Audit financiar, XIX, Nr. 1(161)/**2021**, *17-28*
ISSN: 1583-5812; ISSN on-line: 1844-8801

Riscurile asociate cu amenințările generate de tehnologiile disruptive

în contextul sistemelor informatice financiare actuale

Drd. Lavinia Mihaela CRISTEA,
Academia de Studii Economice din Bucureşti, România,
e-mail: cristealaviniamihaela@yahoo.com

Rezumat

Subiectul studiului îl constituie analiza riscurilor asociate cu amenințările generate de tehnologiile disruptive în contextul sistemelor informatice financiare actuale ale entităților. Fenomenul de criminalitate cibernetică, facilitat de dezvoltarea Inteligenței Artificiale, de Deep Learning şi de frecvența disruptivă a incidentelor de securitate reprezintă fundamentul acestei lucrări. Obiectivul articolului este de a integra, compara şi investiga impactul tehnologiilor disruptive, al riscurilor şi incidentelor de securitate actuale şi de a proiecta măsuri în vederea gestionării riscului. Rezultatele acestei lucrări subliniază Advanced Persistent Threats (APTs), malware-ul, ransomware-ul, sabotajul actorilor externi, amenințările terților în top 5 cele mai frecvente incidente de securitate. Lucrarea admite complexitatea digitalizării şi transpune un model practic de gestionare a riscului. Lucrarea contribuie la informarea părților interesate despre pătrunderea forțată a hackerilor în dispozitivele victimelor, sub pretextul COVID-19.

Cuvinte cheie: *riscuri asociate sistemului financiar; amenințări cibernetice; tehnologii disruptive; sisteme informatice actuale; impactul Inteligenței Artificiale; impactul Deep Learning; COVID-19*

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

Vă rugăm să citați acest articol astfel:
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

Link permanent pentru acest document:
http://dx.doi.org/10.20869/AUDITF/2021/161/002
Data primirii articolului: 24.09.2020
Data revizuirii: 14.10.2020
Data acceptării: 23.01.2021

1. Introducere

Adoptarea unor procese de digitalizare complexe a crescut rapid în ultima perioadă de timp (Forbes, 2020), fiind determinată de cerințe ridicate privind modul de raportare şi prezentare a situațiilor financiare pentru utilizatori şi părți interesate, dar şi din aspirația companiilor de a se menține în trend şi în competiția pe piață, devenind dependente de IT. Procesele de digitalizare, ce stau la baza sistemelor informatice financiar-contabile actuale ale entităților, constau în digitizarea datelor sau în tranziția de la date analogice la date în format digital, reprezentând un proces de colectare a informațiilor disponibile în accesarea digitală. Ca urmare a digitizării datelor analogice, datele rezultate au fost integrate în aplicații software, menite să folosească unor procese de lucru automate sau automatizări pe scară largă în majoritatea industriilor, spre optimizarea productivității şi flexibilității organizaționale.

Entitățile ce prestează servicii de contabilitate şi audit (şi nu numai) se află într-o căutare continuă de automatizări la nivelul proceselor de lucru, deoarece obțin mai uşor o valoare comercială adăugată investițiilor existente prin Automatizarea Robotică a Proceselor (RPA). În acelaşi timp, industria automatizării se orientează către îmbinarea RPA cu tehnologiile de Inteligență Artificială (eng. Artificial Intelligence, AI) şi de învățare automată (eng. Machine Learning), urmărind aceste două frontiere, spre o Automatizare Inteligentă Robotizată. Aplicabilitatea acestor tehnologii emergente contribuie la o reimaginare (completă) a fluxului operațional şi la adăugarea unui plus (de) valoare afacerii.

AI desemnează un termen generic pentru sisteme sau maşini ce imită inteligența umană, în vederea efectuării unor activități care, pe baza informațiilor colectate, pot îmbunătăți considerabil procese de lucru. Principiul AI este de a reproduce modul în care oamenii acționează şi chiar perfecționează sarcini de lucru, acordând o semnificație datelor într-un mod în care nu ar fi fost conceput până în prezent. Machine Learning recunoaşte modele rezultate din datele prelucrate anterior de auditori, astfel încât să poată formula predicții, în vederea automatizării unor procese de afaceri extrem de complexe, ce urmează o anumită rutină. Prin Automatizare Inteligentă Robotizată înțelegem îmbinarea noțiunilor de robotică, automatizare şi AI. În sectorul financiar, prin adoptarea acestor tehnologii disruptive, profesioniştii contabili şi auditori ar avea o libertate de gândire şi de inovare mai complexă.

