Audit financiar, XIX, Nr. 1(161)/**2021**, *119-129*
ISSN: 1583-5812; ISSN on-line: 1844-8801

Risks Associated with Threats Related to Disruptive Technologies in the Current Financial Systems Context

Lavinia Mihaela CRISTEA,
Ph. D. Student,
The Bucharest University of Economic Studies, Romania,
e-mail: cristealaviniamihaela@yahoo.com

Abstract

The subject of the study is the analysis of the risks associated with threats generated by disruptive technologies in the context of current financial information systems of the entities. The phenomenon of cybercrime, facilitated by the development of Artificial Intelligence, Deep Learning and the disruptive frequency of security incidents represents the foundation of this paper. The aim of the article is to integrate, compare and investigate the impact of disruptive technologies, current security risks and incidents, and to design measures in order to manage risk. The results of this paper highlight Advanced Persistent Threats (APTs), malware, ransomware, sabotage of external actors, third-party threats in the top 5 most common security incidents. The paper acknowledges the complexity of digitization and transposes a practical model of risk management. The paper contributes to informing stakeholders about the forced penetration of hackers into victims' devices, under the pretext of COVID-19.

Key words: *risks associated with the financial system; cyber threats; disruptive technologies; current information systems; Artificial Intelligence impact; Deep Learning impact; COVID-19*

JEL Classification: *D83, G32, K24, M41, M42, O33*

To cite this article:
Cristea, L.M., (2021), Risks Associated with Threats Related to Disruptive Technologies in the Current Financial Systems Context, *Audit Financiar*, vol. XIX, no. 1(161)/2021, pp. 119-129, DOI: 10.20869/AUDITF/2021/161/002

To link this article:
http://dx.doi.org/10.20869/AUDITF/2021/161/002
Received: 24.09.2020
Revised: 14.10.2020
Accepted: 23.01.2021

1. Introduction

The adoption of complex digitization processes has grown rapidly in the last period of time (Forbes, 2020), being determined by the high requirements regarding the reporting procedure and presentation of financial statements for users and stakeholders, but also from the companies' aspiration to stay in trend and in market competition, becoming dependent on IT. The digitization processes, which underlie the current financial-accounting information systems of the entities, consist in digitizing the data or the transition from analog data to data in digital format, representing a process of collecting the available information into digital access. Following the digitization of analog data, the resulting data were integrated into software applications designed to use automated work processes or extensively automation in many industries, to optimize productivity and organizational flexibility.

Entities providing accounting and auditing services (and other services) are in a continuous search for automation, as is easier to achieve the commercial value added of existing investments as a result of Robotic Process Automation (RPA). At the same time, the industry is aligning towards joining RPA with Artificial Intelligence (AI) and Machine Learning, following these two borders, to a Robotic Intelligent Automation. The application of the above-mentioned emerging technologies contributes to a (full) ingenious operational flow and an additional value added to the business.

AI designates a generic term for systems or machines that mimic human intelligence, in order to perform activities that, based on the information collected, might significantly improve work processes. The principle of AI is to reproduce the way people act, and even refine work tasks, providing meaning to the data in a way that would not have been conceived until present. Machine Learning recognizes models resulting from previously data processed by auditors so that might formulate predictions, in order to automate extremely complex business processes that follow a certain routine. By Robotic Intelligent Automation we understand the consolidation of robotics, automation and AI. In the financial sector, by adopting these disruptive technologies, professional accountants and auditors would acquire a more advanced freedom of thought and innovation.

Companies will increasingly invest more in intelligent automation of internal processes, methodologies and current practices, to increase the company's reputation, maintaining customer confidence in financial reporting and capital placement by investors. In this regard, a prevention plan is imperative to combat cyber threats at both the individual and organizational levels (Goodman, 2016), given that by 2020, cyber incidents are at the forefront, compared to 2013, where they ranked 15th. Since locally (i.e., Romania) is not acquired a strong information on the topic "The risks associated with threats related to disruptive technologies in the current financial systems context", transparency being limited in this respect, the author discusses the cyber financial current through documentation and critical analysis of the latest digital publications, which might be transposed to the accountant or auditor profession.

The objective of this paper is (1) to identify the current cyberspace that seems unsafe in terms of training professional accountants and auditors, in order to prevent threats arising from emerging technologies, (2) to analyze the risks from security incidents caused by the evolution of disruptive technologies and (3) to design a risk management analysis model in order to be assumed an acceptable level of risk by entities. Through this article, the author contributes to the literature by better information about the current entities system's and designing an analysis model regarding risk management, the aim of this paper being to develop an awareness at the individual and at the company level, to mitigate and why not, to reject the generated threats by disruptive technologies.

