EIRP 2019
THE 14TH EDITION OF THE INTERNATIONAL CONFERENCE
EUROPEAN INTEGRATION
REALITIES AND PERSPECTIVES

Digital Transformation of Managerial Accounting - Trends in the New Economic Environment

Florentina Raluca Bîlcan[1], Ionica Oncioiu[2], Dumitru Alexandru Stoica[3], Alina Stanciu[4]

Abstract: Fluctuations and changes in economic power poles, past financial crises, but also signs of new recession periods, rising capital, multiplying variables and cause-effect factors outline the current economic environment. As an important part of digital transformation, the influence of artificial intelligence in the process of managerial accounting represent the future of taking the best decisions in organizations. The aim of the present study is to explore digital transformation frontiers using the lens of cyber accounting that will help leaders to increase the organizational performance through a clear vision of economic implications of their decisions. The current research contributes both managerial accounting and digital transformation fields by cross-exploring each phenomenon and revealing how digital transformation shape the nature of cyberaccounting as a collaborative research area.

Keywords: digital transformation; cyberaccounting; cybersecurity

JEL Classification: D83; M41; O33

1. Introduction

The global economic entities are facing growing transformation pressures - moving from product-driven business models to new models focused on creating and capturing different sources of new value (Agrawal & Tapaswi, 2017; Tiago, Manoj & Espadanal, 2014; Lee & Kim, 2017). As a result, innovation is becoming more and more complex. The Fourth Industrial Revolution 4.0 rewrite the new global architecture: Globalization 4.0 developing technology, skills and new innovation. And this unprecedented, exponential shift of rhythm is increasingly based on collaborative platforms to achieve more radical innovations driven by shifts in technology (Gandino, Celozzi & Rebaudengo, 2017).

The performance of the digital enterprise has exceeded its profitability boundaries, and any development strategy involves the KPI’s performance indicators predictability and sustainability indicators, but also “digital platform business models, ecosystems and partnerships, as the important angles of responsibility, trust and governance, from multiple levels - corporate, national and international” (Katzenbach & Smith, 2015). Under the action of these forces the new performance concept is divided into three pillars of action: Sustainable Performance, Finding & Retaining Talents, as a source of added

[1] Lecturer, Valahia University, Romania, Address: Targoviste, Romania, Tel.: +40245206101, Corresponding author: bilcan.florentina.raluca@gmail.com.

[2] European Academy of the Regions, Belgium, Address: Brussels, Belgium, Tel.: +32 478 27 82 53, E-mail: nelly_oncioiu@yahoo.com.

[3] PhD student, Valahia University, Romania, Address: Targoviste, Romania, Tel.: +40245206101, E-mail: dumitru.alexandru.stoica@ gmail.com.

[4] PhD student, 1 Decembrie 1918 University, Romania, Address: Alba Iulia, Romania, Tel.: +40-0258-806130, E-mail: alecse.alina@gmail.com.

value in a global competitive market, and Research & Innovation. “High Performance Organizations” which “record exceptional financial results, have satisfactory customers and employees, high productivity, encourage innovation and leadership” are the result of their evolution, trough digital transformation in a Digital Economy (Wang & Hu, 2014).

To better understand why is necessary to develop a structured process of information security risk within the organization, it must be borne in mind that, regardless of the type of organization, the field of activity or form of organization, there is uncertainty both in organization and in the environment in which it operates (Andress, 2003; Stepchenko & Voronova, 2015). The uncertainty may take the form of either threats or opportunities. In this contest, each manager must handle threats, because otherwise the organization’s objectives cannot be met, and, on the other hand, capitalize the opportunities to the benefit of the organization, proving efficiency (Collins & McCombie, 2012; Karim, 2007). Given that uncertainty is a fact of life, then the uncertainty response should become a permanent managerial concern (Landoll, 2010; Karanja, 2017).