Companiile vor investi din ce în ce mai mult în automatizări inteligente ale proceselor interne, metodologii şi practici curente, spre a creşte reputația companiei, păstrarea încrederii clienților în raportarea financiară şi a investitorilor în plasarea capitalurilor. În acest sens, este imperativ necesar un plan de prevenție în vederea combaterii amenințărilor cibernetice atât la nivel de individ, cât şi la nivel organizațional (Goodman, 2016), luând în considerare că pentru anul 2020 incidentele cibernetice se situează pe primul loc, în comparație cu 2013, când se poziționau pe locul 15. Având în vedere că pe plan local (respectiv, România) nu este însuşită o puternică informare pe acest subiect „Riscurile asociate cu amenințările generate de tehnologiile disruptive în contextul sistemelor informatice financiare actuale", transparența fiind limitată în această privință, am dezbătut cadrul cibernetic financiar prezent, printr-o documentare şi analiză critică a celor mai noi publicații digitale, ce poate fi transpus profesiei de contabil, respectiv de auditor.

Obiectivul acestei lucrări este (1) de a identifica spațiul cibernetic actual ce pare nesigur din punct de vedere al pregătirii profesioniştilor contabili şi auditori, în vederea prevenirii amenințărilor generate de tehnologiile emergente, (2) de a analiza riscurile survenite în urma incidentelor de securitate cauzate de evoluția tehnologiilor disruptive şi (3) de a proiecta un model de analiză privind gestionarea riscului în vederea asumării de către entități a unui nivel acceptabil de risc. Prin acest articol, autorul contribuie la literatura de specialitate printr-o mai bună informare cu privire la sistemul informatic actual al entităților şi proiectarea unui model de analiză privind gestionarea riscului, scopul fiind de a dezvolta o conştientizare la nivel de individ, cât şi la nivel de companie, în vederea atenuării şi, de ce nu, a respingerii amenințărilor generate de tehnologiile disruptive.

Lucrarea poziționează incidentele de securitate actuale într-un context de interes pentru utilizatorii de tehnologie şi companii ce persevereză în lupta continuă împotriva riscurilor cibernetice asociate cu amenințările generate de tehnologiile disruptive, survenite în urma dezvoltării acerbe a mediului online, a proceselor de digitalizare şi a sistemelor informatice financiare actuale. Prima secțiune pune accent pe analiza literaturii de specialitate, ce are în vedere analiza cadrului constituit de „Riscurile asociate cu amenințările generate de tehnologiile disruptive în contextul sistemelor informatice financiare actuale", la nivel global. Cea de-a doua secțiune discută metodologia de cercetare proprie a

acestei lucrări. Secțiunea trei prezintă rezultatele obținute, conturează evoluții şi comparații ale celor mai frecvente incidente de securitate raportate de Kaspersky şi Fraud Watch International, alături de o strategie de gestionare a riscului (eng. Risk Management), concepută într-un model de analiză ce ar putea fi luat în considerare de companii în vederea evaluării, prevenirii, transferului şi asumării riscului generat de tehnologiile disruptive. Articolul încheie prin enunțarea concluziilor şi a direcțiilor viitoare de cercetare.

2. Recenzia literaturii de specialitate

Riscurile asociate cu amenințările generate de tehnologiile disruptive în contextul sistemelor informatice financiare actuale continuă să afecteze companii şi utilizatori de tehnologie din întreaga lume (Hawker, 2000; Goodman, 2016; Mohammed, 2018; Rainer, 2020). În acest sens, riscurile asociate cu amenințările generate de tehnologiile disruptive se află în strânsă legătură cu fenomenul de criminalitate informatică (eng. cybercrime) şi securitate cibernetică (eng. cybersecurity) (ISACA, 2015; PwC, 2016; Goodman, 2016; ITU, 2017; E&Y, 2017; von Solms şi von Solms, 2017; Demertzis, 2018; E&Y, 2018; Kaspersky, 2018; Kaspersky, 2019; Alloghani, 2020), fenomen ce pare să devină din ce mai frecvent întâlnit, tot mai sofisticat în privința modalităților de atac şi în privința impactului generat de hackeri. Pentru evitarea pe cât posibil a acestor riscuri, se recomandă proiectarea şi integrarea unor sisteme informatice bine puse la punct, alături de stabilirea din timp a unor măsuri privind respectarea confidențialității, integrității, disponibilității, procesării şi stocării datelor rezultate din procesele operaționale. Aderarea la platformele Cloud poate asigura siguranța datelor (Wang et al., 2011; Faccia et al., 2019; Zhang et al., 2019; Shkarlet et al., 2020) şi poate reprezenta o soluție de business eficientă prin estimări ale cererilor de resurse viitoare necesare bunei funcționări a întreprinderii, folosind o abordare predictivă (Gadhavi, 2020). Înainte de încheierea unor contracte cu terții sau cu furnizorii de Cloud este recomandată o pre-verificare a riscurilor asociate cu respectivele contracte sau cu platformele Cloud ce vizează simplificarea proceselor de afaceri.