The paper places current security incidents in a context of interest for technology users and companies that persevere in the ongoing fight against cyber risks associated with the threats generated by disruptive technologies, arising from the harsh development of the online environment, digitization processes and current financial information systems. The first section focuses on the literature review, which considers the analysis of the framework constituted by "Risks associated with threats related to disruptive technologies in the current financial systems context", at a global level. The second section discusses the research methodology of this paper. Section three presents the obtained results, outlines evolutions and comparisons of the most common security incidents reported by Kaspersky and Fraud Watch International, simultaneously with a risk

management strategy designed in an analysis model, which might be considered by companies in order to assess, prevent, transfer and assume the risk generated by disruptive technologies. The article concludes by stating the conclusions and future research directions.

2. Scientific literature review

The risks associated with threats related to disruptive technologies in the current financial systems context continue to affect companies and technology users around the world (Hawker, 2000; Goodman, 2016; Mohammed, 2018; Rainer, 2020). In this regard, the risks associated with the threats generated by disruptive technologies are closely linked to the cybercrime and cybersecurity phenomenon (ISACA, 2015; PwC, 2016; ITU, 2017; E&Y, 2017; von Solms and von Solms, 2017; Demertzis, 2018; E&Y, 2018; Kaspersky, 2018; Kaspersky, 2019; Alloghani, 2020), a phenomenon that seems to become more frequent, more sophisticated in the way hackers attack, and on the impact generated. In order to avoid these risks as much as possible, it is recommended to design and integrate appropriately-developed IT systems, as well as to establish in time measures regarding the confidentiality, integrity, availability, processing and data storage resulting from operational processes. Joining Cloud platforms might ensure data security (Wang et al., 2011; Faccia et al., 2019; Zhang et al., 2019; Shkarlet et al., 2020) and might be an effective business solution by estimating future resources data requests, needed for the proper activity of the enterprise, using a predictive approach (Gadhavi, 2020). Before concluding contracts with third parties or with Cloud providers, it is recommended to pre-verify the risks associated with those contracts or with Cloud platforms aimed at simplifying business processes.

Despite the offered advantages (e.g. allocation of a shorter time for the preparation and presentation of financial statements, operational processes level automation, computerized systems usage, bookkeeping level efficiency) by disruptive technologies (i.e. Cloud Computing, Big Data, IoT, AI, Machine Learning, Robotic Process Automation) (PwC, 2016; Richins et al., 2016; Mangiuc, 2017; Azvine and Jones, 2019), the generated risks finds support in various computer threats (e.g. Advanced Persistence Threats, phishing, malware, ransomware, DDoS, Man-In-The-Middle, SQL injection, mobile devices cyber-attacks, electronic fraud) (Rîndaşu, 2016; Guo et al., 2016; Hou et al., 2017; Stanciu and Tinca, 2017; Azvine and Jones, 2019), generated by disruptive technologies, emerged in cyber-attacks, which compromise the organization's information systems, as a result of the increasingly complex digitization processes emergence (Goodman, 2016).

For 2020, Kaspersky Lab investors (2019) report that companies and users confront extensive risks, represented by Advanced Persistent Threats (APTs) of the WildPressure type, Backdoor.Win32.Agent malware, spam, phishing, computer incidents, cyber attackers seeking access to biometric data. Lately, hackers have substantially invested in methods that "cheat" anti-fraud systems. As authentication theft is not enough, through access to Personally Identifiable Information (PII), attackers need a fingerprint to withdraw money from the bank. Thus, during 2019, was identified Genesis, an undercover e-store that sells fingerprints of worldwide users, representing one of the associated risks (i.e., theft of fingerprint) with the generated threats (i.e., theft of authentication) by disruptive technologies (i.e., Tenebris Linken Sphere browser) faced by online banking users. More than 60,000 stolen profiles have already been identified, the profiles include browser fingerprints, user and password authentications on various sites, cookies, credit card information, etc. By uploading the fingerprint into the Tenebris Linken Sphere browser, criminals are able to log in as banking legitimate users. This type of attack shows that criminals have in-depth knowledge about the internal functionality of banking systems, which represent a real challenge to protect against such attacks. The best prevention method would be the Multi-Factor Authentication (MFA).

In fact, many of the threats generated by disruptive technologies are against Android. For example, for the third quarter (September, 2019), Zerodium, a brokerage firm, indicated that a day without access to Android would cost more than a day without access to iOS (Apple Inc. operating system), that is $2.5 million. This amount represents a significant increase, which previously would have been paid against an attack on iOS two million dollars, $2 million. On the same day, a threat was identified in the v412 driver (Video4Linux), an Android media driver. If this vulnerability had not been identified in time, it could have allowed user privileges to escalate. The Android generated threat is due to the lack

of updates from September, which should have included this type of vulnerability in the Google's security update. A few days later, another Android vulnerability was identified that would have allowed attackers to give full access to the Samsung, Huawei, LG and Sony smartphone users e-mails by sending a text message (Kaspersky 2019 a).