Another aspect of knowledge management in the open digital era is a technology itself and opportunities it opens for better knowledge use. Thus, in the world of the rapid adoption of online communication, interactions and knowledge sharing, the question of cyber security technology adoption is indisputably important. Modern security-related technologies for, name a few, securing transmissions, verifying identities, enabling the safety of data, asymmetric encryption and digital certificates are more and more demanding by companies with open business models involving peer-to-peer communication and various stakeholders’ interactions (Gandino, Celozzi & Rebaudengo, 2017).

The present research contributes to the understanding of cyberaccounting evolution through the lens of digital technologies development and their ubiquitous nature. The paper also contributes to the understanding of the digital transformation process happening in conditions of knowledge sharing and managerial accounting boundaries. The results presented in this paper can be used for mapping future research agenda or for contributing to the identified research topics. Finally, the research can have managerial implications for leaders by synthesizing knowledge on the cyberaccounting topic, shedding light on opportunities and challenges of the managerial accounting and digital technologies synergy, and analyzing in depth the most influential papers and findings.

2. Managerial Accounting in the Open and Digital Era

2.1. Impact of Digital Transformation on Business

The complete digitization of economic environment change the way that leaders of the future relate with their business (McQuade, 2006; Yang, Wu & Wang, 2014). Leading technologies, Artificial Intelligence (AI), Internet of Things (IoT) involve all the levels of the business, all the functions and all the stakeholders, transforming “the structures of economic interaction: the twin trends of digitization and virtualization are creating an economy of near-unlimited mobility in which cyberspace is home to all data” (Chen, Ge & Xie, 2015), including indicators, accounting and global financial data. Reports, Charts, Technical Indicators, Trend Analysis, Research, Cloud Computing and Mobile Application, today all are interconnected, vertical integrated “creating smart systems that are not just analytical but also predictive and prescriptive” (Hiller & Russel, 2013) in cross-country surveys with all stakeholders linked.

Recent research and studies are strengthening the opinion that “businesses are experiencing massive disruption as they respond and attempt to capitalize on the on-going changes (Schwab, 2019; Zangeneh

& Shajari, 2018; Lin, Lin & Pei, 2017). Digital transformation is more far-reaching than just technology (Hadžiosmanović, Bolzoni & Hartel, 2012). If we look at how the digital market is evolving, it is very clear that people are a constant and at the heart of digital evolution (Lee, Lee & Kim, 2016). Harnessing the collective intelligence of employees, partners and customers is a critical success factor for digital transformation" (Choi, Lee, Kim, Jung, Nam & Won, 2014; Khan, Gani, Wahab, Shiraz, & Ahmad, 2016).

In the opinion of Klaus Schawb, Founder and Executive Chairman of the World Economic Forum, these technologies have the power to connect the businesses in a "global digital and virtual system and the related flow of ideas and services" (Singh & Fhom, 2017). The impact of digital transformation on business is remove all borders and to replace old economies of scale (Yar, 2006; Kurosawa, Ohta & Kakuta, 2017).

In 2016, a study made by McKinsey & Company calculated that "digital flows—which were practically nonexistent just 15 years ago—now exert a larger impact on GDP growth than the centuries-old trade in goods" (Friedberg et al., 2016). The study reveal a "45-fold increase in the amount of cross-border bandwidth from 2005 to 2016 and predicted another 5-fold increase by 2022" (Kurosawa, Ohta & Kakuta, 2017).

In 2019, another study "Measuring the Digital Transformation - A Roadmap for the future" made by the Organization for Economic Cooperation and Development – OECD, reveal a roadmap with nine action step that if they are prioritized and implemented would help the countries to monitor the process of digital transformation and its impacts on economic environment (Schwab, 2019). First four action steps are directed to build with a new generation of stakeholders, a new generation of data and indicators capable of dealing with challenges of digital transformation: make the digital economy visible in global economic statistics, understand the cross-countries economic impacts of business digital transformation, measuring well-being in the digital age, and design new and interdisciplinary approaches to data collection. The next five action steps are directed towards specific areas of interests: fast accelerating transformative digital technologies, global data infrastructure, data flows, and skills in the digital era, trust in online environments, and governments' digital strengths and policies.