În ciuda avantajelor oferite (e.g. alocarea unui timp de lucru mai scurt pregătirii şi prezentării situațiilor financiare, automatizări la nivelul proceselor operaționale, utilizarea unor sisteme computerizate, eficientizarea la nivel de înregistrare a operațiunilor financiare) de tehnologiile disruptive (cum ar fi Cloud Computing, Big Data, IoT, Inteligența Artificială, Machine Learning, Automatizarea Robotică a Proceselor sau Robotic Process Automation) (PwC, 2016; Richins et al., 2016; Mangiuc, 2017; Azvine şi Jones, 2019), riscurile generate îşi regăsesc fundament în amenințări informatice variate (de ex. Advanced Persistance Threats, phishing, malware, ransomware, DDoS, Man-In-The-Middle, injectarea SQL, atacuri cibernetice pe dispozitivele mobile, frauda electronică) (Rîndaşu, 2016; Guo et al., 2016; Hou et al., 2017; Stanciu şi Tinca, 2017; Azvine şi Jones, 2019), generate de tehnologiile disruptive şi concretizate în atacuri cibernetice, ce compromit sistemele informatice organizaționale, ca urmare a apariției unor procese de digitalizare din ce în ce mai complexe (Goodman, 2016).

Pentru anul 2020, investitorii Kaspersky Lab (2019) relatează că riscurile cu care companiile şi utilizatorii se confruntă sunt de ordin major, fiind reprezentate de amenințări avansate şi persistente (APT-urile) de tip WildPressure, malware de tip Backdoor.Win32.Agent, spam, phishing, incidente informatice, atacatorii cibernetici căutând accesul la date biometrice. În ultima perioadă, hackerii au investit substanțial în metode ce „păcălesc" sistemele anti-fraudă. Nefiind suficient furtul autentificării, prin acces la PII (eng. Personally Identifiable Information), atacatorii necesită amprenta digitală pentru extragerea banilor din bancă. Astfel, pe parcursul anului 2019 a fost identificat Genesis, un e-magazin sub acoperire ce comercializează amprente digitale ale utilizatorilor din întreaga lume, reprezentând unul dintre riscurile asociate (i.e. furtul amprentei digitale) cu amenințările generate (i.e. furtul autentificării) de tehnologiile disruptive (i.e. browserul Tenebris Linken Sphere) cu care se confruntă utilizatorii de servicii bancare online. Au fost identificate deja peste 60 de mii de profiluri furate; pofilele includ amprente digitale ale browser-ului, autentificări pe diverse site-uri prin user şi parolă, cookie-uri, informații despre cardul de credit etc. Prin încărcarea amprentei în browserul Tenebris Linken Sphere, infractorii sunt capabili să se dea drept utilizatori legitimi ai serviciilor bancare. Acest tip de atac arată că infractorii dețin cunoştințe aprofundate despre funcționalitatea internă a sistemelor bancare, ceea ce reprezintă o adevărată provocare în a fi protejat împotriva unor asemenea atacuri. Cea mai bună metodă de prevenție ar fi autentificarea cu mai mulți factori (Multi-factor authentication, MFA).

