Mihaela, Cristea Lavinia

Article

Current Security Threats in The National and International Context

Journal of Accounting and Management Information Systems (JAMIS)

Provided in Cooperation with:
The Bucharest University of Economic Studies

Suggested Citation: Mihaela, Cristea Lavinia (2020) : Current Security Threats in The National and International Context, Journal of Accounting and Management Information Systems (JAMIS), ISSN 2559-6004, Bucharest University of Economic Studies, Bucharest, Vol. 19, Iss. 2, pp. 351-378, https://doi.org/10.24818/jamis.2020.02007

This Version is available at:
https://hdl.handle.net/10419/310775

Accounting and Management Information Systems
Vol. 19, No. 1, pp. 351-378, 2020
DOI: http://dx.doi.org/10.24818/jamis.2020.02007

Current security threats in the national and international context

Cristea Lavinia Mihaela[1,a]

[a]*Bucharest University of Economic Studies, Romania*

Abstract

Research Question: What are the main security threats emphasized by national and international surveys? **Motivation:** The rapid growth of IT brings worldwide security issues (Takahashi *et al.*, 2010; Benjamin *et al.*, 2015). IT usage brings new challenges (e.g. higher risks of data exposure, sensitive corporate data, phishing, electronic fraud, impersonations, information security issues) (Morrow, 2012; Thielens, 2013; Rîndașu, 2016), cybercrime being a "sophisticated transnational threat operating on an industrial scale" (Hunton, 2012: 203). **Idea:** This paper intends to underline the great exposure of financial and non-financial information in the new cybersecurity context, indicated by IT impact on security threats and cyberattacks. **Data:** The author traced the analysis of the most frequent cyber threats, over a period of six years (2013-2018), based on 20 security reports. **Tools:** The author adopts the qualitative method, applying critical observations on emerging technologies impact. A hand-collecting method is required, for the analysis and comparison of cybersecurity threats reports. **Findings:** This investigation highlights Targeted attacks/ APTs, malware and ransomware on top security threats that continue to disrupt worldwide and Romanian landscape, along with a major rate of employee errors. The paper enhances on the consequences, main security threats and concludes on security cybercrime prevention (i.e. adequate business model implementation, Cloud security solutions, 24/7 monitoring for continuous protection, continuous IT security training, implemented modules against a variety of security incidents, regular updates). **Contribution:** By bringing to the fore actual security issues, the author concludes on main security threats and completes previous specialized works on security against cybercrime.

Keywords: cybersecurity attacks, cybercrime prevention, top cyberattacks, current security threats

JEL codes: M41

[1] *Corresponding author*: Cristea Lavinia, Bucharest University of Economic Studies, 6-8 Piata Romana, Bucharest, Romania, email address: cristealaviniamihaela@yahoo.com

1. Introduction

The whole world is experiencing a great informational change conducted by reshaping and redefining technological processes. The rapid growth of information technology (IT) has evolved worldwide security issues. Besides the aforementioned (worldwide) effects, the current requirements of the digital era facilitate the restructuring of information systems and force companies to adopt new strategies that respond to the challenges of information security. In addition to the advantages (e.g. shorter time for preparing and presenting financial information, automation and usage of computerized systems, financial transactions recording, improved accuracy for a better external reporting) (Ghasemi *et al.*, 2011), IT usage brings new challenges (e.g. higher risks of data exposure, sensitive corporate data, phishing, electronic fraud, impersonations, information security issues) (Morrow, 2012; Thielens, 2013; Rîndașu, 2016).

It is accepted that cybercrime is a global issue being already a "sophisticated transnational threat operating on an industrial scale" (Hunton, 2012: 203). Information security is a complex and vast subject, current and interesting for any field of professional activity. Information security is a concept that is ensured by implementing a complex set of policies, procedures and organizational structures that have dynamically evolved over the past 10 years as a response to globalization issues and IT-based business processes expansion. The paradigm of security is shifting (Takahashi *et al.*, 2010; Benjamin *et al.*, 2015) and further developments in technology have brought new concepts such as borderless security, cloud computing, big data, mobility, IoT, Machine Learning, Artificial Intelligence (Morrow, 2012; Shayan *et al.*, 2013; PwC, 2016; Richins *et al.*, 2016; Mangiuc, 2017; Azvine & Jones, 2019).

Companies' information systems and supporting business processes could only be integrated through a set of essential information security features. That is, any security system must ensure confidentiality, integrity, availability and processing data storage. Since Cloud platforms incorporate four models (i.e. public, private, community and hybrid) (Mell & Grance, 2009), information security plays a cyber challenge in terms of data protection, information way of usage, data manipulation, data confidentiality, integrity, data encryption, data security. Cloud computing, according to NIST (National Institute of Standards and Technology) (Mell & Grace, 2009) is recognized by a model that allows convenient, fast provided and enabled on-demand network access to applications, services, servers, with a minimum management endeavor or service influence provider.

Cybersecurity represents an umbrella term for proactive and reactive measures focused on confidentiality, integrity and availability (CIA) of information, contrary to potential vulnerabilities (von Solms & von Solms, 2017). The cyberspace is a virtual enclosure caused by cyberinfrastructure, incorporating the extent of

information gathered, processed or transmitted. In this context, cybercrime appeared under the fact that a criminal constitutes or materializes a particular vulnerability or a constant threat for a third party, under a certain financial-economic motivation. There are also newer coordinates in the cyberattacks close to political and military areas.

The objective of the author is (1) to gain an understanding of the worldwide and local dynamic cybersecurity landscape, investigating the main security threats and cyberattacks typology emphasized by the national and international surveys, (2) to develop a discussion on this critical topic and (3) raise cyber criminality awareness. The present inquiry *"Current security threats in the national and international context"* represent a challenge for the author itself, nowadays, security problems generating a true debate among specialists. As the Romanian literature along with Romanian cybersecurity issues are scarce on the subject and there is limited transparency, the present research aims to (re)activate the interest for the research on this field. The author hopes to increase the transparency on this subject by implying companies, government representatives, individuals, information security specialists.

This paper is structured as follows. The first section provides the introduction on cybersecurity subject, emphasizing the challenges that companies face up to, presenting paradigm changes on information security and the cybercrime context (worldwide and local). The second section supports this paper by reviewing literature review, describing IT environment and critical vulnerabilities, highlighting the alertness of cybercrime climate and extending the security information importance, emphasizing why a strong communication in this context is essential. The third section discusses the research methodology and the questions this study intends to answer. The fourth section presents the investigations resulted, based on both global and local (i.e. Romania) security reports analysis, followed by conclusions and future research directions.

2. Literature review

Nowadays, digital systems interfere between user and information accessed. Digitization mediates the user's endeavor in processing, displaying, analyzing and storing information. Along with digitization, new technologies are continuously conducting to irrevocable transformations of the global economy. Internet connectivity provides huge business opportunities, redefines communication technology, but a generous room for Cybercrime actors too. "We live and operate in an ecosystem of digitally connected entities, people and data, increasing the likelihood of exposure to Cybercrime in both the work and home environment" (E&Y, 2014). In this context, Cybersecurity is no longer an information security specialists' concern but implies individuals, companies' board members and governments in the common effort to face and mitigate Cybercrime. According to

E&Y (2019), companies seem to be prepared to oppose Cyber-attacks. Larger companies are more likely to raise budgets for 2018 (63%) and 2019 (67%) compared to smaller companies (50% for 2018 and 66% for 2019). The reality is that for both individuals and organizations, large and small companies, vulnerabilities have become progressively more difficult to be detected in a short time, taking into account that security threats might appear from unforeseen origins.

Cybersecurity threats are not slowing down and they have no boundaries. All security specialists recognize the Cybersecurity's increase in frequency, impact and rate of success. The diversity and complexity of attacks maintain a permanent flag alert for the CISO and board members. "Enterprises continues to struggle with traditional security threats such as loss of devices, insider threats, malware, hacks and social engineering, while simultaneously trying to keep sophisticated attacks by nontraditional thereat actors" (ISACA, 2015:12). With each transitory year, the threating perspective represents a more diverse avenue which seems to not stop from evolution. Financial institutions, critical utility services like power generation plants are also susceptible to cyberattacks and due to the fact that today's world is so much inter connected, the impact on a single country or a zonal boundary can have a ripple effect and can have disastrous financial impact globally.

As the increased frequency, complexity and volume of threats evolved (e.g. WannaCry and Petya/ NotPetya spread), cybercriminals are now starting to concentrate on other financial opportunities (e.g. Bitcoin Mining: The New Gold Rush), in order to mine cryptocurrency. In many countries there had been recent incidences where skimming devices were used on ATM machine based outlets, stealing user's information, resulting in huge amount of fraudulent transactions. This affected the banking system and also had a financial impact on both money market and also the respective governments and statutory bodies.