Digital Transformation is about cloud computing, mobility, Internet of Things (IoT), Artificial Intelligence related science and technologies, Big Data Analytics, replacing the power of one with the power of many and develop a new practical paradigm of economic value (Fischbacher-Smith, 2016).

A survey from 2019 reveal that between 2013 and 2016, 5 economies of the World – USA, China, Chinese Taipei, Japan, USA and Korea, develop between 70% - 100% of cutting-edge digital technologies. Digital business transformation under the digital are the based tech entities. In less than 25 years, Amazon grew from a startup e-commerce store to the world's second-largest traded company, revolutionizing retail, cloud computing, and other Web services. Apple became the world's first trillion-dollar company in 2018, barely a decade after it released the first iPhone. In Asia, Alibaba Group registered a market value of $ 499.4B (Schwab, 2019).

Digital Transformation subject has challenged practitioners and theoreticians to analyze this business expansion and to outline new horizons' (He, Chen, Chan & Bu, 2012; Broadbent & Schaffner, 2016; Liaudanskienel, Ustinovicius & Bogdanovicius, 2009). Business expansion is based on two directions (Malatras, Geneiatakis & Vakalis, 2016; Arukonda & Sinha, 2015). First is the economic entities that have included on their business model the new industries: cloud computing, healthcare, loans and payments. The second direction is represented by economic entities that have disrupted social patterns trough global tech platforms, without any physical assets as a support for their services, but having a strong ally: Artificial Intelligence, Big Data and a capacity to build the necessity of their services (Peltier, 2010; Hjortdal, 2011; Agrawal & Tapaswi, 2017). Tech entities, including computers and mobile phones succeeded this in past 12 to 14 years and they continue expanding at global level, worldwide, becoming digital conglomerates, gaining market power and counting billion of users (Tropina & Callanan, 2015; Gaidelys & Valodkiene, 2011).

2.2. Cyberaccounting – New Force of Accounting in Digital Economy

The exponential growth of new technologies, sustained by the increasing number of mobile and wireless devices and services, the customers need to respond in real time at their demands represent an Artificial Intelligence vast exploration field for today and future economic entities, worldwide, medium size, small or start-ups. Artificial Intelligence became a powerful tool with critical impact on finance functions and workflows reshaping the accounting departments and connecting them with cybersecurity in a new intelligence perspective: Cyberaccounting (Schwab, 2019).

Studies and reports from the industry reveal the positive impact of Artificial Intelligence implication on accounting area, reshaping the vision of data on stakeholders based on the association between the Artificial Intelligence and natural language interfaces with high change potential (Mittelman, 2011; Smith, 2005; Lee & Kim, 2017). From the perspective of an economic entity, Cyber accounting is the new force of accounting in Digital Economy. The purpose is to make a significant, reliable and positive impact on the finance department, by redefining key performance indicators and especially real profits, creating new business models, develop revolutionary business solutions for all type of economic entities, covering Accounting Services, Bookkeeping, TAX filing and VAT reporting services as “technology building blocks” (Okamoto & Takashima, 2015) with the expansion in maximizing the value of financial data even if the threat of cybersecurity risk still exists.

In the vision of practitioners, Cyber Accounting will be the new language in which Accounting and Finance will speak to the world. The impact of Artificial Intelligence with innovations in technology include “bookkeeping apps, tax software, auditing automation, and platforms that generate financial projections and visualized data” (Willems, 2011). By adding block chain technology between them and financial institutions, auditing and anti-fraud race to automation, we sustain our opinion that Cyber Accounting will help the leaders of the future to build a strong economic entity by developing a better business model.

The classical accounting procedures in which accountants “processed invoices, purchase orders, or deliver orders on paper documents which manually were introduced in computer systems, coded, and finally transmitted to the managers for approval and payment” is replaced by “automated workflow process and software that analyzes, recognizes, directs, and exports data into a company’s ERP/financial system”(Karanja, 2017).