The hackers are the actors who seek to threaten, create costly globally damage and find weaknesses in terms of information security especially in companies where data vulnerability might be easily endangered. Cyber attackers are constantly concerned about initiating attacks against Android or iOS, or to the area of politics, military, hospitals around the world, where WannaCry is already history in this regard (CERT.RO, 2018; Azvine and Jones, 2019; Kaspersky, 2019). Most of the time, the risk of being attacked is taking place, leading to litigation or lawsuits (Forbes, 2020). Cyber incidents are listed no. 1 in ranking risks that companies around the world are afraid of, the emergence of a cyber-attack representing a real risk that threatens the economic activity (Allianz Risk Barometer, 2020).

3. Research methodology

This article aims to address the latest episode in "The risks associated with the threats generated by disruptive technologies and digitization processes" topic. Digital currents issued by the software company Kaspersky Lab are debated, a company that has proven over time professionalism in the design and implementation of effective security programs. We consider that for the understanding of current cyber security phenomenon that underlies these risks, is necessary to examine the current cyber state and cyber attackers' movements that seem to be increasingly complex, sophisticated, fast and documented. This examination was performed by investigating the reports issued by Kaspersky Lab for the last three years - 2017, 2018, 2019. The research method of this paper is based on fundamental qualitative research and critical observation, applied to investigate trendy digital reports and practices, which have as a purpose user's information about the threats generated by disruptive technologies, towards a better protection against vulnerabilities, which seem to monopolize the computer systems of the entities.

The article is divided into (1) analysis and comparison of Kaspersky Lab security reports for the period 2017-2019, (2) examination of security incidents presented by Kaspersky Lab and Fraud Watch International and (3) threats generated by the Artificial Intelligence and Deep Learning globally impact. Data source finds its origins in online digital publications specialized bodies and other current publications concerned with stopping these attacks. In 2020, due to the COVID-19 pandemic, the threats generated by this virus induced a deep fear around the world, hackers finding the perfect opportunity for repeated infiltrations and technology users attacks, (users) particularly interested in this topic and protection against the virus. The article provides details on the complexity of the risks associated with the adoption of disruptive technologies in the context of current financial information systems. For the analysis of the current phenomenon and in order to identify the present reported threats, security reports issued by the specialized security company Kaspersky Lab were taken into account, as mentioned above, but also records of the Internet security organization, Fraud Watch International, specialized in online protection against fraud.

This paper investigates the threats generated by disruptive technologies, especially Artificial Intelligence and Deep Learning, through a documentary research of the latest technological currents that signal the threats generated by digitization processes. International databases such as ProQuest, Springer Link, ResearchGate and Google Scholar were consulted to identify the literature suitable for this study. Sorting items was manually performed by the author, and only articles that discuss the risks associated with threats related to disruptive technologies in the context of current financial accounting information entities system by first ensuring that key information is included.

The paper initiates discussions and explores the risks associated with the threats posed by disruptive technologies on the financial accounting system and the development of digitization processes, emphasizing (1) the evolution of the most common five security incidents, (2) recommendations issued by banks (e.g., ING Bank), companies and specialized organizations (e.g., Europol, CERT.RO) in terms of information security. The terms "vulnerability", "alerts", "hackers", "cyber attackers" are used alternately in this paper. Considering that it has been noticed reluctance on the current state of cyber-attacks and a large reporting number of security incidents faced by companies and worldwide users, it was impossible covering all security events.

4. Results and discussions

The focus of this paper is the risks that arise once with the development of digitization associated to disruptive technological threats and reported by informatics systems, by both the organizational and individual level. In the new COVID-19 pandemic context, ING Bank took action. Specifically, the bank informs about the new ways of attacking, hackers using this epidemiological pretext to send phishing e-mails to ING customers, under the subject regarding protection against this virus (i.e., COVID-19). Cyber Attackers are using current and the current trending topic on which there is an instant action (by clicking on the infected link). The e-mails appear to be sent from trusted sources, but by a closer look, it could be detected e-mails from illegitimate sources. Phishing e-mails require users to take various actions, such as accessing links, downloading files or images (which may be infected with a virus), providing confidential data (e.g., bank details, card names or passwords). ING Bank warns about these suspicious actions taking place on a large scale, once with the emergence of COVID-19 virus.

Also, under the COVID-19 pandemic pretext, cyber attackers send false advertisements (e.g., "Measures against COVID-19", "Donate 2 euros"), under the WHO (World Health Organization) logo, notifies CERT.RO (2018) and Europol (2020). These false advertisements baffle online users, hackers turning to so-called fund-raising campaigns, promotion of investment products, gloves purchase, treatments, vaccines, masks.

Phishing e-mails are sent under the hospitals or medical clinics name, users being informed about a relative or acquaintance who has been infected with this virus, asking from the recipient money for treatment. Professional organizations advice is to ignore these malicious campaigns, to not open unknown links from e-mails and to check the sending source. For users who intend to purchase online or to donate during this period and beyond, prior documentation before making the transaction is recommended. Installing an antivirus or security solution would provide anti-phishing, anti-malware and anti-spam protection.