IT environment is getting more complex, day-by-day, under the business competition pressure and business globalization. In this context, it is proved that new technologies' adoption is moving faster than security implemented solutions. There is a huge effort to deploy policies and controls aiming at securing information assets. "Procuring the advanced security technologies does not necessarily lead to a secure environment as their performance critically depends on how they are implemented" (Alhogail, 2014: 540). There is a disruptive cyber activity regarding web threats, where malware, coin miner detection, percentage spam rate, ransomware variants, attacks against IoT devices, industrial control system (ICS) connected to vulnerabilities increased by far.

In order to start the Cybercrime prevention, it is important to define security policies and identify the most adequate solutions in a proactive approach, starting from the business processes characteristics and industries' specificity. However, information security starts from business operations understanding and enclosing

Cyber possibilities as extensive as possible. "The companies are investing more and more in security solutions but they use the resources building a fence around their internal organization — including their data, systems and personnel… but the perimeter is no longer stable, and a fence no longer possible. Most of today's business is done outside the defensive fence" (E&Y, 2014:7:19). For example, Symantec (2019) underlines the importance of filtering emails and web requests by using advanced Machine Learning techniques, providing the possibility of monitoring traffic network or system behaviour, in order to identify organizational processes that could harm business prospects. An indispensable pillar against cybercrime is the proper definition and prediction of cyber threats. There prevail trends or megatrends which may happen from past events or clear present signals. A relevant classification is represented by high-impact low-frequency (HILF) cases, assigned to cyber-attacks (Masys *et al.*, 2014; Veeramany *et al.*, 2016), perceived as big probabilities by the universal public or as an incident that is most likely to occur.

Security procedures should be designed, implemented and updated according to the business operations and processes. As long as the processes are interrelated and the information flow follows the business chain, the security system design should integrate all the linked systems. Once vulnerabilities penetrate the system, the business chain is exposed. Companies should take attitude fast enough to mitigate the known vulnerabilities (E&Y, 2014:2). As IT environments register faster development and "are getting more and more complex, avoidance of information security incidents requires cooperation not only in the technological area but also across strategic, process and organizational area." (Drtil, 2013: 44).

In this respect, the implementation of IPv6 is a definite advantage in securing data communications. So far, it is used internet protocol version 4 (IPv4), which were forecasted to eventually run out of addresses, given the vast number of IP address requirement to this ever growing demand. IPv4 also lacked some of the security features which IPv6 does have and definitely an added advantage of huge numbers of IP addresses that shall be available for the World Wide Web. IPv4 had 32-bit address length, whereas IPv6 have 128-bit address length. IPSEC is an inbuilt security feature in IPv6, along with end to end connection integrity. IPv6 also have the advantage of multicast and any cast message transmission scheme. There is a significant volume of tasks, also cost of migration from already existing IPv4 to IPv6. CISCO, HP and other router manufacturers and service providers are integrating new security features, advanced firewall configurations etc., as of now both IPv4 and IPv6 coexists, eventually IPv4 will be phased out.

New malware is appearing and is growing year-over-year (Ledin, 2011; Ahmadi *et al.*, 2016; Guo *et al.*, 2016; Hou *et al.*, 2017; Aleshkin, 2019) and the great challenge consists of designing an accurate detection method to recognize the clusters that match to a predefined conduct template (Shan, 2013). In most cases, threats persistence problem belongs to old operating systems. Operational systems should run on their last version, either operate on phones, mobiles, MAC, or

computers. Taking into account cyberattacks continue to surge, Symantec gathers data each day, for fundamental analysis on spam, email malware trends, phishing, ransomware. This action would help organizations to identify the uncovered from the most concealed and persevering vulnerabilities, supported by a Global Intelligence Network.

Still, one of the most significant vulnerabilities of all security systems seems to be the user itself. "Enterprises that offer awareness training do not seem to be benefitting from a corresponding decrease in successful attack types; the nature of their attacks remains human-dependent, similar to those of enterprises without a program" (ISACA, 2015). The information security awareness programs should continue more than never because is tremendously important to change security attitudes and behavior among employees. In this respect, companies are responding with updated and continuous IT security training. There is room for improvement regarding building skills for non-technical disciplines, necessary to integrate cybersecurity into the core business (E&Y, 2014: 7). The companies' culture and existing security risks should be revised and understood in a proactive approach and addressed accordingly.

Azvine and Jones (2019) are emphasizing on most significant vulnerabilities (e.g. conventional malware, ransomware attacks, WannaCry attacks, Advanced Persistent Threats (APTs), spam, email malware trends) because of a technological complex change, consisting of the Internet of Things (IoT), Artificial Intelligence (AI), Big Data Analytics (BDA), Complex Adaptive Systems (CAS), non-state actors, hacktivists, criminals, individuals or lone hackers, cloud computing. This technological change is propagating on: careless or unawareness of employees, employees' insufficient monitoring, hardware failure, threats from third parties or partners, industrial software errors, sabotage by both external parties or employees. The main causes that contribute, directly or indirectly, to this insecure environment are outdated security procedures, old architecture design, inadequate mobile computing use, exploitation of social media use against internal organization procedures. The likelihood that a number of companies being attacked are quite low compared to the risk constituted by an attack. The complexity of an attack is determined by a start to end plan, proper documentation about the target and well-resources in place. Cybercriminals have increasingly applied a serious disruption and stealing of (perhaps) the most valuable information a company possess. The reasons are obvious since is so much intelligence gathered in one single action.

2.1 The Cybercrime and Cybersecurity landscape

Evolution in Cybersecurity has experienced over time a notable development since have been reported computer and network intrusion, hitting the nation's critical infrastructure. Year-over-year, more sophisticated ways of the attack appeared onto Cyber "stage", hackers target adversaries and continuously blow up informational systems. Whether Cybersecurity landscape is weak in system protection, compromises are most likely to appear. According to general investigations performed by FBI, Cyber events involve the theft of documents, inquisition

employees or customers' data, misappropriation of funds, intellectual property theft, a data breach of personal information, that is performed by hackers, non-state actors, hacktivists, to capture the system and get (full) access to (company's) valuable information.

Cyber-attacks are considered various and complex social events (Kumar and Carley, 2016) and a constant threat in the whole economy (Alloghani *et al.*, 2020). On-time detection implies challenges for companies because many threats are found in computing platforms. In this respect, Machine Learning and Data Mining are technologies which would control vulnerabilities doorway, by analyzing event logs, providing automatic and real-time defenses. By using analytical models, Machine Learning technology is continuously improved, by learning new processes and possibilities to capture hidden data without even programming computers to find it. For the cybersecurity landscape, Machine Learning implementation could contribute to a large spectrum of solutions development (Anderson *et al.*, 2017) and time series forecasting (Krollner *et al.*, 2010).

Nowadays, cybersecurity software (e.g. TitanHQ Web Titan, Keeper for Business, Webroot, Cryptosense, Flowmon) help companies in a consistent way, being flexible and easier to implement. Flowmon provides an absolute traffic monitoring over the network, Cryptosense offers visibility on organization's crypto-use by examining security issues and formulate recommendations to implement. Webroot is specialized in protection against Ransomware, Anti-Phishing, Identity theft, Internet Security, Business Mobile protection, Web Security Service products and automated backup. Keeper for Business provides large spectrum applicability. It can be used for businesses, enterprises, Managed Service Providers (MSP), personal or family support. The support consists of password management, Dark Web Monitoring & Account Takeover Protection, Free Dark Web Scan, to protect a company against Takeover Attacks. The advantage of TitanHQ Web Titan Cloud is that it not requires on-premise software or End-user license agreement (EULA). Because of this is easy to implement and quick, providing support in creating policies against malware, viruses, block accesses, phishing or inopportune materials.

Most of the Cyber-attacks occur from internal and external actor threats. Human thinking must be completely aware of the consequences of inadequate management of the used software. Alloghami *et al.* (2020) suggest that is not about a complex coding and evaluation knowledge necessary to be possessed, but a basic tool regarding both detection and prevention of cyber-attacks, a failsafe approach included. Employees' should possess basic knowledge regarding internet security suite, strong password change, keep updated software, being informed about security breaches, protection against identity theft. Taking into account information is the most wanted data for hackers; companies are continually seeking for advanced protection. Continuing in this respect, proper information about security threats in a continuously changing world is of a top priority for seniority level and it will always be.

