Academic Journal of Economic Studies
Vol. 5, No. 3, September 2019, pp. 138–143
ISSN 2393-4913, ISSN On-line 2457-5836

Cyber security for Cyber accounting - Tool for the Digital Enterprise

Cristina Ștefănescu[1], Loredana Elena Comănescu[2], Ciprian Buhuși[3], George Adrian Bîlcan[4]

[1,2,3,4]Valahia University, Romania,[1]E-mail: cristina.stefanescu@gmail.com, [2]E-mail: comanescu.loredana.elena@gmail.com, [3]E-mail: ciprian.buhusi@gmail.com, [4]E-mail: bilcangeorgeadrian@gmail.com

Abstract

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. This article presents the future leader's perspective the impact of business digital transformation, but also the threats and vulnerabilities on managing accounting information system using Cyber security. The results show that the analytical cyber reveal that working in a digitized environment offer possibility for accountants to touch a field of cyber security.

Key words

Cyer security, cyber accounting, managerial decisions, digital enterprise

JEL Codes: H55

Received: 28 July 2019 **Revised: 12 August 2019** **Accepted: 22 August 2019**

1. Introduction and literature review

As a result of Fourth Industrial Revolution, digital transformation represent a challenge for all economic entities, governments and societies and limit the actions of them on three options. First is to protect the "losers" of revolution change, sustaining "social safety nets, active labour-market policies" (Schwab, 2019). Second is to support laissez-faire economic policies, hoping that the result will balance all sectors of economic environment. And, at the end, is that economic entities benefit from the opportunities of the Fourth Industrial Revolution, trough redesigning "inclusive platforms and systems that are fit to deal with the complexity of the new wave of global integration", diving in Accounting Information Systems – the core of the businesses (Singer and Friedman, 2014). Truth the know-how offered including accounting cycles and processes, characteristics, reviews different types of information system designs and architectures, Accounting Information System's is a perfect framework of their business evolution, offering the possibility to obtain in real time a financial translation of their vision, with all the resources involved, a mirror of present and a transition on the expanded future having the support of Artificial Intelligence.

Economic entities from Industrial Revolution 3.0 also benefited from winner-takes-all dynamics, but their economies of scale were limited by natural or by legislation. The entities from industry cars or planes expanded and reached the limit of 50 million users in 60 years (Mittelman, 2011). Under these conditions, safety culture, with technical measures, complete the puzzle assembly steps necessary protection of information handled electronically.

The speed and efficiency brought by instant communications that contain economic information in the form of documents, files and messages (e-mail, electronic messaging, electronic funds transfer, etc.), the decision-making act of the managers acting in a highly competitive economy, they lead to a kind of euphoria of network use, based on a false sense of communications security, which can turn potential gains from access to information into major losses caused by data theft or false or distorted data insertion.

The process of digital transformation, new technologies implementation in the business process allows the transition on two development axes (Karim, 2007). On horizontal axe the transition on the economic entity core is from the local representation at global coverage. On vertical axe the digital transformation allows leaders to extend the field of data science from Artificial Intelligence at Machine Learning and Deep Learning. These technologies help them to analyse and interpret all the dates, including also accounting and finance. Moreover, Artificial Intelligence in accounting and cloud computing systems reveals also threats and weaknesses such as: vulnerabilities, loss of control, cyber security attack, cybercrime, and defence strategies.

The vulnerability of systems based on computer networks and implicitly on the Internet is much greater than that of the systems that preceded them. The claim is justified in the first place because the volume of information is much larger than

in other systems. Secondly, the growth of the Internet has been rapid and without being accompanied by special concerns to ensure a limitation of vulnerability. It seemed important at one point to be present on the Internet and less to make sure.

The integrity of the database refers to the validity and coherence of the stored data. Usually, integrity is expressed in terms of constraints, which represent rules of coherence, which the database is not allowed to violate. Constraints can be applied to data items in a single record or to the relationships between records.

Cyber security incidents recorded in recent years are likely to demonstrate that while policies and technology are critical components of any system of data protection, they alone can not provide effective protection of information. Risk awareness information security is the first line of defense personnel is true perimeter security computer networks, and their behavior is critical to the protection of information handled by these systems.