De altfel, multe din amenințările generate de tehnologiile disruptive sunt la adresa Android. Spre exemplu, pentru trimestrul 3 (septembrie, 2019), Zerodium, o firmă de brokeraj, a indicat faptul că o zi fără acces la Android ar costa mai mult decât o zi fără acces la iOS (sistemul de operare Apple Inc.), valorând 2,5 milioane de dolari. Această sumă reprezintă o creştere semnificativă, ce anterior ar fi fost plătită contra unui atac la adresa iOS, de 2 milioane de dolari. În aceeaşi zi, a fost identificată o amenințare în driverul v412 (Video4Linux), un driver Android de tip media. În cazul în care această vulnerabilitate nu ar fi fost identificată la timp, ar fi existat riscul escaladării privilegiilor utilizatorilor. Amenințarea generată de Android se datorează lipsei actualizării de soft (eng. update) din luna septembrie ce ar fi trebuit să includă acest tip de vulnerabilitate în actualizarea de securitate efectuată de Google. Câteva zile mai târziu a fost identificată o altă vulnerabilitate Android, care ar fi permis atacatorilor accesul complet la e-mailurile utilizatorilor de telefoane inteligente Samsung, Huawei, LG şi Sony, prin transmiterea unui mesaj de tip text (Kaspersky 2019 a).

Hackerii sunt actorii ce caută să amenințe, să creeze daune costisitoare la nivel global şi să găsească puncte slabe din punct de vedere al securității informației, în special în companii unde vulnerabilitatea datelor poate fi uşor periclitată. Atacatorii cibernetici sunt preocupați în mod continuu de inițierea unor atacuri împotriva Android sau iOS, sau către zona politicii, militare, spitalelor din întreaga lume, unde WannaCry constituie deja istorie în acest sens (CERT.RO, 2018; Azvine şi Jones, 2019; Kaspersky, 2019). De cele mai multe ori, riscul de a fi atacat este concretizat în fapte reale, ce conduce la apariția litigiilor sau a proceselor în instanță (Forbes, 2020). Incidentele cibernetice figurează pe locul 1 în clasamentul riscurilor cu care se confruntă companii din întreaga lume, apariția unui atac cibernetic asupra business-ului reprezentând un adevărat pericol ce amenință activitatea economică (Allianz Risk Barometer, 2020).

3. Metodologia cercetării

Acest articol îşi propune să trateze cel mai nou episod cu privire la „Riscurile asociate cu amenințările generate de tehnologiile disruptive în contextul sistemelor informatice financiare actuale". Sunt dezbătute curente digitale emise de compania software Kaspersky Lab, companie ce a dovedit de-a lungul timpului profesionalism în proiecția şi implementarea unor programe de securitate eficiente. Considerăm că pentru înțelegerea fenomenului de securitate cibernetică actual ce stă la baza acestor riscuri este necesară examinarea stării cibernetice curente şi a mişcărilor atacatorilor, ce par a fi din ce în ce mai complexe, sofisticate, rapide şi documentate. Această examinare s-a realizat prin investigarea rapoartelor emise de Kaspersky Lab pentru ultimii trei ani - 2017, 2018, 2019.

Metoda de cercetare a acestei lucrări are la bază cercetarea calitativă fundamentală şi observația critică, aplicată pentru investigarea rapoartelor şi practicilor digitale în trend, ce au ca scop informarea utilizatorilor cu privire la amenințările generate de tehnologiile disruptive, spre o mai bună protecție împotriva vulnerabilităților ce par să acapareze sistemele informatice ale entităților.

Articolul se împarte în (1) analiza şi compararea rapoartelor de securitate Kaspersky Lab pentru perioada 2017-2019, (2) examinarea incidentelor de securitate prezentate de Kaspersky Lab şi de Fraud Watch International şi (3) amenințările generate de impactul Inteligenței Artificiale şi Deep Learning la nivel global. Sursa datelor îşi regăseşte originea în publicații digitale online ale organismelor de specialitate şi în alte publicații curente, preocupate de stoparea acestor atacuri. În anul 2020, din cauza pandemiei COVID-19, amenințările generate de acest virus au generat o teamă profundă în lumea întreagă, hackerii găsind prilejul perfect pentru infiltrări repetate şi atacuri asupra utilizatorilor de tehnologie, deosebit de interesați de acest subiect şi de protecția împotriva virusului. Articolul oferă detalii cu privire la complexitatea riscurilor asociate cu adoptarea tehnologiilor disruptive în contextul sistemelor informatice financiare actuale. Pentru analiza fenomenului actual şi în vederea identificării prezentelor amenințări raportate, au fost luate în considerare rapoarte de securitate emise de compania specializată în securitate Kaspersky Lab, aşa cum am precizat mai sus, dar şi evidențe ale organizației de securitate pe internet Fraud Watch International, specializată în protecția online împotriva fraudei.