Table no. 1 examines the alarming evolution of phishing e-mails sent by attackers claiming to be bank personnel (Santander Bank, Wells Fargo Bank), financial services companies (American Express), courier (FedEx) or video streaming (Netflix), software for sending and receiving e-mails (Outlook, Global E-mail Server) or from an operator of an online payment system (PayPal). These phishing alerts are only some of the millions received and reported worldwide victims (i.e., organizations, individuals). Risks associated with such threats generated by the advent of online payment methods, available courier service, information download or view, vary in the manner and diversity of attack, the ultimate goal being device infestation and theft of personal data. Privacy is not respected by cyber attackers, they seek to permeate all sectors, undermining users' technology rights. The leader in anti-phishing protection, Fraud Watch International, notifies about the latest phishing activity (**Table no. 1**).

Table no. 1. Evolution of phishing alerts for March 2020

Phishing Incidents	The subject of the e-mail	Date
Microsoft - File "Lewis Invoice 076689.pdf" Has Been Shared With You	Install Update for Microsoft Outlook	26 March 2020
Netflix - Please Verify Your Account?	Netflix account verification	24 March 2020
Global E-mail Server (Webmail Login) - Urgent Account Verification Needed!!!	Urgent account verification	20 March 2020
PayPal - Your Account cannot be used until you verify it	Urgent account verification to be used	18 March 2020
Outlook - Notification: Release Your 12 held E-mails	E-mail notification	17 March 2020
1 New Security Message from Wells Fargo Bank	Security message from Wells Fargo Bank	17 March 2020
Banco Santander S.A - Aviso Santander Way (41855)	Information from Santander S.A.	03 March 2020
American Express - ***Your Account Has Been Flagged***	The American Express account needs your attention	02 March 2020
FedEx - FedEx Support on Coronavirus	Coronavirus support	02 March 2020

Source: Author's projection based on https://fraudwatchinternational.com

Phishing alert has been identified by the FanCourier company, under whose name hackers send payment messages or opening of attachments to users who have placed orders or who have had at least one order operated by the company (FanCourier, 2019). To avoid the risk of infestation or damage to personal data, it is recommended to pay more attention to these e-mails, to identify unknown e-mail addresses that transmit information about the so-called expeditions operated by FanCourier. The e-mails do not come from the FanCourier company, but from some cyber attackers specialized in malicious phishing campaigns. Hackers use the FanCourier name to distribute Trojan-infested files. The risk of infection is huge, it is recommended to avoid opening files from unknown senders or access to online deals that seem untrue, whatever form that was the basis of their receipt (e.g., message received telephone link submitted online). Following the warning issued by ING Bank, FanCourier, Europol, CERT.RO, it is recommended for devices non-stop connected to the Internet and used for browsing purposes to be updated and to include effective security solutions.

About the impact of Artificial Intelligence today, it could be said that this technology could not fully replace human workload. By looking more carefully at this phenomenon, details are known about a GPT-2 robot creation, which might generate coherent text paragraphs, might translate from various languages and is able to answer various questions and even develop abstracts (Prangate, 2019). OpenAI, the company that designed it, points out that the robot is able to write online false news and create confusion, claiming it could be anyone. There is no doubt the ability of this robot, showing how advanced it is, but nor the result obtained is a perfect one. It is brought into discussion a risk associated with the disruptive technology, Artificial Intelligence, which humanity may face, by creating a confusion state. There is a risk that should not be underestimated, even if in the first instance the effect is unexpected.

Another situation transposed by Artificial Intelligence is the generation of images through Deep Learning algorithm, GAN (Generative Adversarial Network). The results of this algorithm could be used for both positive and negative purposes. Positive, by exempting costs for fashion designers, advertising agencies or clothing manufacturers, they use GAN to create the necessary models and promote clothing items. Negatively, malicious actors might use the algorithm for a broad propaganda, images obtained after running this software undermining public confidence respecting these digital tools.

Head of research at Microsoft, Eric Horvitz, believes that the development of Artificial Intelligence brings into discussion certain risks or legal, psychological and ethical nature (Bellini, 2018). Personal data identification must remain personal. It might be considered that Artificial Intelligence, in one form or another, might have access to confidential data (e.g., home address, bank account, daily routine and housework, illnesses, emotional state). The question will be to what extent Artificial Intelligence will penetrate people's lives, but also what will be the rights and freedoms in a world of Artificial Intelligence.

With the development of this disruptive technology, aspects of redefining jobs and creating new ones must also be considered. It is well known that the fourth industrial revolution will lead to the replacement of millions of jobs (Kaeser, 2018; Borak, 2018), humanity needing better education, vocational and academic training, innovation and adaptation to everything is new. Since 2022, Singapore will introduce driverless buses (BBC, 2017), while in Sweden, since 2018 there is risk involving the gradual disappearance of jobs that require drivers. Another question that derives from all these inventions and implicitly, risks, generated by Artificial Intelligence, is whether entrepreneurs will prefer robots or human beings in their daily work. It seems that there are already companies that have moved towards this trend (The Guardian, 2017), preferring to work with Artificial Intelligence, from the perspective of lower costs, an efficiency that increases considerably, requiring no breaks, annual leave or monthly salary.