On the other hand, cloud computing is revolutionizing many ecosystems by providing organizations with computing resources featuring easy deployment, connectivity, configuration, automation and scalability. Cloud computing as an enabler provides scalable resources and significant economic benefits in the form of reduced operational costs. This paradigm raises a broad range of security and privacy issues that must be taken into consideration. Multi-tenancy, loss of control, and trust are key challenges in cloud computing environments.

2. Cyber security Framework - Essential for Ensuring Business Continuity and Accounting Intelligence

Information security technologies of an economic nature have several components and attributes that must be considered when analyzing the potential risk (Mittelman, 2011). Broadly, they can be classified into four categories:

- *Confidentiality* - protection of information in the system so that unauthorized persons cannot access it. It is about controlling the right to read information. Almost every organization has information that, if disclosed or stolen, could have a significant impact on competitive advantage, market value or revenue. Additionally, a firm can be held responsible for disclosing private information. Crucial aspects of confidentiality are user identification and authentication.

- *Integrity* - protection of information against unintentional or accidental changes; provided that the information from / or produced in a computer environment reflects the source or processes it represents. It is about the need to ensure that the information and programs are changed only in the specified and authorized manner and that the data present are original, unaltered or deleted in transit. As in the case of confidentiality, user identification and authentication are key elements of an information integrity policy.

- *Availability* - refers to ensuring that computing systems are accessible to authorized users when and where they need it and in the required form (provided that the electronically stored information is where it should be, when it should be there and in the required form).

- *Non-repudiation* - the characteristic of the transactions in which the parties to a transaction are certified, so that neither party can deny the participation or details of the actions or decisions taken during the participation.

On the other hand, new elements of digital vulnerability, vulnerability induced by the Internet and intranet networks, human interaction on the Internet have emerged. In addition, the security of economic information distributed in computer networks is not a problem of technology - it is a human and management problem.

According to CGMA – Association of International Certified Professionals Accountants the leaders of the economic entities are 100% responsible for " managing the cyber risk" taking in consideration that technology breaches: cost entities financial losses and reputation, have organizational impact, loss of client trust in the economic entity (Peltier, 2010).

In the 2018 Cost of Data Breach Study "the average consolidated total cost of a data breach is $3.62 million, a decrease of 10 percent over last year" and in 2017 Cost of Data Breach Study: Global Overview "the average cost of a date breach is $3.51 million." As an extension the study reveal that 72% of economic entities that suffer data losses and are unprotected from cyber threats in 24 months become inoperable (Schwab, 2019).

As we have presented the theoreticians and practitioners are preoccupied to support the stakeholders with the real impact of the cyber threats which can disrupt business (McQuade, 2006; Fischbacher-Smith, 2016). 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 (Figure 1).

Source: National Institute of Standards and Technology, U.S.Department of Commerce (www.nist.gov/cyberframework)

Figure 1. Framework for Improving Critical Infrastructure Cybersecurity

The Cybersecurity Framework descends to the deepest level of economic entity, including primary and vital dates for the leaders as financial dates. Around this Cyber security Framework the business is organized with a cyber-security management at first level of importance and with leaders decisions based on risk management analyses. The Cyber security Function represents 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 (Landoll, 2010).

Identify - the first function reveal the business context and support the leaders in the process of building the culture of managing cyber security risk involving the economic entity system, human resources, data, assets and other resources. The function help the economic entity to prioritize the efforts related with cyber security risks and the leaders to respond at these priorities accordingly with a risk management strategy. The results of applying the Identify function are represented by:

- The opportunity of implementing software assets as a base for the development of Asset Management Program.
- Economic Entity status: industry, global/local level, positioning related at the competitors, the role of economic entity in the supply chain.
- Assets weaknesses, threats inside and outside of the economic entity and the response activities as a basis for the entity Risk Assessment.
- Cyber security policies established in accordance with the Code of Governance and taking into account the legal and regulatory requirements regarding the cyber security capabilities.
- Supply Chain Risk Management strategy: strengths, priorities, weaknesses, risk tolerances, and assumptions used to support risk decisions associated with managing supply chain risks.