Also, strong communication within the team has always been encouraged. The same applies to the Chief Information Security Officers (CISOs) and Chief Executive Officer (CEO) leadership. The source of information is critical. To receive information from employees who are directly implied in information security is crucial for organizations. They possess valuable information regarding vulnerabilities and forecasts that the company is confronting to. Implicitly, a cyber-defense process requires a free and undeviating flow of information. This is critical for security posture improvement and creating a strong CISO-CEO leadership. Direct communication with the CEO enhances transparency and contributes to the definition of decision making. The same assumes Bitdefender (2018), strong cyber defenses demand faster decision making and without a direct reporting to the command chain, cybersecurity may endure unfavorable consequences. Financial Services Information Sharing and Analysis Center (FS-ISAC) had drawn attention on a direct reporting method, by CISO to CEO. However, only 8% of CISOs report to the CEO and 66% to the CIO, CRO, and COO.

Financial companies are encouraged to persevere in fighting against cybercrime. This could reduce portion pressures that hackers are exerting on their targets. Step by step, this attitude contributes to better prevention, implying current resources. Yet, small measures are contributing to reducing the potential of future attacks, intended to ruin company reputation and stakeholders trust. A preventive measure that companies could adopt would be the forensic analysis, a detailed investigation recommended to be performed by organizations in documenting the reasons, course and consequences of a violation organization rules. This type of analysis has been considered an important topic in Cybercrime, many researchers discussing it (Bassett, 2006; Donalds, 2006; Park, 2009; Yeager, 2006; Stephens, 2007; Demertzis, 2018; Joseph, 2019).

Attacks seem to evolve on a daily basis and the most frequent threat actors which exploit enterprises are represented by cybercriminals (45.6%), followed by non-malicious insiders (40.72%) and hackers (40.09%). Those cyber actors undertake skeptical actions for financial gain, intellectual property theft, and classified data access, personally identifiable information, service security disruption (ISACA, 2015). For example, Sony becomes the victim of a malware cyberattack, purposing to steal confidential information. Hackers are concerned in finding new and intelligent ways to broke security systems to request for ransom. Principally, seniority level is concerned among protection, detection and identification; hackers are clever enough to anticipate next movements. Nine of ten IT decision-makers admit that information security plays an important role within their company. Nonetheless, only 64% of cyber-attacks can be prevented, discovered and blocked, with the company's resources employed (Bitdefender, 2016). That is, there is always room for improvement when is discussed about cybersecurity. To keep hackers far away is a great responsibility for companies.

3. Methodology and data

This paper aims to investigate, synthesize and compare current security threats in both national (Romania) and international context (globally: West, North-East, South, Mid-West world). The research method is based on an empirical approach, where the author adopted the qualitative research methodology. In order to offer a large perspective on the Cybersecurity threats evolution, this paper commenced with an observant review of Cybersecurity contemporary situation, through an attentive review of specialized international and national literature, comprising digital aspects and analyzing past years' major incidents in the international landscape, 2013-2018, and national landscape, during 2015-2017.

This study is focusing on understanding the changing and sophisticated Cybersecurity landscape, presenting a comparative synthesis on the evolution of current security threats, a general overview of Cybersecurity debates and financial aspects of data breaches. The information presented in this paper resulted from critical observations regarding attacks identified and traced through 2013-2018, based on the analysis of specialized security reports and surveys published online by globally major market players: Kaspersky, ISACA, Ponemon Institute, Symantec, ITU, CA Technologies, Bitdefender, Security Intelligence, CERT.RO, including Big Four companies (PricewaterhouseCoopers, Ernst & Young, KPMG), worried about this corrupting trend.

Firstly, the present investigation commenced with a careful review of specialized literature, performed on ProQuest, Springer Link, ResearchGate and Google Scholar databases. This research process is based on sorting for the most conclusive scientific literature on current security threats, searching for these terms: "information security", "information security threats/incidents", "cyberattacks", "attack", "information security change", "motivation of cyberattacks" terms. Whether a relevant article was detected, the reference list was reviewed in order to check that other key information was included.

Secondly, the author conducted online research to identify and analyze relevant of Cybersecurity reports and online professional websites (Kaspersky, ISACA, Ponemon Institute, Symantec, ITU, CA Technologies, Bitdefender, Security Intelligence, CERT.RO), emphasizing the global (world-wide) and local (Romanian) Cyber landscape, based on the following terms: "Cybersecurity threats report", "global information security survey", "top 10 cyberattacks", "protection against Cybercrime", "Cybercrime prevention", "DDoS attacks", "data breach cost". Cybersecurity reports and online news websites represent adequate evidence for this paper because Cybersecurity reports are issued by the major companies in security consulting, protection against Cybercrime and security programs support.

Whether a relevant report/ website was identified, the content was checked to ensure that other key information was comprised.

Thirdly, the author traced the analysis of the most frequent cyber threats, over a period of six years (2013-2018). The analysis provided is based on 20 security reports. The present investigation opens the debate on a detailed exploration and discussion about a needed employees awareness in information security topic, intending to find the answer about (1) what are the most common types of emerging cyber-attacks globally and nationally and (2) what recommendations result from the performed analysis. "Threats", "vulnerabilities", "alerts" are terms used interchangeably in this paper. Taking into account the large number of cyber-attacks attempted from day to day on a global scale and the limited information organizations typically reveal, it was impracticable for the author to obtain a full evidence of Cybersecurity events and evidence.

4. Results of the paper

This investigation was based on 20 security reports, besides news and events reported by important actors in the security industry. This section describes the main threats investigation and provides important observations among security alerts, analyzing the last years' major events. It is also introduced a discussion of the security incidents evolution, companies' average costs and the security challenges that appeared over time. In this section, the author debate Cybersecurity subject, aggregating the traced results with the analysis of security information.

4.1 An international insight

Continuously progressing technology brings shifts in security threats and companies have no choice than to align to the new digitalized world, by adopting new and different strategies. As a result of security reports, according to PwC, in 2015, security incidents increased by 66% compared to 2009 (PwC, 2015). This suggests that security threats continue to evolve in a multifarious phenomenon, bringing an appearance of impossibility for required controls to face all risks implied by the attacks. However, the chosen technology should be implemented according to an adequate business model, keeping in mind the financial impact to these upgradations as well. Depending on the industry type (e.g. financial, healthcare, airline) there is a business model which represents the criteria adoption (quality of reporting, prevention, diagnosis and treatment, transporting passengers' conditions). The picture we get from this example is that through the existence of an adequate business model, companies should check whether proper controls exist and employees react in the company's best interest. Proper management plays an important role in decisions making process and proper security solutions as well. Organizations responsibility but at the same time, the objective is to prevent

vulnerabilities, by examining past events and overcome security problems by adopting new strategies. By adopting this approach, fighting against Cybercrime would not be the most difficult challenge for organizations.

KPMG (2018) consider that employees play a doubtless important role in an organization. The perception of the misuse of a privileged account by an inside employee seems to conclude at 23%, placed on the 5th top on Cybersecurity vectors. For example, each employee should (definitely) know how to react in case of an attack. It is not recommended to shut down the server or to restart the computer system. When a shutdown is requested from the server, automatic deletion of the memory eventuates, if there are no log backups kept. Thus, a forensic analysis would be impossible to be performed by the intervention IT department since no evidence exists. It is highly recommended for companies to agree on a back-up procedure on an external hard drive, is scheduled a daily copy of the data or at a certain period of time. In case of a computer restart, the backup is possible to be already infected. The system could be contaminated a while ago and though installation of the infected backup, the contamination would happen again. Because of threats persistence, it would take 90 days for a total awareness about infections.

The same found PwC (2015); incidents are caused by the staff (43%) but ranked as the 1st security incident. Kaspersky (2017 and 2018) split damages caused by the employees between intentional (30%, respectively 51%) and unintentional actions (31%, respectively 49%). CA Technologies (2018) reveal the lack of employee training/awareness at a percentage of 31. Information security would meet concrete criteria whether employees would read and engage for security policies, by creating an active curiosity among work-groups and enthusiasm through active participation at workshops or training.

For US retail stores the average cost of cybercrime incident implies $8.6 million (2014), double compared to 2013 (ISACA, 2015). This suggests the actual damage which cyberattacks run on economic business in billions of dollars. Hackers look for big prizes and are constantly finding new ways to attack web applications or websites. E&Y (2017, 2018) estimates that the average cost of a single data breach for $3.62 million, confirmed by the Ponemon Institute report as well. By 2019, Cybercrime is estimated to become a problem which might cost $2.1 trillion dollars (Security Intelligence, 2016). Whether those costs would rise higher, companies would definitely be affected. Consequences can sphere troublesome to downright critical.