Based on cloud solutions which are available in real time for millions of economic entities and users, the force of Cyber accounting is reflected in: the improvement of cloud-based software solutions (SaaS/software-as-a-service) for managing financial documents with variable structure, in automatically recognition with no prior configuration, in the usage of optical recognition of codes using OCR/optical recognition technology, processes and routes invoices, in accuracy to rebuild an automatized relation with suppliers and in the clear vision offered to leaders on payment deadlines, approval workflows, management decisions based on financial reports, in improvements in invoice processing time from 30 days to 2 days, processing costs per invoice reduced from $13.00 to about $2.00, and the opportunities to capture early payment discounts rise from only 20% of the time to 80% of the time (Chen, Ge & Xie, 2015).

The self-learning—machine learning—capabilities of cloud-based software solutions for data processing, verifications, referrals, and fraud detection are constantly improving and up-date. These solutions essentially learn from their mistakes and do not make them again once accountants correct them. Based on that, their productive time directed towards value-added for economic entities trough analysis, strategy, creative thinking, meaningful reporting and decision-making will increasing exponentially with the business force of Cyber accounting.

As practitioner and a cloud AP automation user, Bryan Schmidt, controller for Unite Here Health support the idea of a better business model through cyber accounting: "The improvements are due to capturing, automatically coding and storing invoices instead of handling paper or sending around PDF files. The system observes and learns from clerks' keystrokes, continuously improves GL coding, and reduces errors" (Tropina & Callanan, 2015). Therefore, another impact of cyber accounting is on human resource. Studies reveal that the jobs with repeatable actions will be replaced by automated: "bookkeepers have a 97.6 percent chance of seeing their jobs automated, accountants and auditors 93.5 percent chance and financial analysts 23.3 percent chance" (Zangeneh & Shajari, 2018), while those that require human resource skills, analysis and reporting capacity will become key positions looking for key persons.

3. Digital Transformation of Managerial Accounting – Tool for the Leaders of the Future

In practice, changes produced by business digital transformation are the result of digital technology waves: increase demand of cloud computing services, rise of AI and Big Data analytics, the necessity of building a global data infrastructure, mapping AI economic entities from all sectors, impact of digitization on operations, work process and young generations and the evolution of "digital divides" (Landoll, 2010). Digital Era Trends are the reflection of a new Digital Integrated Global Framework Policy where all the stakeholders are involved: The increasing of AI and the human replacement with algorithms who manage the financial documents, learning machine and deep learning lead to the emergence and development of new related concepts at the new digital economy: Accounting Intelligence or Cyber Accounting, a new force who will reshape the business financial information through use of "computers that recognize and analyze documents automatically" (Agrawal & Tapaswi, 2017) and improvement of accounts payable processes. Cyber Accounting is about capture the financial anticipation, about using Cloud, Edge and 5G Technology to build a new Modern Economic Infrastructure and about believe in the magic of tech innovations (Chen, Ge & Xie, 2015).

Still a question remain for the leaders of the future: "Is Accounting Information Systems capable to offer the answers according with their Vision?" In our opinion, based on latest theoretical interpretation of digital transformation and the emerging cyber accounting, we sustain that AI impact on accounting will increase and expand the volume of processed data with the help of algorithms in order to improve the process of making decisions in an empirical way.

Nevertheless, the predictions of the business future requires leader vision expansion until the core of the business, in a complex and intuitive medium, where all the business growth capabilities are waiting to be augmented (Kurosawa, Ohta & Kakuta, 2017). Real business growth is based on strategy, on the ability to develop a real, powerful and trust based relation between leader of the future and accountants, in order to reshape the business on digital transformation requirements.

Prevention means that the attack will be prevented (Fischbacher-Smith, 2016). Typically, prevention involves implementation of mechanisms that users not be able to counteract and are implemented correctly, unaltered, so the attacker cannot alter those (Singer & Friedman, 2014). Prevention mechanisms are cumbersome and often interfere with the use of the system to the point that, sometimes hamper normal use thereof (Winkler, 2010). But some simple preventive mechanisms with as passwords (which are designed to prevent unauthorized users from using the system) have become widely accepted plan (Gandino, Celozzi & Rebaudengo, 2017). Once implemented, the resources protected by mechanisms not are monitored to identify any security issues, at least in theory (Ruževičius & Gedminaitė, 2007).