Protect - the 2nd function have the role to protect the vital and critical data of economic entity and to limit the economic impact of a cyber-security attack. Theoreticians and practitioners have defined the attack through certain characteristics: circumstance with important potential to adversely affect operations, asset or other resource involved though unauthorized access, destruction, disclosure, and modification of information or denial of service. In our opinion, this function reflects the stewardship of leaders for the most valuable resources of their business. This function effects are reflected in:

- Development of a Data Security protection based on risk strategy and related at the CIA Triad, represented by Confidentiality, Integrity and Availability of dates.
- Development and implementation of Information Protection Process and Procedures, Access Control and Management of Identity in order to protect the data and the assets.
- Building awareness and training organizational culture related at data security.
- Implementing and managing new technologies to ensure the resilience of the system.

Detect represent the 3rd function of the Cybersecurity Framework and is related with the imminence of an attack, with the focus on the activities unfolded in sight to detect the threats and to measure the impact on economic entity evolution.

Detect function cover the areas of the effectiveness of protective measures of networks and activities developing Security Continuous Monitoring capabilities able to reveal in a committed manner the unauthorized access to critical data.

Respond is the 4th function and for the economic entity is the answer of all the measures implemented and of Cybersecurity Strategy. Depending on the capacity of understanding and assumption the attack can be countered trough proper activities. For an entity to be able to respond in the best manner to a potential cyber security attack is crucial to develop this respond based on simulations as close as possible to the reality of possible attacks.

- Developing a continue Response Planning, 24/7, train the involved resources and improve the Communication Management regarding the Attacks Response between all the stakeholders, accountants and legal adviser in order to scale the financial losses and impact, to recover and to offer the necessary support.
- Increasing the capacity of economic entity to stop the expansion of the attack and to operate in an optimal time.
- Developing a best practice code based on the previous response

Recover is the last function of Cybersecurity Framework and for the leaders of entities represent the resilience and restore capabilities after a cyber-security attack. Through a proper involvement of the economic entity resources time of recovery is reduced. Recover function is reflected in:

- Development of a Recover Plan with processes and procedures for the restore of assets and system after a cyber-security attack.
- Implementing the Best Practices Code and Security Strategy adjustment.
- Improvement and coordination of internal and external communication at the time of cyber-attack.

As a result of the previous and in opinion of researchers, Cybersecurity Framework represents the approach, "tool, technique, methodology that provides a fit-for-all capacity for all-round attribute modelling and simulation of security risks" (Hong *et al*., 2010; Tropina and Callanan, 2015). The new technologies, Internet of Things, new cyber security threats emerge that require specific security solutions represented by "modelling and simulation of critical infrastructure systems using attributes, functionalities, operations, and behaviours to support various security analysis viewpoints, recognizing and appropriately managing associated security risks (…). It is found that empirical-based, agent-based, system dynamics-based, and network-based modelling are more commonly applied than economic-based and equation-based techniques, and empirical-based modelling is the most widely used" (Fischbacher-Smith, 2016). On short term, cyber accounting 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.

Another important issue regarding cyber accounting is ensuring the coherence and integrity of financial-accounting data against intentional or unintentional deletions. This objective is achieved through validation procedures, concurrent control protocols and procedures to restore the database after incidents. All these facilities are automatically provided by the management system of the financial database through specific components. The components of the database management system ensure coherence and integrity by treating separately the causes that can alter the database: semantic integrity, competing access control, saving/restoring.

Semantic integrity is ensured by operations performed by the database management system on data and processing. These operations make up a set of rules called integrity restrictions. The database management system ensures such implicit restrictions (result from the implemented data model) and explicit (procedures included in the application programs).