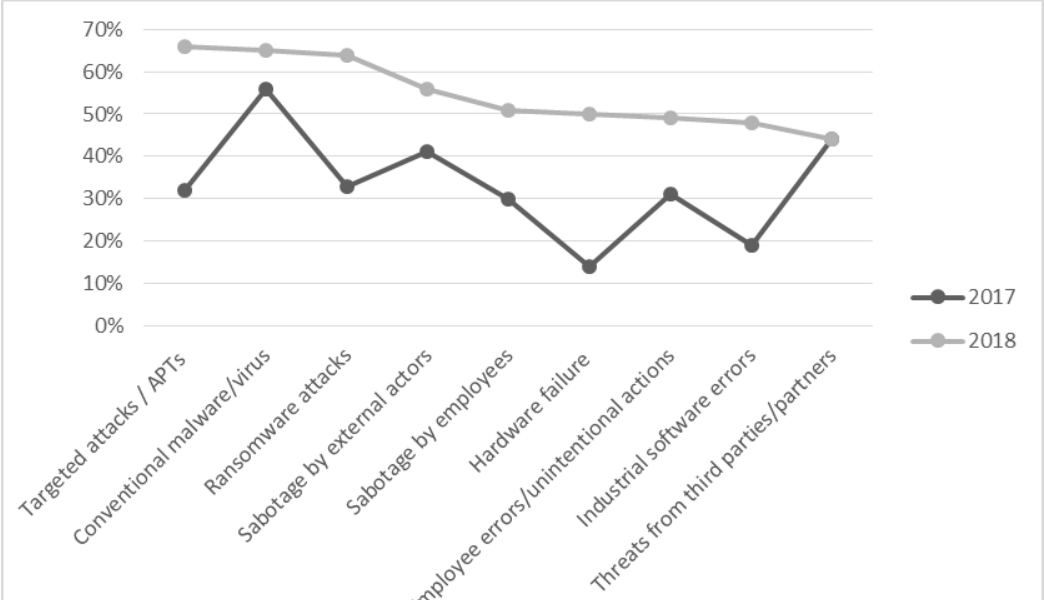
The high concern is determined by the actors' cyber ability in covering their criminal actions. If the Kaspersky report stated that the longest Q2 2015 DDoS attack lasted 291 hours, the longest attack in Q3 2018 lasted 239 hours. This

finding is in line with Netwrix (2018), where the 1st of top 10 overwhelming types of attack was defined by the distributed denial-of-service attacks (DDoS). The system presents a huge explosion in terms of the impact that will deny the user access, by overloading and signal to a total non-operational state. It can be observed the complexity of the attacks, targeted and well prepared, since every year attacks develop meaningfully and destination change.

Even the most common DDoS attack could evolve in a genuine malware infection for computers or IoT devices. DDoS attacks have become a serious threat of both organizations and the government. DDoS flit around the company's hazard, by delaying the system flow with internet traffic, to be rendered unusable. Ziwit, a French company specialized in Cybersecurity, provides a variety of solutions for security incidents, such as Ransomware, Phishing and Spear phishing, Pirated software and websites, Malicious Websites, Malware
 Provider, DDoS Attack, Zero-Day Attacks, Data and passwords flaws. In this respect, implemented modules would ensure protection against a variety of security incidents that organizations face, including DDoS.

Compared to 2017, Kaspersky research team reveals for 2018 a visible enhancement in the evolution of security incidents. Security threats continue to record high, presenting Targeted attacks/APTs (1st), succeeded by conventional malware (2nd) and ransomware attacks (3rd). A line with markers (Figure 1) is defining the 2017-2018 security incidents evolution.

Figure 1. Security incidents evolution during 2017-2018



(*Source*: author projection based on KASPERSKY reports)

Malware represents an umbrella-term for Trojans, viruses, worms and spyware or other intruding codes. There are detection techniques that can be used for malware detection, such as anomaly-based detection technique that decide on the maliciousness of the program inspected based on its knowledge and signature-based detection which construct a model representative for the malicious behavior in order to model in the process of malware detecting. However, the objective of this article is to emphasize the most common Cyber threats and to find solutions on this various thematic perspective. Returning to malware infections, proactive alerts must never get postponed. Important malware alerts should not get missed in order to impede malicious macros execution.

Kaspersky report (2019) presents the old ransomware as targeted ransomware. A new evolution of this concept is concentrated on more aggressive attempts to money extortion, publishing data against making inoperable files. Ransomware is a very common attack among hackers and can encrypt data on computers, mobile phones, servers, smart TVs, smart houses or smartwatches. Abusive Cybersecurity incidents are supported by a large technology usage of non-stop connection at the Internet. This available connectivity monetizes access for hackers very easy and brings for ransomware the first place winner in security incidents on financial profit extraction. After the encryption of data, hackers ask for a ransom in exchange for data description.

For example, during February – March 2020, Coronavirus, also known as COVID-19, played an important alert in the whole world. Under the fake Coronavirus Emails, TrickBot Malwarebyte aim Italy in a new spam campaign. Users tend to open this type of emails to get information about protection against COVID-19. In this context, malware allocators use current news that induces fears, actual events or political circumstances and also affects the stock markets with even false information. As there is not known enough about the spread of this virus, a new malicious spam expedition has been initiated under the claim of a doctor, apart from the World Health Organization (WHO). Under the subject "Coronavirus: Informazioni importanti su precauzioni" and attaching a doc. where the user is invited to read all necessary preventive measures against COVID-19, WHO is strongly recommending to read the attached document from the email. On 4 March 2020, Sophos News explains about the steps of a TrickBot Malwarebyte effect. When the Word document is opened, whether macros are disabled, there is a message for the receipt to enable the content. But if the macros are enabled or the user who executes the document act according to the instructions, the VBA script proceed in disgorging the files already encoded on the disk. The macro already contains a JavaScript (jse) file, connecting to a PHP script that exists on a remote server. By proceeding with the IP address and fundamental details about the victim through an HTTP GET request. This action calls for the macro file, necessary for Java Script setter and a .bat Batch file in order to execute the setter with the script.

Sabotage by external actors represents another incident that registers an increase of 56% from 41%. The first step for minimizing this situation would be to identify the external threat actors, to proceed for measuring the risk impact for the organization and to appreciate exposure grade of external actors' capacities. Companies should extend controls in order to protect the infrastructure. Of the new security incidents that Kaspersky research team reported for 2018, 51% were related to Sabotage or other intentional damages by employees compared to a percentage of 30, declared for 2017. This employee behavior is associated with performance measurements, either from the individual and group rewards or effect for costumers. This Cyber evidence could be inspired from old antipathies over a bad personal evaluation, conflicts within the team or management, pressure from outside or other ideological vision, different from the company's view. Security professional should observe unusual behaviors among employees, such as unsuccessful attempts to log in, frequency and type of download, early arrivals at the offices or late leaving when all employees are missing. In order to prevent intentional damages by employees would be essentially a Co-ordinate connection between HR and IT security department to distribute advance remark of pending employment termination.

Companies either apply very little or no enterprising measures to mitigate insider risk. The basic steps adopted are no use of external drives, restriction in access to certain departments/hierarchy and also some external websites/IP addresses. Surprisingly, hardware failure increased a lot in 2018. All electronic devices company's using should be protected by anti-malware software which performs specific action against Trojan viruses, CIH virus (known as Chernobyl or Spacefiller), disrupted Flash BIOS, many a times a backup BIOS variant on-board helps. Whether protection is damaged, a hardware failure may cause impossibility on booting or starting the system.

Employee errors/unintentional actions represent another negative evolution in the Cybersecurity landscape. There is a trend among employees to use their own devices, by Bring Your Own Device (BYOD) adoption. This finds support in the organizational system imposed, restrictions that do not allow easy access and implicitly, prompt information access via e-mail, chat, voice or text. Businesses should adopt this trend to allow immediate information access, to overpower the productivity and provide maximum protection in opposition to a catastrophic event. Employees might extend vulnerabilities to the company system through the devices they use and connection to unsecured apps. Because the majorities of apps request an online connection during their usage and may end up in contact with office mainframe, it is very likely to open the gate for hackers, as users knowingly or sometimes unknowingly provides permissions to access data on any device, be it a smartphone, tablet, laptop. It is recommended for employees that mobile phones they use to be connected to their own data connection, avoiding the office connection. Industrial software errors are caused by software bugs and present a

continual evolution for 2018. The implemented software program should suit with the company's vision, strategy and mission.