IBM vision on cyber security is that "Security doesn't need more tools. It needs new rules", while Patrick Buono in Cybersecurity for Accountants reveal that "global cost of cybercrime will reach $2 trillion by 2019" (Schwab, 2019). In the vision of Warren Buffett cyber-attacks represent "a bigger threat to humanity than nuclear weapons," and for Ginni Rometty, IBM President & CEO, cybercrime as "the greatest threat to every profession, every industry, every company in the world" (Schwab, 2019). Statistics conducted by The National Computer Security Survey, U.S. Department of Justice's Bureau of Justice Statistics, found 68% of cyber theft victims will incur losses of $10,000 or more, and victims of cyber-attacks will experience downtime of 24 hours or more" (Lee & Kim, 2017).

In our opinion, the leaders of the future are the key persons who will implement and encourage the emerging technologies of automating accounts payable processes in the economic entities, streamlining the entire financial process. Cyber accounting must be seen more as a driving force than a threat. The advantages that Artificial Intelligence create on the businesses are multiples: building a clear representation of financial incoming and outgoing with real time control on payment, offering the possibility of creating new business models in which a central role is played by algorithms. The solutions offered by Artificial Intelligence are flexible, adaptable at multiple variables, with the capacity of automatically "data recognition in an exhaustive and reliable way, with no prior configuration" (Stepchenko & Voronova, 2015). Is for the first time in the economic environment when "the value of financial data in an accounting information system is extremely high" and for the first time when Accounting Information Systems (AIS) is able to support all accounting functions and activities: financial reporting, auditing, taxation, and management accounting (Lin, Lin & Pei, 2017).

4. Conclusion

Business expansion and digital transformation have produced significant changes at all business levels, on vertical and horizontal plan (Hong, Kim & Cho, 2010). Therefore, on vertical plan the digital transformation change the perspective of stakeholders represented by" broad group interested in the success or failure of a business: shareholders, creditors and customers, employees, the local community, and the government" (Kesan & Hayes, 2012). At the top of pyramid the founders, investors and other shareholders and at the bottom the employees replaced step-by-step with different forms of Artificial Intelligence (Krombholz, Hobel, Huber & Weippl, 2015). On horizontal plan, digital transformation rewrite the organizational structure of economic entity, the organizational culture, the human resource participation and also the operations.

On that basis, IT and Accounting become the most powerful "defensive weapons" for the leaders of the future, and accountants have the mission to protect the economic entities in front of cyber-attacks, mitigate and help them recover. As a consequence, for all the economic entities that acts in actual and future Digital Economy, a guide adapted at the economic entity characteristics was developed: The NIST Cybersecurity Framework. A six core components correspond at five Cybersecurity Framework's Functions: Predict, Identify, Prevent, Detect, Respond and Recover. Around this Cybersecurity

Framework the business is organized with a cybersecurity management at first level of importance and with leaders decisions based on risk management analyses. The Cybersecurity Function represent three parts: “Framework Core, Framework Implementation Tiers, and Framework Profiles” rewriting the connection between stakeholders and the IT and Accountants representatives, who translate in reality the strategic directions of action (Schwab, 2019).

The present article provide to readers valuable information, new insights regarding the force of business digital transformation and its impact on accounting, reinforcing the beliefs that business digital transformation at the end is about: “Going Digital, Shaping Policies, Improving Lives.”

On short term, cyberaccounting will improve the international compatibility of current performance indicators and make statistical systems more flexible and responsive to the introduction of new and evolving, disruptive concepts such as Cloud, Edge Computing and 5G Technology. The true digital transformation will be on long term achieved by the global economic community with redesign of a new, interdisciplinary, and protected from cyber-attacks platform and interconnected through partnerships between all the stakeholders involved with the powerful support of researchers.

5. References

Agrawal, N. & Tapaswi, S. (2017). Defense schemes for variants of distributed denial-of-service (DDoS) attacks in cloud computing: A survey. *Information Security Journal: A Global Perspective,* 26(1), pp. 1-13.