A robot becomes a legal issue, where for the first time Sophia was presented, a robot receiving the citizenship of Saudi Arabia (Weisberger, 2017), being considered a citizen with full rights and with its own personality. In Romania, for the first time, it seems that there will be a form of Artificial Intelligence as an ambassador, who will recommend places to visit, will answer various questions about Romania in order to satisfy the foreigners' interest, it will talk about the habits and lifestyle of Romanians (EMEA, 2017).

Regarding the dynamics of security incidents, the Kaspersky Lab study reveals the most feared security incident, Advanced Persistence Threats (APTs), which ranks first in top 5, for 2018 and 2019, while in 2017, the malware were first reported. APTs represent a recent class of threats that seems to have gained a higher

impact, a maximum of 68% for 2019 compared to malware and ransomware, with a percentage of 66%, respectively 70%. This ranking of APTs has been maintained for the last two years, 2018 and 2019, and is due to new hackers' attack methods, the complexity of the attacks and the accurate target (**Table no. 2**).

Table no. 2. Dynamics of the 5 most frequent security incidents between 2017-2019

Security incidents	2017	2018	2019
APTs	32%	66%	68%
Malware	56%	65%	66%
Ransomware attacks	33%	64%	70%
Sabotage by external actors	41%	56%	35%
Threats from third parties/ partners	44%	44%	44%

Source: Author's projection based on Kaspersky Lab security reports

In the malware case, the evolution registers higher values every year. The purpose of these malware attacks is information theft, a situation that particularly faces the financial-accounting sector. The hacker seeks for weaknesses in the entities' computer system in order to enforce an attack plan, by installing the malware and completing the perfect attack (e.g., password theft, (theft of) banking data, financial information, investment programs data, audit plans or other confidential information). An example of malware is the Trojan (e.g., Poweliks, FakeAV), a malicious program that disguises as a seemingly legitimate software. This type of infestation is a real challenge in detecting the type of attack, misleading users about the true intent. Once this infectious software enters the system, it is activated, which allows the hacker to extract data from the victim's device.

Ransomware attacks ranks 3rd in Kaspersky Lab hierarchy and continue to increase. Ransomware is a new form of malware that seeks to install malicious software on the victim's device (e.g., computer, phone, tablet) by tracking data encryption. In exchange for restoring access, the hacker requires a certain amount of money. If the victim does not pay on time or does not prove the payment, there is a risk that the data might not be recovered, access to data being allowed only after the hacker receives the requested amount. In the ransomware category, CryptoWall 3.0 is a very dangerous ransomware that has generated $325 million from ransom schemes.

Sabotage by external actors ranks 4th in the evolution of security incidents. The evolution of this type of attack presents an evolution for 2018, where for 2019 the sabotage by the external actors registers a decline of 21 percent. However, this incident, frequently in worldwide companies, continues to register risks caused by insufficient computer protection. Companies should analyze the risks they face and adopt implementation strategies for safer protection.