International security reports (E&Y, 2013-2018; KPMG, 2017, 2018; PwC, 2015) emphasize phishing attacks, fraud tentative, spam content, vulnerabilities associated with the system, cyber-attacks intended to steal money, to disrupt or to steal IPs. Information security procedures must be revised according to this sophistication of cyber-attacks. However, this trend seems to not stop. In this respect, IT specialists, board members and investors continue to offer attention to security problems and are more day by day engaged. Even so, those actions are not enough. Organizations have to do more to reach a level of awareness greater than the actual one. Confidentiality regarding company processes and procedures, regularly checking of the authentication system, integrity of data, segregation of duties, authorization provided only to the personnel responsible with that particular process and availability of resources represent actions to be implemented. Knowledge of cybercrime prevention and incident reporting topic among employees must be encouraged. Pro-actions security services, forecasting true budgets and allocation of economic resources on IT security should be on the to-do list. All cyber threat forecasts have to be included in the management analysis to adopt better protection against potential hackers.

In line with Kaspersky, malware and ransomware are presented on top international threats during 2013-2018, according to E&Y, (PwC, 2015), KPMG (2017, 2018), Kaspersky (2017, 2018), MIT Technology Review (2018). Those reports reveal the complexity, sophistication and dangerous evolution of security incidents. Following the analysis performed, it seems hackers are finding new targets on their radar screen, since cyberattacks continue to develop in an alarming manner, for all security incidents. Online professional websites interested in new attacks and their effects are emphasizing both effects and solutions for an early prevention that is more conscious decisions, better information about technology cyberattacks and professional solutions for companies. Following a hypothetical case scenario introduced by Cyber Risk Management (CyRIM), a ransomware effort could interrupt the activity of more than 600,000 global companies within 24 hours. Whether companies remain unprepared to confront present attacks, a malicious global cyber-attack could cause global economic losses in the amount of $200 billion (The State of Security, 2019). Table 1 is summarizing the 2017 and 2018 evolution of security incidents discussed in this section.

Table 1. Evolution of security incidents during 2017-2018

Security Incidents	2017	2018
Targeted attacks / APTs	32%	66%
Conventional malware/virus	56%	65%
Ransomware attacks	33%	64%

Security Incidents	2017	2018
Sabotage by external actors	41%	56%
Sabotage by employees	30%	51%
Hardware failure	14%	50%
Employee errors/unintentional actions	31%	49%
Industrial software errors	19%	48%
Threats from third parties/partners	44%	44%

(*Source*: author projection based on KASPERSKY reports)

It is well known the challenge that companies face in relation to technology to implement an application that fits 100%. In this respect, companies should adopt the software according to their strategic plan and train employees about the working processes. This action would facilitate system-employee-company connection. Last, but not least, threats from third parties or partners register the same. Organizations should examine third parties history whose behavior could have a negative impact on the company's reputation. The most adequate solution is to make business with the right partner that fits the business Cyber Security needs. It is recommended 24/7 monitoring for continuous protection, contributing to a brilliant communication. A Cloud solution would provide those security measures.

Even so, technology provides both challenges and opportunities. After all, majority of companies perceive technology as a robotic process, characterized by automatic learning, artificial intelligence, contrary to natural intelligence. Based on the model and data the employee loads, Machine Learning will search for patterns will be capable of analyzing and making predictions, providing the possibility to recognize system anomalies or potential damage. All these changes include in both ways new Cyber risks and necessary investments. Since digital transformation agenda continues to dominate, a larger budget for IT security is more than needed along with innovative modes of governance in response to Machine Learning and AI, taking into account the automated decisions that are resulting through the interference of their usage.

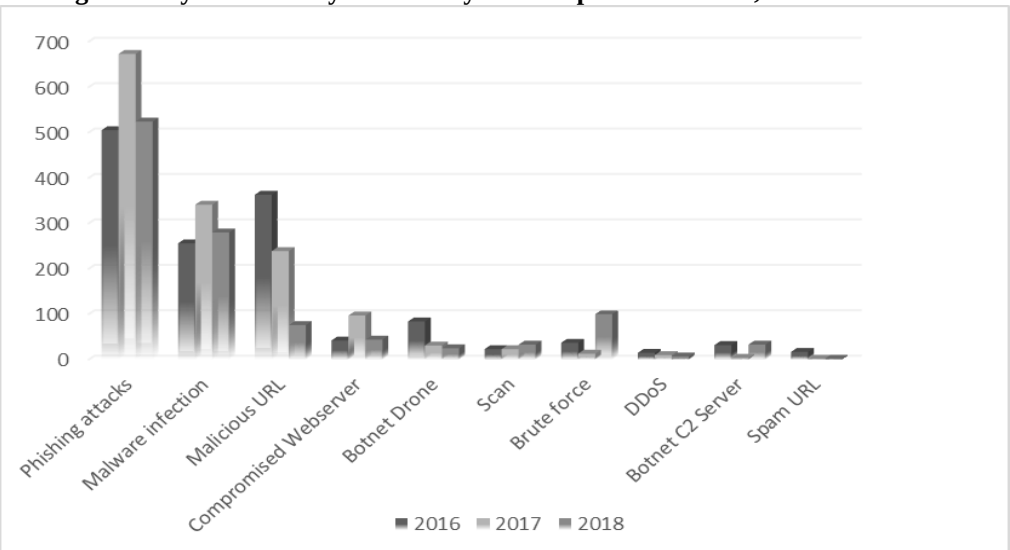
4.2 A Romanian insight

Romania is both a Cybersecurity incidents-generating country and a proxy (transit) for attackers outside of the national space through the use of vulnerable or compromised computer systems that are part of the national cyberspace. It is concerning as to find that the vulnerabilities' sources remain the same situation year after year: not updated or unsecured systems, inappropriate configurations etc. (CERT.RO, 2017). What are the causes? Without detailed data, we can presume as possible causes the following: insufficient budgets for information security issues (this being a national concern), insufficient security specialists (this being a global issue as well), insufficient training of employees and scarce knowledge about

information security specialists' in regard to the specificity of the domain their company is operating in, inappropriate organizations' culture on information security risks etc.

Cyber threats and vulnerabilities of the national cyberspace continue to register diversification, evidenced by the fact that starting with 2016 CERT.RO introduced new types of alerts. As technology developed, a complication of computer networks leads to more measures for confidentiality and integrity of information protection. For 2018, there is a novel element which is a custom-global concept following the coming into force of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 regarding the high importance of information security and networking in the European Union. A concerning increase of the compromised web servers is reported: 13 incidents in 2016 compared to 97 reported incidents in 2017, but lower for 2018, 44 cybersecurity alerts. There is a significant increase in phishing attacks and malware infections (an increasing rate of 33%) comparing 2016 to 2017, but a slow decrease in 2018 (Figure 2).

Figure 2. Dynamics of Cyber security alerts reported for 2016, 2017 and 2018



(*Source*: author projection based on CERT.RO reports)

Romania faces difficulties in protecting national IT infrastructures, generated, among others, by the lack of IT security specialists. To encourage and motivate talented young people in this field to join the teams of specialists involved in the efforts to ensure IT security, work competitions are organized. This measure would minimize security issues since for 2018 the alerts involved 175,890,000.00 alerts detected, more than double compared to 2015. CERT.RO public reports evidence are reflecting the evolution of alerts distribution. The dynamics of Cyber security

alerts between 2015 and 2017 for the Romanian cyberspace exposure is revealed in table 2.