Andress, A. (2003). *Surviving Security: How to Integrate People, Process, and Technology*. USA: Auerbach Publications, Boca Raton, FL.

Arukonda, S. & Sinha, S. (2015). The innocent perpetrators: reflectors and reflection attacks. *Advanced Computer Science*, 4, pp. 94–98.

Broadbent, A. & Schaffner, C. (2016). Quantum cryptography beyond quantum key distribution. *Designs, Codes and Cryptography*, 78(1), pp. 351- 382.

Chen, H.; Ge, L. & Xie, L.A. (2015). User Authentication Scheme Based on Elliptic Curves Cryptography for Wireless Ad Hoc Networks. *Sensors,* 15, pp. 17057-17075.

Choi, Y.; Lee, D.; Kim, J.; Jung, J.; Nam, J. & Won, D. (2014). Security Enhanced User Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography. *Sensors,* 14, pp. 10081-10106.

Collins, S. & McCombie, S. (2012). Stuxnet: the emergence of a new cyber weapon and its implications. *Journal of Policing, Intelligence and Counter Terrorism,* 7(1), pp. 80-91.

Fischbacher-Smith, D. (2016).Breaking bad? In search of a (softer) systems view of security ergonomics. *Security Journal,* 29(1), pp. 5-22.

Friedberg, I.; McLaughlin, K.; Smith, P.; Laverty, D. & Sezer, S. (2016). STPA-SafeSec: Safety and security analysis for cyber-physical systems. *Journal of Information Security and Applications,* 29, pp. 1-12.

Gaidelys, V. & Valodkiene, G. (2011). The Methods of Selecting and Assessing Potential Consumers Used of by Competitive Intelligence. *Inzinerine Ekonomika-Engineering Economics,* 22(2), pp. 196-202.

Gandino, F.; Celozzi, C. & Rebaudengo, M. (2017). A Key Management Scheme for Mobile Wireless Sensor Networks. *Applied Sciences,* 7, p. 490.

Hadžiosmanović, D.; Bolzoni, D. & Hartel, P.H. (2012). A log mining approach for process monitoring in SCADA. *International Journal of Information Security,* 11(4), pp. 231-251.

He, D., Chen, C., Chan, S. & Bu, J. (2012). Secure and efficient handover authentication based on bilinear pairing functions. *IEEE Transactions on Wireless Communications,* 11(1), pp. 48–53.

Hiller, J. & Russel, R. (2013). The challenge and imperative of private sector cybersecurity: An international comparison. *Computer Law & Security Review,* 29(3), pp. 236–245.

Hjortdal, M. (2011). China’s use of cyber warfare: Espionage meets strategic deterrence. *Journal of Strategic Studies,* 4(2), pp. 1–24.

Hong, J.; Kim, J. & Cho, J. (2010). The trend of the security research for the insider cyber threat. *International Journal of Future Generation Communication and Networking,* 3(2), pp. 31–40.

Karanja, E. (2017). The role of the chief information security officer in the management of IT security. *Information & Computer Security*, 25(3), pp. 300-329.

Karim, H.V. (2007). *Strategic security management: a risk assessment guide for decision makers*, Elsevier Inc.

Katzenbach, J.R. & Smith, D.K. (2015). *The Wisdom of Teams: Creating the High-Performance Organization*. Boston/Massachusetts, USA: Harvard Business Review Press.

Kesan, P.J. & Hayes, M.C. (2012). Mitigative counterstriking: Self-defense and deterrence in cyberspace. *Harvard Journals of Law and Technology,* 25(2), pp. 474–529.

Khan, S.; Gani, A.; Wahab, A.W.A.; Shiraz, M. & Ahmad, I. (2016). Network forensics: review, taxonomy, and open challenges. *Journal of Network and Computer Applications,* 66, pp. 214–235.

Krombholz, K.; Hobel, H.; Huber, M. & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications,* 22, pp. 113-122.

Kurosawa, K.; Ohta, H. & Kakuta, K. (2017). How to make a linear network code (strongly) secure. *Designs, Codes and Cryptography,* 82(3), pp. 559- 582.

