to-day tasks or strategic decisions in order to fix a critical vulnerability, regardless of cost or schedule.

Rapid technology and information turnover make understanding and processing information in a timely manager challenging under the best of circumstances. Although Business Intelligence and Analytics provides the methodologies and tools to help meet this challenge, there is also an issue with data accuracy and associated business functions and systems, especially in large, complex and distributed organizations. What appears to be a simple and straight forward task is not. Business functions may differ from location to location and at the level in an organization, especially in international companies. For example, logistics at an organizational level may look at strategic needs and desires whereas at the operator level, it will be on obtaining resources. For cyber and mission assurance, it is about securing the supply chain. Each function and level has different information needs and requirements and at different times. Mapping these functions to the associated data and system and prioritizing them can be daunting.

Davenport and Prusak [8] provide suggestions on how to design and build knowledge systems. To build the repository, they suggest starting with the business problem and identifying information of high value to the organization and include technical, organizational, and cultural influences. However, it may become too costly and time consuming to manage a knowledge systems in a dynamically changing environment, especially if the organization is large and complex. Information can soon be outdated before all of it is accurately captured.

Regardless of the approach, the most important factor is that knowledge is shared throughout the organization. Creating knowledge networks and leaders is beneficial, but only if information and feedback is pushed to all layers of the organization. Leaders must understand the culture and encourage actions to move forward and change. They must adopt constructive attitudes and establish new relationships. Likewise, employees should be encouraged to share and manage their knowledge on a daily basis. Knowledge managers and senior people in the organization must have the skills to extract and manage knowledge across the corporation [8]. The knowledge manager should be skilled in multiple areas to help shape and manage the program and teach others. Finally, politics and other cultural sensitivities must be dealt with at all levels in the organization in order to effectively communicate.

CONCLUSIONS

Many organizational problems come down to knowledge. Cybersecurity is one area where knowledge is a challenge. There is a great deal of knowledge that must be understood and in a timely manner to make decisions. It involves multiple stakeholders who come from different groups, often with their own unique languages, cultures and standards. Most importantly, it is complex, involving a holistic approach in which most organizations would need some type of Business Intelligence and Analytic processes and tools to manage it. It can be a lack of knowledge, lack of sharing knowledge, not knowing how to share knowledge, or differing opinions about the knowledge. The individual or groups may not even be aware there is a problem.

To better manage cybersecurity, the following points should consider that: (1) the technology view of cybersecurity is not sufficient; (2) an organization should be viewed as a complex system; (3) employees, at all levels, must participate in the information management process and create and share information; (4) a cybersecurity knowledge manager, skilled in multiple organizational areas, could benefit an organization; and (5) cybersecurity functions and systems can be identified by starting with the business problem to identify information, its priority, and associated information systems. These points need further research to understand the comprehensive, complex nature of cybersecurity management and how best to secure information systems.

REFERENCES

1. Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. WEIS, 2012, 265-200, retrieved from weis2012.econinfosec.org/program.html.
2. Anderson, R., & Moore, T. (2006). The economics of information security. *Science*, *314*(5799), 610-613.
3. Atoum, I., Otoom, A., & Abu Ali, A. (2014). A holistic cyber security implementation framework. *Information Management & Computer Security*, *22*(3), 251-264.
4. Avolio, B., Walumbwa, F., & Weber, T. (2009). Leadership: current theories, research, and future directions. *Annual Review of Psychology*. 60, 421-49. doi: 10.1146/annurev.psych.60.110707.163621.
5. Bunker, G. (2012). Technology is not enough: Taking a holistic view for information assurance. *Elsevier* Information Security Technical Report 17, 19-25, retrieved from www.compeseconline.com/publications/prodinf.htm. doi:http://dx.doi.org/ 10.1016/j.istr.2011.12.002.
6. Chen, H., Chiang, R. H., & Storey, V. C. (2012). Business intelligence and analytics: From big data to big impact. *MIS quarterly*, *36*(4), 1165-1188.
7. Clarke, N. (2013). Model of complexity leadership development. *Human Resource Development International*, *16*(2), 135-150.
8. Davenport, T.H., & Prusak, L. (2000). *Working knowledge: how organizations manage what they know.* Boston MA: Harvard Business School Press.
9. Federal CIO Council. (2012). 2012 Clinger-Cohen core competencies & learning objectives. Retrieved from: https://cio.gov/wp-content/uploads/downloads/2013/02/2012-Learning-Objectives-Final.pdf
10. Hofstede, G., G. J., & Minkov, M. (2010). *Cultures and organizations: Software of the mind.* New York: McGraw.
11. Hughes, J., & Cybenko, G. (2013). Quantitative metrics and risk assessment: The three tenets model of cybersecurity. *Technology Innovation Management Review*, *3*(8).
12. Jirasek, V. (2012). Practical application of information security models. *Elsevier Information Security Technical Report 17*, 1-8. doi:http://dx.doi.org/10.1016/j.istr.2011.12.004.

13. Julisch, K. (2013). Understanding and overcoming cyber security anti-patterns. *Computer Networks*, *57*(10), 2206-2211.
14. Polanyi, M. (1966). *The tacit dimension.* Chicago: University of Chicago Press.
15. Ponemon Institute Research Report. (2015). 2015 cost of data breach study: global analysis. Ponemon Institute LLC, Michigan, Retrieved on 1 June 2015, from: ww.ibm.com/services/costofbreach.
16. Skyttner, L. (2005). *General Systems Theory: Problems, Perspectives, Practice*. Hackensack, NJ: World Scientific.
17. Thomas, R. C., Antkiewicz, M., Florer, P., Widup, S., & Woodyard, M. (2013). How bad is it?–A branching activity model to estimate the impact of information security breaches. WEIS, 2012, 265-200, retrieved from weis2012.econinfosec.org/program.html.
18. Turban, E., Sharda, R., Delen, D., & King, D. (2011). *Business intelligence: A managerial approach, 2nd ed.* Boston: Prentice Hall.
19. Uhl-Bien, M., Marion, R., & McKelvey, B. (2007). Complexity Leadership Theory: Shifting leadership from the industrial age to the knowledge era. *The Leadership Quarterly (18)4,* 298–318. doi:10.1016/j.leaqua.2007.04.002.
20. vom Brocke, Becker, J., Braccini, A., Butlens, R., Hofreiter, B., Kapociius, K., De Marco, M., Schmidt, G., Seidel, S., Simons, A., Skopal, T., Stein, A., Stieglitz, S., Suomi, R., Vossen, G., Wintger., R., & Wrycza, S. (2011). Current and future issues in BPM research: A european perspective from the ERCIS meeting 2010. *Communications of the Association for Information Systems*, 28(25), pp. 393-414.