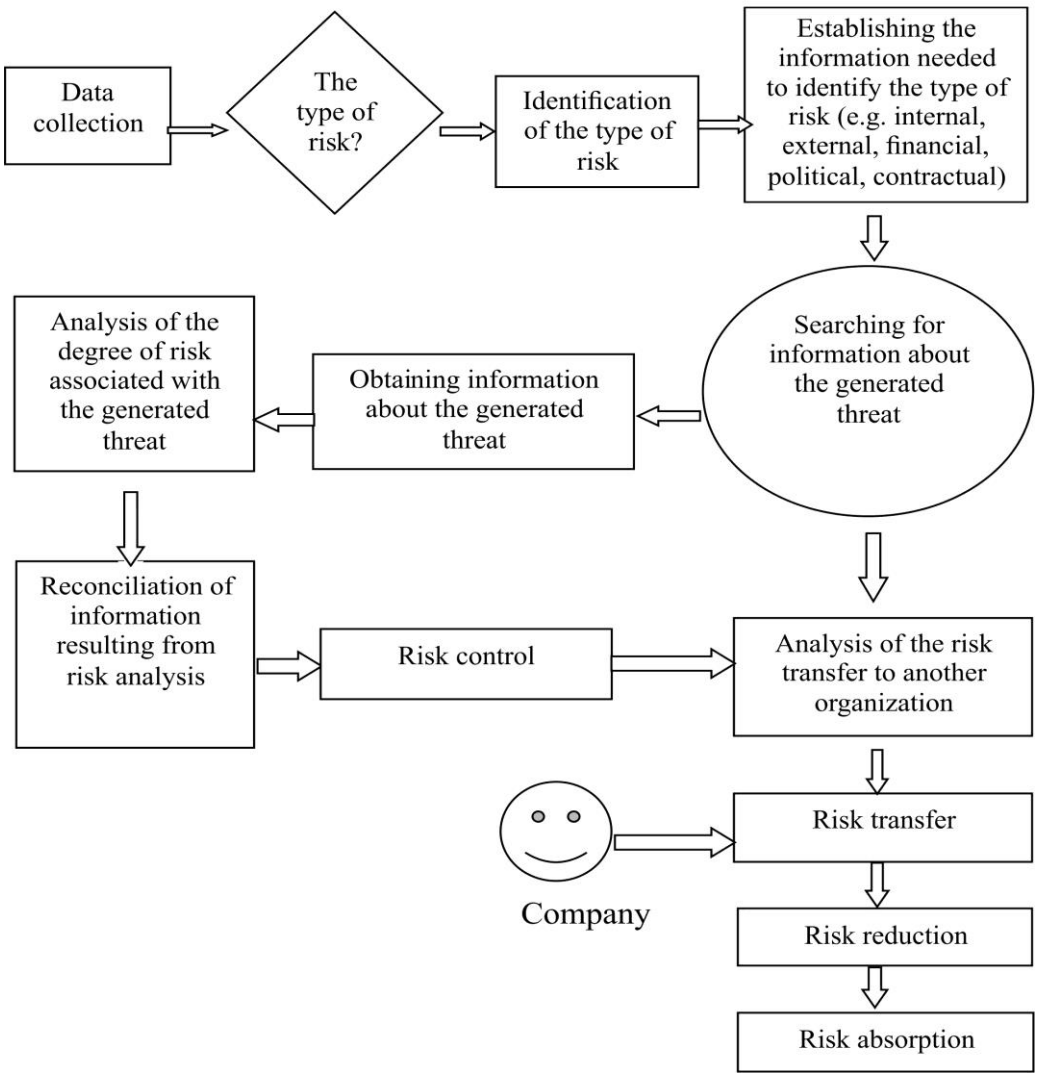
Threats from third parties or partners are not less popular in top 5 security incidents, recorded for 2017-2019 (**Table no. 1**). A constant support of 44% defines each reported year (**Table no. 2**). The target of the attacks might be any type of company, regardless of size or industry in which it performs. Increased attention is recommended to contracts with unknown partners or recently active in the market, as well as with Cloud providers, considered the most important future information security technology (i.e., the Cloud). Companies should test the partners and third parties before signing the contract regarding the competence on promised preservation, given the later major dependence.

The risks associated with information security threats not only derive from the used software, but also depend on how users manage it. Because employees are the ones who use computer systems, the security of the organization risks to be threatened by their actions. A first dangerous action that might expose computer systems to security incidents is to visit websites including malicious content or websites that process credit card information. There are entities that perform financial-accounting activities on the same network, without a segmentation of professional activities. In the event of a cyber attack, all operational activity would be compromised. Therefore, the network should be divided into activity areas and high value assets, "isolated". To the unknown devices should not be allowed Wi-Fi access, by setting up a private or public network (i.e., private, public network). Moreover, Wi-Fi connections are not secure, especially when making online payments. It is recommended to avoid connecting to public Wi-Fi because it has been detected

hackers' techniques to connect to the Wi-Fi server, acquiring the data. Then, when users connect to the hacker's Wi-Fi network, the hacker will have access to the victim's browsing history, implicitly in case of a payment, to user confidential data (i.e., name and surname, bank card number, card expiration date, CVV code).

Risk management, a controversial topic, is based on extensive management experience in identifying the risk generated by disruptive technologies or as a result of the risks associated with the digitization processes. The first step is to collect the data in order to determine the type of risk the company confront. The identification of the risk type facilitates the establishment of the necessary information to establish the type of risk (e.g., internal, external, financial, political, contractual) in order to analyze the degree of risk. Following the reconciliation of information, risk control arises, which aims to transfer the risk or to move it to another organization or person. The transfer is usually made to the insurer (e.g., the bank), against an insurance premium. In this way, the risk is reduced, the company managing the remaining assumed risk (***Figure no. 1***).

Figure no. 1. Risk management analysis model



Source: Author's projection

5. Conclusions

Discussions regarding threats generated by disruptive technologies (i.e. Cloud Computing, Artificial Intelligence, Machine Learning through the Deep Learning subset) that generate frequent security incidents (e.g. APTs, phishing, malware, ransomware, sabotage by external actors, threats by third parties / partners, loss of access to mobile devices by accessing malicious links) were included in this paper, along with the analysis of the impact generated by disruptive technologies based on the security reports issued by Kaspersky Lab over a period of 3 years (2017, 2018, 2019) and based on frequent phishing records, according to Fraud Watch International. The Cloud Computing, Artificial Intelligence and Deep Learning progress is a fact that cannot be challenged. The adoption of Robotic Process Automation would contribute to a Robotic Intelligent Automation, materialized by the emergence of new tasks and the automation of routine activities (which follow the same flow each time), creating an added value to existing investments. Given the result of this investigation, where security incidents are showing successive increases, companies will increasingly invest in intelligent automation of internal processes, will require greater assurance from Cloud providers, will design new methodologies and current practices, which will need protection in order to maintain the company's reputation, maintaining the clients' confidence in the financial reporting and the investors in continuing the capital investment.