Landoll, D.J. (2010). *The security risk assessment handbook: a complete guide for performing security risk assessment.* 2nd Edition. CRC Press, Taylor & Francis Group.

Lee, C.; Lee, C.C. & Kim, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity. *Computers & Security*, 59, pp. 60-70.

Lee, W. & Kim, N. (2017). Security Policy Scheme for an Efficient Security Architecture in Software-Defined Networking. *Information*, 8, p. 65.

Liaudanskienel, R.; Ustinovicius, L. & Bogdanovicius, A. (2009). Evaluation of Construction Process Safety Solutions Using the TOPSIS Method. *Inzinerine Ekonomika-Engineering Economics,* 64(4), pp. 32-40.

Lin, Z.; Lin, D. & Pei, D. (2017). Practical construction of ring LFSRs and ring FCSRs with low diffusion delay for hardware cryptographic applications. *Cryptography and Communications,* 9, pp. 431-440.

Malatras, A.; Geneiatakis, D. & Vakalis, I. (2016). On the efficiency of user identification: a system-based approach. *International Journal of Information Security,* 15(1), pp. 1-19.

McQuade, S. (2006) *Understanding and Managing Cybercrime*. Boston, MA: Allyn & Bacon.

Mittelman, J.H. (2011). Global (in) security: the confluence of intelligence and will. *Global Change, Peace & Security,* 23(2), pp. 135-139.

Okamoto, T. & Takashima, K. (2015). Achieving short ciphertexts or short secret-keys for adaptively secure general inner-product encryption. *Designs, Codes and Cryptography,* 77(2), pp. 725–771.

Peltier, T.R. (2010). *Information security risk analysis*. 3rd Edition. CRC Press, Taylor & Francis Group, Auerbach Publications.

Ruževičius, J. & Gedminaitė, A. (2007). Business Information Quality and its Assessment. *Inzinerine Ekonomika-Engineering Economics,* 52(2), pp. 18-25.

Schwab, K. (2019). *Globalization 4.0. A New Architecture for the Fourth Industrial Revolution. A call for engagement.* Geneva, Switzerland: World Economic Forum.

Singer, W.P. & Friedman, A. (2014). *Cyber Security and Cyber War: What Everyone Needs to Know*. New York: Oxford University Press.

Singh, A. & Fhom, H.C.S. (2017). Restricted usage of anonymous credentials in vehicular ad hoc networks for misbehavior detection. *International Journal of Information Security,* 16(2), pp. 195-201.

Smith, D. (2005). Dancing with the mysterious forces of chaos: Issues around complexity, knowledge and the management of uncertainty. *Clinician in Management*, (3/4), pp. 115–123.

Stepchenko, D. & Voronova, I. (2015). Assessment of Risk Function Using Analytical Network Process. *Inzinerine Ekonomika-Engineering Economics*, 26(3), pp. 264-271.

Tiago, O.; Manoj, T. & Espadanal, M. (2014). Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors. *Information & Management,* 51(5), pp. 497-510.

Tropina, T. & Callanan, C. (2015). *Self- and Co-regulation in Cybercrime, Cybersecurity and National Security.* New York: Springer International Publishing.

Wang, W. & Hu, L. (2014). A secure and efficient handover authentication protocol for wireless networks. *Journal of Sensors,* 14, pp. 11379–11394.

Willems, E. (2011). Cyber-terrorism in the process industry. *Computer Fraud & Security*, 3, pp. 16 – 19.

Winkler, I. (2010). *Justifying IT Security – Managing Risk & Keeping your network Secure*. Qualys Inc.

Yang, C.N.; Wu, C.C. & Wang, D.S. (2014). A discussion on the relationship between probabilistic visual cryptography and random grid. *Information Sciences,* 278, pp. 141–173.

Yar, M. (2006). *Cybercrime and Society*. London: Sage.

Zangeneh, V. & Shajari, M. (2018). A cost-sensitive move selection strategy for moving target defense. *Computers & Security*, 75, pp. 72-91.