The control of the concurrent access ensures data coherence and is an objective of the database management system that is imposed with acuity especially on distributed databases. In this sense, the database management system has a distinct data processing unit called a transaction, which consists of a sequence of operations marked by starting and ending points. The transaction can be controlled by the default database management system, when the start and end points are automatically defined, or explicitly, when the start and end points are defined by commands specific. At the concurrent execution of transactions the database management system must ensure the blocking of the data used at a given time. This means that the access of the other concurrent transactions to the same data is forbidden, until the end the current transaction. The blocking technique used by the database management system can be applied at the level of the entire database, of a file, of a record or even of a field. It can be for reading (shared) or for writing (exclusive).

Saving/restoring as a facility of the database management system allows restoring the consistency of the data that have been physically altered for different reasons. Saving financial-accounting data is a storage process by making backups and

by logging transactions and images. The database management system can ensure the saving automatically or at the request of the database administrator. The restoration starts from the collections of data stored by salvage and restores the consistency of the database, minimizing lost processing. The restoration is provided automatically by the database management system but can also be performed manually.

It should be mentioned that the protection of the financial accounting database is a set of measures necessary to ensure the integrity and security of the data. The necessary measures are provided, to a large extent, by facilities offered by the database management system, but also by other tools built by the database designer. There are two trends regarding data protection: against accidental defects or errors (incomplete); idem as above and in addition against some deliberate actions to destroy the database (complete).

In addition, data integrity refers to the accuracy of the uploaded data - handled in such a way as to comply with the integrity restrictions of the model implemented by the database management system, while data security (confidentiality) means prohibiting access to data for unauthorized users.

3. Result and discussions

Digital Transformation subject has challenged practitioners and theoreticians to analyse this business expansion and to outline new horizons' (Yar, 2006). Business expansion is based on two directions. First are 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. 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 (Andress, 2003).

The protection methods specific to the information technology of today are varied, depending on the type of vulnerabilities they protect. Solutions provided by antivirus, antispam, antispyware, firewall equipment or programs, intrusion detection and prevention programs, or encryption of information are widely used by all who are aware of the risks of Internet age communication. Because this process, which is information security, is an essential component of the information society, specific international standards have been created.

Security is difficult to quantify. I can only estimate it as being high, medium, low or not at all. However, we can do (at least financially) quantify the level of security. Always implementing security or testing and improving it generate equipment and human costs.

Establishing a security program is the process by which security is offered to the company. It involves five steps: establishing the personnel responsible for ensuring the security, establishing the main steps for ensuring the security, defining the requirements for improving the security, informing the personnel about the security measures imposed, auditing and monitoring the security.

The results show that "proactively taking measures to prevent cybercrimes is a business necessity" (Arukonda and Sinha, 2015). The complexity of economic entity cyber security strategy supposed to develop a cyber-security action plan based on privacy-preserving sensitive data approaches in cloud computing: privacy threat model and privacy enhancing protocols and solutions.

4. Conclusions

Information security technologies are not only aimed at disaster prevention, they are means of achieving business objectives. Information security technologies, especially when distributed on computer networks, are absolutely necessary for success, so they must be included in the strategic thinking process of companies. Computer security should be seen as a process that is essential in meeting the legitimate needs of partners and customers and not something that can be "added". On the other hand, companies need to ensure that their marketing and public relations departments are versed in the principles of information security technologies in order to effectively communicate to the public the measures that are being taken to protect the money and the privacy of customers.

Implementation of information security measures, however, is not always a smooth process. In addition to the issues raised by the high cost of implementing security measures, the authorities control law implementation (enforcement) face a number of problems socially (Hiller and Russel, 2013). Contingency plan testing should be done according to a schedule approved by the manager of the organization, which contain concrete objectives and activities, as close as possible to

some emergency situations occur. Evaluation contingency plan must include all elements specified in the plan. Testing the effectiveness of the plan can be executed by conducting regular exercises that can be of type.

In conclusion, 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. Thus, if all the elements of this analysis (the value of assets, impact severity, frequency threats, effectiveness of controls, uncertainty and probability threat materializes) are expressed in quantitative terms, the process can be characterized as a fully quantitative one. Otherwise, depending on the wording of these measurements, risk management is partly or wholly qualitative one.

References

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

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

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

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

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),* 31–40.

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

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

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)*, 135-139.

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

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.

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

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