Professional bodies, experts in the field and banking experts are facing a cybernetic phenomenon (i.e., cybercrime) that seems to meet no boundaries. The use of a research methods mix has contributed to a further detailed investigation and a broader framework analysis for the current context, marked by risks resulting from non-stop connections to the online environment and threats posed by hackers, given the economic context, currently influenced by the COVID-19 pandemic. Users are overwhelmed by these unprecedented threats for two reasons:

- The subject of the e-mail seems to be very credible (e.g., "Measures against COVID-19", "Donate 2 euros" campaigns);
- The source (i.e., the sender) is well known (i.e., WHO), users considering for the credibility of the recipient.

The increasing level of transmission, in frequency and impact, marks an extremely vulnerable environment for users and companies of disruptive technologies. May be taken into account the human risks factor, subject of Artificial Intelligence, concluding on ethical issues, legal or psychological (e.g., Sophia case) or GPT-2 robot, which might generate paragraphs of coherent text, might translate into various languages and would be able to answer various questions and even conceive online false news, by creating confusion, pretending to be someone else. In fact, connections to a public Wi-fi should be absolutely avoided, especially if online payments are made at that time, there are various ways hackers might steal confidential data.

This article also outlined some unconventional measures that would help the financial sector, professional accountants and auditors to mitigate the risks associated with threats generated by disruptive technologies. Increased attention is recommended to the software working and management process, since computer systems (even the newest ones) are exposed to cyber attacks. Both locally and internationally, numerous information campaigns might be considered aimed at raising awareness of the risks associated with the discussed threats, in order to ensure the quality of the audit, financial reporting system. If are received messages that appear to be suspicious or subject to a popular topic (COVID-19), from unknown recipients and even officials (WHO), a preliminary documentation is recommended before accessing the data. For accountants and auditors, deepening new technologies (Artificial Intelligence, Deep Learning, RPA) is recommended, given that in Romania these technologies are insufficiently assimilated. In the current information systems context, an analysis model has been outlined, that aims risk management by organizations concerned with this issue, detailing the phases of this process, contributing to a better information and awareness, needed in a continuous changing and uncertain world in terms of information security.

As future research directions, the author undertakes to investigate in a future material the extent to which the risks associated with threats from disruptive technologies impact the financial field, in particular accounting and auditing.

REFERENCES

1. 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*, 855, pp. 47-76.
2. Azvine, B. şi Jones, A. 2019. Meeting the Future Challenges in Cyber Security. *Industry 4.0 and Engineering for a Sustainable Future*, pp. 137-152.
3. 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*, 2(4), pp. 35.
4. Faccia, A., Al Naqbi, M. Y. K., & Lootah, S. A. 2019. Integrated Cloud Financial Accounting Cycle: How Artificial Intelligence, Blockchain, and XBRL will Change the Accounting, Fiscal and Auditing Practices. In *Proceedings of the 2019 3rd International Conference on Cloud and Big Data Computing,* pp. 31-37
5. Gadhavi, L. J., & Bhavsar, M. D. 2020. Efficient Resource Provisioning Through Workload Prediction in the Cloud System. *Smart Trends in Computing and Communications*, pp. 317-325.
6. Goodman, M. 2016. X-CYBER: viitorul începe azi. O viziune a expertului în securitate globală asupra infracțiunilor informatice, *Editura RAO*, Bucureşti.
7. Guo, H., Cheng, H. K., & Kelley, K. 2016. Impact of network structure on malware propagation: A growth curve perspective. *Journal of Management Information Systems*, 33(1), pp. 296-325.
8. Hawker, A. 2000. Security and control in information systems: A guide for business and accounting, Vol. 1. *Psychology Press*.
9. Hou, S., Ye, Y., Song, Y., & Abdulhayoglu, M. 2017. Hindroid: An intelligent android malware detection system based on structured heterogeneous information network. În *Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 1507-1515.
10. Mangiuc, D., 2017. Accountants and the cloud – Involving the professionals. *Accounting and Management Information Systems*, 16(1), pp. 179-198.
11. Mohammed, A. L., Al-Hosban, A., & Thnaibat, H. 2018. The impact of the risks of the input of accounting information systems on managerial control, accounting control and internal control in commercial banks in Jordan. *International Journal of Business and Management*, *13*(2), 96-107.
12. Prangate, B. 2019. Algoritmul care îşi dă seama când un text a fost scris de un robot. [online] disponibil la https://playtech.ro/2019/algoritm-text-robot/, accesat la data de 8 martie 2020.
13. Rainer, R. K., Prince, B., Splettstoesser-Hogeterp, I., Sanchez-Rodriguez, C., & Ebrahimi, S. 2020. Introduction to information systems. *John Wiley & Sons*.
14. 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*, 31(3), pp. 63-79.
15. Rîndaşu, 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*, 16(4), 581-609.
16. Shkarlet, S., Dubyna, M., Shtyrkhun, K., & Verbivska, L., 2020. Transformation of the Paradigm of the Economic Entities Development in Digital Economy. *WSEAS Transactions on Environment and Development*, *16*, 413-422.
17. Von Solms, B., von Solms, 2018. Cybersecurity and information security – what goes where?. *Information & Computer Security*, 26(1), pp. 2-9.
18. Wang, C., Chow, S. S., Wang, Q., Ren, K., & Lou, W. 2011. Privacy-preserving public auditing for secure cloud storage. *IEEE transactions on computers*, *62*(2), 362-375.
19. Zhang, Y., Xu, C., Lin, X., & Shen, X. S. 2019. Blockchain-based public integrity verification for cloud storage against procrastinating auditors. *IEEE Transactions on Cloud Computing*.