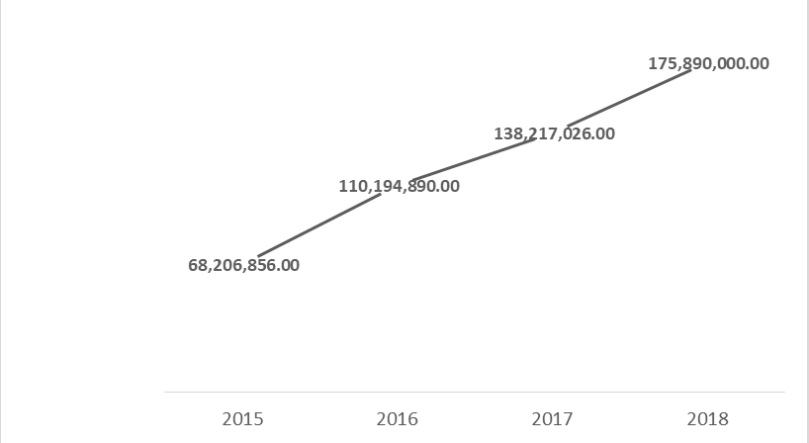
Table 2. Dynamics of Cyber security alerts during 2015-2018

Year	Cyber security alerts
2015	68,206,856.00
2016	110,194,890.00
2017	138,217,026.00
2018	175,890,000.00

(*Source*: author projection based on CERT.RO reports)

According to the Global Cybersecurity Index 2017, Romania has placed the group of maturing stage countries demonstrating developed complex commitments and engagement in cybersecurity programs and initiatives (Global Cybersecurity Index, 2017). From the European Region, Romania scored 0.585, being on 42nd global rank, following ITU Member States Global Cybersecurity Commitment Score by Region. Compared to the European Region, Romania's score is favorable considering the extensive global rank (5-165) and range of score (0.040[i] and 0.846[ii]). According to CGI evaluation, Romania presents red flags are in the following areas: standards for organizations and professionals, cybersecurity metrics, cybersecurity good practices, R&D programs, multilateral agreements. Satisfactory results are registered in areas of cybercriminal legislation, National CERT issues, child online protection, standardization bodies, public awareness campaigns, public-private relationships (GCI, 2017). The application of a proportional response to cyber security events would ensure a new and redefined paradigm for this area of competence. For the Romanian landscape, cybersecurity alerts continue to develop in terms of the reported incidents and complexity, as figure 3 presents.

Figure 3. Cyber security alerts evolution between 2015–2018



(*Source*: author projection based on CERT.RO reports)

Seeking for a detailed picture of cyber security alerts in the Romanian landscape, phishing attacks were registering 524 alerts for 2018, compared to 673 alerts reported for 2017 and 505 alerts for 2016. Is seems security solutions (e.g. employees awareness, frequent training, regular updates) that Romania starts to implement, are to some extent, effective. October 2019, is currently marking the European Cybersecurity Month (ECSM), coordinated by the Agency for European Cyber Security countries (ENISA) and the European Commission, and other members. ECSM is the annual European Union awareness campaign dedicated to promoting cybersecurity among citizens and organizations by providing up-to-date information. The 2019 campaign focuses on various themes: to raise the awareness of citizens across Europe about cybersecurity, to addresses the need to change behaviors and identifies opportunities to help users recognize the risks involved in new technologies, good cybersecurity skills needed in the daily routine of all users, guidelines on the issues that should be given attention in the context of new technologies.

Even if the number of incidents reported for webservers compromise does not provide the same alarming picture malware and phishing does, the increasing rate emphasizes (another) hackers' point, web servers. This is more concerning if we take into consideration the social and industries domains asked to notify the incidents as NIS Directive requirement (Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union): energy, banking, health, water, transports, financial market infrastructure and digital infrastructure.

It is relevant to mention that in 2016, Kaspersky analysis on web attacks (ranked by percentage of targeted users) places Romania in the countries' group of medium risk with a percentage of 27.4% (Kaspersky, 2016). During the analysis performed on CERT.RO reports, the author gathered the data and represents a top 10 security threats during 2015-2018. Detailed capture of cybersecurity alerts for the three years is presented in table 3.

Table 3. Cyber security alerts during 2016-2018

Cyber security alerts	2016	2017	2018
Phishing attacks	505	673	524
Malware infection	256	341	280
Malicious URL	363	239	76
Compromised Webserver	42	97	44
Botnet Drone	84	31	25
Scan	23	23	33
Brute force	37	13	100
DDoS	15	10	7
Botnet C2 Server	32	4	33

(*Source*: author projection based on CERT.RO reports)

Nevertheless, phishing and malware attacks continue to remain the main security issues. The malware registers an important increase in complexity and sophistication. By identifying classes of incidents, The Fraud Incident class is one of the most common types of an incident declared for 2018, followed by malware. Analyzing types of malware concerning Romanian cyberspace could be identified as preferred targets the Windows systems and the shift to Android OS (see Ghost-Push attacks). This is why the government information security agency insists on the urgent update of Windows systems both in the case of companies and individuals. The year 2017 has brought a premiere: the first attack on a Romanian hospital. The WannaCrypt "wave" affected a Romanian hospital, an automobile manufacturing plant (making unfunctional same of the robotized production lines) and Ministry of Foreign Affairs, where many organizations were affected. Comparing CERT.RO with Kaspersky evidence, the Kaspersky analysis of WannaCry ransomware attacks places Romania on the 9th place in the top of the first 20, in the group with a medium point of infection risk.

For 2018, CERT.RO presents the 1st position regarding affected systems for online or cloud services. That is due to the failure in scrutinizing and recognizes the latest threats or institutional instigations from the online/ cloud environment. Companies should not neglect the incidents provided from the payments through the banking system. This environment is also on the hacker's target and for the first time, ERP/ CRM systems were affected. Private companies are the most affected by cyberattacks (41.74%) compared to public institutions (27.39%). This result implies a less controlled environment for the private landscape and a lower developed internal tracking system. Companies (in general) might take into account the importance of the investment and the implementation strategy appropriation. Management decisions should fit the policies and the policies must conform to an optimal cybersecurity level.

CERT.RO (2018) identifies through Security Complex Mechanisms Darknet, alerts from Information Gathering and Scanning class, that the attack source originates (primarily) from China, with an impact of 63.32% of total attacks, followed by Russia (12.76%), Ukraine (5.84%), USA (5.31%), Germany, UK, Holland, France and others. Romania is responsible for 0.28% of the total attacks. Regarding Bruteforce attack, there were identified two types, which is SSH Bruteforce originated from China (91.77%) and Telnet Bruteforce (42.46%). These dynamics introduces new vulnerabilities and new paths companies must explore. Cryptojacking has increased significantly during 2018 and were identified malicious applications such as MoneroMiner, CoinMiner and BitcoinMiner. Even was declared as the oldest malware network in the whole world, EITest infection network is closed from 2018, but the infection is still active. This might affect vulnerable servers which are executing the malicious code.

WannaCry malware has not yet died. This type of attack is both a story and a present fact. For Romania, 2018 brings this presence as real damage for IPs, suggesting that this ransomware is still active, as well as Locky and VPNFilter. In case of an infection with Locky Ransomware, the wallpaper is replaced by an image where is communicated to the user that has to access one of the links. To ransom, the files are requested for a payment in Bitcoin virtual currency. As a solution, Avast is offering protection against Locky Ransomware, to detect and remove from the system. VPNFilter, a more advanced actor, is willing to destroy users' devices to cover their tracks, advancing further than simply removing malware. VPNFilter is actively infecting systems in Ukraine, running a command control (C2) particular for this country. All these phenomena are happening at an alarming rate.

5. Conclusions

Relevant worldwide literature and the reports of major players in the security market have been included in this paper and urge on the implementation of measures to defend a digital world (e.g. standardization bodies, public awareness campaigns, public-private relationships, employees awareness, frequent training, regular updates, innovative modes of governance). This present paper on cybersecurity threats uses a mix of research methodologies for the identification and evolution of the most encountered security threats in the national and international context. It is hoped that the information from this paper will raise employees and managers awareness on this critical problem, engage in discussion future research and put on alert the importance of this subject. This investigation emphasizes a set of step-by-step measures (public awareness campaigns, frequent training) that should be embracing each control system to contribute for a better understanding of the evolution of the threats.

This paper concludes on future visions and solutions that technological news is offering to the world, through implementation and appropriation of Machine Learning, Cloud services, AI, Big Data (Analytics), because of the high exposure of both financial and non-financial information, major vulnerabilities that characterizes this new, challenging and technological cyber context. Furthermore, it is important for companies to align and to be updated with the new digitalized world, by adopting different strategies and embrace Cloud solutions, the Internet of Things (IoT), AI, Big Data Analytics (BDA), Complex Adaptive Systems (CAS) and Machine Learning. In the future, it is possible humanity, thinking and technology to shift to the immersive point: connecting people with hundreds of edge devices. Through this paper, it has been emphasized that cybersecurity has no boundaries and hackers do not stop from threats appearance novelty. It is important to understand that automation has added a new security paradigm and increased the potential of being an everywhere victim (online, cloud, network, website, email). It is important to stimulate user thinking about information security. An important

vector could be proactive training in regard to information security. Users should be open, vigilant and critical to AI, Big Data Analytics (BDA) and Machine Learning technology; companies should "teach" technology and supervise learning, as an essential key to success.

The evolution of cyber alerts shows the intelligent and new strategies hackers apply. In the analysis performed, the author concluded on top 10 security threats, during 2016-2018 for the Romanian landscape and 2017-2018 for the world-wide landscape. Both investigations concluded that malware and phishing continue to disrupt in 2016 and 2017 company's existence. For 2018, the situation seems to meet a minor decline, in terms of number and security impact. It has been emphasised that Romania plays an important role in terms of transition, currently, our country is cohorting vulnerable systems that allow for the transition and evolution of another target (country) attack. From an international perspective for 2013-2018, the most encountered threats of IT and Operational Technology (OT) have been investigated and analysed during this paper, as cybersecurity becomes one of the most discussed topic of the 21st century.

Companies represent a constant target of arranged cybercrime and implicitly, cyber-attacks. As cybercrime rise in sophistication, both managers and organizations argue the easiness of attackers in achieving access at the sensitive information. Organizations have to work hard and smart to protect their information, business processes, to seek for the resistance against cybercrime. Whether all staff would be adequately prepared, updated about the risks of the involved transactions, innovative implementation of governance in place, business leaders experienced in cybercrime detection, organizations would be ready to confront security breaches and their reputation protected. Employee errors or unintentional actions would register a diminution instead of a high arise as discussed during this paper. Moreover, it is important to find a balance between protection, exposure and response strategies before the cybercrime event. The current state of preparedness must be compared with the future required state. This rigorous and objective evaluation will facilitate the right response, necessary for the improvements and the gaps that an organization accost over time.

The Romanian regulatory framework should innovate new modes of governance and establish a guideline for companies that encounter problems in security protection or seek instructions in adapting their strategy. CERT.RO embraces the custom-global concept which is characterized by limitless borders in terms of a strong global character and dynamism. The future represents global cooperation and the implementation of both sensors and detection methods. Cybersecurity development must be fully understood, although the national security target is scarcely prepared regarding potential risks, implementation of engineering solutions, protection of cybercrime infrastructure, strategies and policies regarding counter aggression.

In order to minimize cybersecurity incidents, at the EU level, Member States make efforts to harmonize the information for infrastructure protection against cybercrime. It is absolutely necessary a world-wide alignment regarding cybersecurity and not only at a local perspective because of highly percentages cybercrimes currently reported. In this context, Romania recognizes the existence of WannaCry, Malware, Phishing attacks and other unintentional or intentional actions from employees, Brute Force, DDoS, Spam or compromised webservers. The vulnerabilities presented through this paper are well known by NATO and EU level. This organization seeks a common, integrated and coordinated supports, from all member states, in order to provide a timely and accurate response to cyber-attacks. In this way, the global protection that members of the EU build will be effective in cybersecurity strategy adoption. It is crucial that everyone would be willing to share cybercrime investigation knowledge to win for protection against cybercrime.

This study opens the gate for further research in the cyber context. The author plans to continue this research, by adding new future tendencies in evolution and cybersecurity insights. Research is needed in understanding practical issues regarding how new technologies (AI, Machine Learning, Big Data Analytics) function, how are designed and how could be implemented in order to help organizations in this cyber defending. Future research may adopt the analysis of other states involved in security attacks, where the situation is really intense, such as Mauritius, United States of America, Oman, Singapore, Malaysia, Estonia, and others.

Acknowledgements

This paper was presented in the 14th International Conference on Accounting and Management Information Systems AMIS 2019, Bucharest, Romania. The author benefited of the recommendations of the participants and incorporates the feedbacks of the specialists and suggestions from active debates that took part at the conference.

References

Ahmadi, M., Ulyanov, D., Semenov, S., Trofimov, M., & Giacinto, G. (2016) "Novel feature extraction, selection and fusion for effective malware family classification", *Proceedings of the sixth ACM conference on data and application security and privacy*, pp. 183-194

Aleshkin, A. & Lesko, S. (2019) "Predicting the growth of total number of users, devices and epidemics of malware in internet based on analysis of statistics with the detection of near-periodic growth features", *2019 XXI International Conference Complex Systems: Control andModeling Problems (CSCMP)*, pp. 347-352

Alhogail, A. & Abdulrahman, M. (2014) "A framework of information security culture change", *Journal of Theoretical and Applied Information Technology*, vol. 64, no. 2: 540-548

Alloghani, M., Al-Jumeily, D., Hussain, A., Mustafina, J., Baker, T. & Aljaaf, A. J. (2020) "Implementation of machine learning and data mining to improve cybersecurity and limit vulnerabilities to cyber attacks", *Nature-Inspired Computation in Data Mining and Machine Learning. Studies in Computational Intelligence*, vol. 855: 47-76

Anderson, B., & McGrew, D. (2017) "Machine learning for encrypted malware traffic classification: accounting for noisy labels and non-stationarity", *Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 1723-1732

Azvine, B. & Jones, A. (2019) "Meeting the future challenges in cyber security", *Industry 4.0 and Engineering for a Sustainable Future*, pp. 137-152

Bassett, R., Bass, L., & O'Brien, P. (2006) "Computer forensics: An essential ingredient for cyber security", *Journal of Information Science & Technology*, Vol. 3, No. 1

Benjamin, V., Li, W., Holt, T., & Chen, H. (2015) "Exploring threats and vulnerabilities in hacker web: Forums, IRC and carding shops", *2015 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pp. 85-90

Bitdefender (2016) "Virtualization makes CIOs role key (A survey on US IT decision makers)", available on-line at https://download.bitdefender.com /resources/files/News/CaseStudies/study/141/small-Bitdefender-Whitepaper-Virt-CIO-A4-en-EN-screen-compressed.pdf (accessed on 01 February 2019)

Bitdefender, (2018) "CISOs should report directly to the ceo, study shows", available on-line at https://businessinsights.bitdefender.com/cisos-should-report-directly-to-the-ceo-study-shows (accessed on 01 February 2019)

CA Technologies (2018) "Insider threat report 2018", available on-line at https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf (accessed on 03 January 2019)

CERT.RO (2015) "RAPORT cu privire la alertele de securitate cibernetică procesate de CERT-RO în anul 2015" [Report on cybernetics security alerts processed by CER-RO in 2015], available on-line at https://cert.ro/vezi/document/raport-alerte-cert-ro-2015 (accessed on 04 January 2019)

CERT.RO (2016) "RAPORT cu privire la alertele de securitate cibernetică procesate de CERT-RO în anul 2016" [Report on cybernetics security alerts processed by CER-RO in 2015], available on-line at https://cert.ro/ vezi/document/raport-alerte-cert-ro-2016 (accessed on 04 January 2019)

CERT.RO (2017) "Raport privind evoluția amenințărilor cibernetice în 2017" [Report on evolution of cybernetic threats], available on-line at https://cert.ro/vezi/document/raport-alerte-2017 (accessed on 04 January 2019)

CERT.RO (2017) "The New Global Challenges in Cyber Security 2017, Conference Report", available on-line at https://cert.ro/vezi/document/certcon7-report (accessed on 04 January 2019)

CERT.RO (2018) "Threats evolution in the Romanian cyberspace" available on-line at https://www.cert.ro/vezi/document/cert-ro-cyberthreats-2018 (accessed on 01 March 2020)

CERT.RO (2018) "VPNFilter - o nouă amenințare care vizează routerele utilizatorilor" [VPN filter – a new threat for routers], available on-line at https://www.cert.ro/citeste/alerta-vpnfilter (accessed on 01 March 2020)

Demertzis, K., Kikiras, P., Tziritas, N., Sanchez, S. L., & Iliadis, L. (2018) "The next generation cognitive security operations center: network flow forensics using cybersecurity intelligence", *Big Data and Cognitive Computing*, vol. 2, no. 4: 35

Donalds, C., Osei-Bryson, K. (2006) "Criminal Investigation Knowledge System: CRIKS", *In: Proceedings of the 39th Hawaii International Conference on System Sciences*, pp. 155-164

Drtil, J. (2013) "Impact of information security incidents – theory and reality", *Journal of Systems Integration*, no. 1: 44-52

ENISA (2019) "A fost lansată luna europeană a securității cibernetice 2019" [The European month of cybernetic security was launched], available on-line https://www.enisa.europa.eu/news/ecsm-2019-pr/cnect-2019-00640-00-00-ro-tra-00.pdf (accesed on 21 March 2020)

E&Y (2014) "Get ahead of cybercrime", available on-line at https://www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/%24FILE/EY-global-information-security-survey-2014.pdf (accessed on 10 March 2019)

E&Y (2017) "Cybersecurity regained: preparing to face cyber-attacks - 20th Global Information Security Survey 2017–18", available on-line https://www.ey.com/Publication/vwLUAssets/GISS_report_2017/$FILE/REPORT%20-%20EY%20GISS%20Survey%202017-18.pdf (accessed on 24 December 2018)