20. CERT.RO, 2018. THREATS EVOLUTION IN THE ROMANIAN CYBERSPACE. [online] available at: https://www.cert.ro/vezi/document/cert-ro-cyberthreats-2018, accesed 15 March 2020.
21. Europol, 2020. How Criminals Profit From The Covid-19 Pandemic. [online], available at: https://www.europol.europa.eu/newsroom/news/how-criminals-profit-covid-19- pandemic, accessed 28 March 2020.
22. FanCourier, 2019. Alertă de atac tip phishing. [online] available at: https://www.fancourier.ro/alerta-de-atac-tip-phishing/, accessed 28 March 2020.
23. E&Y, 2017. Cybersecurity regained: preparing to face cyber-attacks-20th Global Information Security Survey 2017 18. [online] available at: https://www.ey.com/Publication/vwLUAssets/GISS_report_2017/$FILE/REPORT%20-%20EY%20GISS%20Survey%202017-18.pdf, accessed 18 March 2020.
24. E&Y, 2018. Is cybersecurity about more than protection? - EY Global Information Security Survey 2018–19. [online] available at: https://www.ey.com/Publication/vwLUAssets/ey-global- information-security-survey- 2018-19/$FILE/ey-global-information-security-survey-2018-19.pdf, accessed 18 March 2020.
25. ISACA, 2015. State of cybersecurity: Implications for 2015. An ISACA and RSA Conference Survey. [online] available at: https://www.isaca.org/cyber/Documents/State-of-Cybersecurity_Res_Eng_0415.pdf, accessed 12 March 2020.
26. ITU, 2017. Global Cybersecurity Index 2017. [online] available at: https://www.itu.int/dms_pub/itu-d/opb/str/d-str-gci.01-2017-pdf-e.pdf , accessed 12 March 2020.
27. Kaspersky, 2017. Kaspersky Security Bulletin. Overall statistics for 2017. [online] available at: http://www.dataproof.co.za/index.php/2017/12/14/kaspersky-security-bulletin-overall-statistics-for-2017/, accessed 12 March 2020.
28. Kaspersky, 2018. The State of Industrial Cybersecurity 2018 - Kaspersky-ICS-Whitepaper. [online] available at: https://ics.kaspersky.com/media/2018-Kaspersky-ICS- Whitepaper.pdf, accessed 12 March 2020.
29. Kaspersky Security Bulletin, 2019. Advanced threat predictions for 2020. [online] available at: https://securelist.com/advanced-threat-predictions-for- 2020/95055/, accessed 12 March 2020.
30. Kaspersky, 2019 a). APT trends report Q3 2019. [online] available at: https://securelist.com/apt-trends-report-q3- 2019/94530/, accessed 12 March 2020.
31. Kaspersky, 2019. The State Of Industrial Cybersecurity. [online] available at: https://ics.kaspersky.com/media/2019_Kaspersky_ARC_ICS_report.pdf, accessed 12 March 2020.
32. Kaspersky, 2019. Kaspersky Security Bulletin Statistics. [online] available at: https://securelist.com/kaspersky- security-bulletin-2019-statistics/95475/, accessed 10 March 2020.
33. Kaspersky, 2019. Cyberthreats to financial institutions 2020: Overview and predictions. [online] available at: https://securelist.com/financial-predictions-2020/95388/, accessed 10 March 2020.
34. PWC, 2016. Toward new possibilities in threat management. [online] available at: http://www.pwc.com/ee/et/publications/pub/gsiss-report-cybersecurity-privacy- possibilities.pdf, accessed 8 March 2020.