E&Y (2018) "Is cybersecurity about more than protection? - EY Global Information Security Survey 2018-19", available on-line at https://www.ey.com/ Publication/vwLUAssets/ey-global-information-security-survey- 2018-19/$FILE/ey-global-information-security-survey-2018-19.pdf (accessed on 10 January 2019)

Ghasemi, M., Shafeiepour, V., Aslani, M., & Barvayeh, E. (2011) "The impact of Information Technology (IT) on modern accounting systems", *Procedia-Social and Behavioral Sciences*, vol. 28: 112-116

Guo, H., Cheng, H. K., & Kelley, K. (2016) "Impact of network structure on malware propagation: A growth curve perspective", *Journal of Management Information Systems*, vol. 33, no.1: 296-325

Hou, S., Ye, Y., Song, Y., & Abdulhayoglu, M. (2017) "Hindroid: An intelligent android malware detection system based on structured heterogeneous

information network", *Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 1507-1515

Hunton, P. (2012) "Data attack of the cybercriminal: Investigating the digital currency of crime", *Computer Law and Security Review,* 28: 201-207

ISACA, RSA (2015) "State of cybersecurity: Implications for 2015. An ISACA and RSA Conference Survey", available on-line at https://www.isaca.org /cyber/Documents/State-of-Cybersecurity_Res_Eng_0415.pdf (accessed on March 2019)

ITU (2017) "Global Cybersecurity Index 2017", available on-line at https://www.itu.int/dms_pub/itu-d/opb/str/d-str-gci.01-2017-pdf-e.pdf (accessed on March 2019)

Joseph, D. P., & Norman, J. (2019) "An analysis of digital forensics in cyber security", *In First International Conference on Artificial Intelligence and Cognitive Computing,* pp. 701-708

Kaspersky (2016) "Kaspersky security bulletin 2016", available on-line at https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07182317/KASPERSKY_SECURITY_BULLETIN_2016.pdf (accessed on 21 January 2019)

Kaspersky (2016) "DDoS 2015 intelligence report for Q2 2016", available on-line at https://securelist.com/kaspersky-ddos-intelligence-report-for-q2-2016/ 75513/ (accessed on 12 March 2019)

Kaspersky (2018) "The State of Industrial Cybersecurity 2018 - Kaspersky-ICS-Whitepaper", available on-line at https://ics.kaspersky.com/media/2018-Kaspersky-ICS- Whitepaper.pdf (accessed on 12 March 2019)

Kaspersky (a) (2018) "DDoS Attacks in Q3 2018", available on-line at https://securelist.com/ddos-report-in-q3-2018/88617/ (accessed on 13 March 2019)

Kaspersky (b) (2018) "DDoS Attacks in Q4 2018", available on-line at https://securelist.com/ddos-attacks-in-q4-2018/89565/ (accessed on 13 March 2019)

Kaspersky Security Bulletin (2019) "Advanced threat predictions for 2020", available on-line at https://securelist.com/advanced-threat-predictions-for-2020/95055/ (accessed on 03 February 2020)

Kumar, S. & Carley, K. M. (2016) "Approaches to Understanding the Motivations behind Cyber Attacks", *2016 IEEE Conference on Intelligence and Security Informatics (ISI),* pp. 307-309

Ledin, G. (2011) "The growing harm of not teaching malware", *Communications of the ACM,* vol. 54, no. 2: 32–34

Mangiuc, D. (2017) "Accountants and the cloud – Involving the professionals", *Accounting and Management Information Systems*, vol. 16, no. 1: 179-198

Masys, A., Ray-Bennett, N. S., Shiroshita, H. & Jackson, P. (2014) "High impact/low frequency extreme events: enabling reflection and resilience in a hyper-connected world", *Procedia Economics and Finance,* vol. 18: 772-779

Morrow, B. (2012) "BYOD security challenges: Control and protect your most sensitive data", *Network Security*, no. 12: 5-8

MIT Technology Review (2018) "Six cyber threats to really worry about in 2018" available on-line on https://www.technologyreview.com/s/609641/six-cyber-threats-to-really- worry-about-in-2018/ (accessed on 15 January 2019)

Netwrix (2018) "Top 10 Most Common Types of Cyber Attacks" available on-line at https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/ (accessed on 21 January 2019)

Park, H., Cho, S., Kwon, H. (2009) "Cyber forensics ontology for cyber criminal investigation", *International Conference on Forensics in Telecommunications, Information, and Multimedia*, vol. 8: 160–165

Ponemon Institute (2018) "Cost of a Data Breach Study: Global Overview. Benchmark research sponsored by IBM Security Independently conducted by Ponemon statute LLC", available on-line at https://www.intlxsolutions. com/hubfs/2018_Global_Cost_of_a_Data_Breach_Report.pdf (accessed on 16 March 2019)

Ponemon, L., (2018) "Calculating the Cost of a Data Breach in 2018, the Age of AI and the IoT", *Security Intelligence*, available on-line at https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/ (accessed on 20 March 2019)

PwC (2015) "Information Security Breaches Survey 2015 – Full Report", available on-line at https://assets.publishing.service.gov.uk/government/uploads/ system/uploads/attachment_data/file/432412/bis-15-302-information_security_breaches_survey_2015-full-report.pdf (accessed on 07 February 2019)

PwC (2015) "Cyber Security Breaches Survey 2015 - PwC", available on-line at https://dm.pwc.com/HMG2015BreachesSurvey/ (accessed on 21 February 2019)

PWC (2016) "Toward new possibilities in threat management", http://www.pwc.com/ee/et/publications/pub/gsiss-report-cybersecurity-privacy-possibilities.pdf (accessed on March 2019)

Richins, G., Stapleton, A., Stratopoulos, T. C. &Wong, C. (2016) „Data Analytics and Big Data: Opportunity or Threat for the Accounting Profession?", *Journal of Information Systems*, vol. 31, no. 3: 63-79

Rîndașu, S. M. (2017) "Emerging information technologies in accounting and related security risks-what is the impact on the Romanian accounting profession", *Journal of Accounting and Management Information Systems*, vol. 16, no. 4: 581-609

Shan, Z., & Wang, X. (2013) "Growing grapes in your computer to defend against malware", *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 2: 196-207

Security Intelligence (2016) "Know Your Enemy: Understanding the Motivation behind Cyberattacks", available on-line athttps://securityintelligence.com/ know-your-enemy-understanding-the-motivation-behind-cyberattacks/ (accessed on 08 March 2019)

Stephens, P., Induruwa, A. (2007) "Cybercrime investigation training and specialist education for the european union", *Second International Workshop on Digital Forensics and Incident Analysis (WDFIA)*, pp. 28-37

Symantec (2019) "Internet Security Threat Report", available on-line at http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D_ISTR23_Main-FINAL-APR10.pdf?aid=elq (accessed on 24 February 2020)

Takahashi, T., Kadobayashi, Y. & Fujiwara, H. (2010) "Ontological approach toward cybersecurity in cloud computing", *In Proceedings of the 3rd international conference on Security of information and networks,* pp. 100-109

The State of Security (2019) "Report: Concerted Global Cyber Attack Could Disrupt Global Economy", available on-line at https://www.tripwire.com/state-of-security/featured/report-cyber-attack-disrupt-global-economy/ (accessed on March 2019)

Veeramany, A., Unwin, S.D, Coles, G.A, Dagle, J.E, Millard, W.D, Yao, J., Glantz, C.S & Gourisetti, S.N.G. (2016) "Framework for modeling high-impact, low-frequency power grid events to support risk informed decisions", *International Journal of Disaster Risk Reduction*, Vol. 18: 125-137

Von Solms, B., von Solms, B. R. (2018) „Cybersecurity and information security – what goes where?", *Information & Computer Security*, vol. 26. no. 1: 2-9

Shayan, J., Azarnik, A., Chuprat, S., Karamizadeh, S. & Alizadeh, M. (2013) „Identifying Benefits and risks associated with utilizing cloud computing", *The International Journal of Soft Computing and Software Engineering*, vol. 3, vo. 3: 416-421

Thielens, J. (2013) "Why API are central to a BYOD security strategy", *Network Security*, no. 8: 5-6

Krollner, B., Vanstone, B. J., & Finnie, G. R. (2010) "Financial time series forecasting with machine learning techniques: a survey", *European Symposium on Artificial Neural Networks*, pp. 25-30

Yeager, R. (2006) "Criminal Computer Forensics Management", *InfoSecCD '06: Proceedings of the 3rd annual conference on Information security curriculum development*, pp. 168-174

[i] assigned to the highest global rank correlated to the lowest commitment

[ii] assigned to the lowest global rank correlated to the highest commitment