Lucrarea prezentă investighează amenințările generate de tehnologiile disruptive, îndeosebi de Inteligența Artificială şi Deep Learning, prin cercetarea documentară a celor mai recente curente tehnologice ce semnalează asupra amenințărilor generate de procesele de digitalizare. Pentru identificarea literaturii de specialitate potrivite acestui studiu au fost consultate

baze de date internaționale precum ProQuest, Springer Link, ResearchGate şi Google Scholar. Sortarea articolelor a fost realizată manual de către autor, fiind alese numai articolele ce dezbat riscurile asociate cu amenințările generate de tehnologiile disruptive în contextul sistemului informatic financiar-contabil actual al entităților, prin verificarea în prealabil a includerii informațiilor cheie.

Lucrarea inițiază discuții şi explorează riscurile asociate cu amenințările generate de tehnologiile disruptive asupra sistemului financiar contabil şi dezvoltării proceselor de digitalizare, accentuând (1) evoluția celor mai frecvente cinci incidente de securitate, (2) recomandări emise de bănci (e.g. ING Bank), companii şi organizații abilitate (de ex. Europol, CERT.RO) în ceea ce priveşte securitatea informației. Termenii „vulnerabilitate", „alerte", „hackeri", „atacatori cibernetici" sunt folosiți alternativ în această lucrare. Luând în considerare faptul că s-a constatat o reticență asupra informării privind starea actuală a atacurilor cibernetice şi raportării numărului mare de incidente de securitate cu care se confruntă companii şi utilizatori din întreaga lume, a fost practic imposibilă cuprinderea tuturor evenimentelor de securitate.

4. Rezultate şi discuții

Punctul de interes al acestei lucrări îl constituie riscurile ce apar odată cu dezvoltarea proceselor de digitalizare, asociate amenințărilor tehnologice disruptive şi raportate de sistemele informatice, atât la nivel organizațional, cât şi la nivel de individ. În contextul noii pandemii, COVID-19, ING Bank a luat atitudine. Mai exact, banca informează despre noile modalități de atac ale hackerilor, care se folosesc de acest pretext epidemiologic pentru a transmite clienților ING e-mailuri de phishing ce au ca subiect protecția împotriva acestui virus (COVID-19). Atacatorii cibernetici se folosesc de curente actuale şi de cele mai în vogă subiecte la care ar exista o acțiune instantanee (printr-un click pe linkul infectat primit). E-mailurile par a fi transmise din surse sigure, însă, printr-o observare mai atentă, se pot depista e-mailuri provenite din surse nelegitime. Prin e-mailuri de phishing le sunt solicitate utilizatorilor diverse acțiuni, precum accesarea unor link-uri, descărcarea de fişiere sau imagini (ce pot fi infectate cu virus), furnizarea de date confidențiale (de ex. coordonate bancare, nume de card sau parole). ING Bank avertizează despre aceste acțiuni suspicioase ce au loc pe scară largă, odată cu apariția acestui virus, COVID-19.

Tot sub pretextul pandemiei COVID-19, atacatorii cibernetici transmit anunțuri false (e.g. „Măsuri împotriva COVID-19", „Donați 2 euro"), sub sigla OMS (Organizația Mondială a Sănătății), notificate de CERT.RO (2018) şi Europol (2020). Aceste anunțuri false bulversează utilizatorii online, hackerii apelând la aşa numitele campanii de strângere de fonduri, promovări de produse de investiție, achiziția unor mănuşi de protecție, tratamente, vaccinuri, măşti de protecție. Sunt transmise e-mailuri cu un conținut de phishing sub numele unor spitale sau clinici medicale, unde utilizatorii de tehnologie sunt informați despre o rudă sau cunoştință care ar fi fost infectată cu acest virus, solicitând destinatarului bani pentru tratament. Sfatul organizațiilor profesionale este de a ignora aceste campanii rău intenționate, de a nu deschide linkurile din e-mailurile necunoscute şi de a verifica sursa expeditoare. Pentru utilizatorii care intenționează să achiziționeze de pe internet sau să doneze în această perioadă şi nu numai, se recomandă o documentare prealabilă înainte de a face tranzacția. Instalarea unui antivirus sau a unei soluții de securitate ar oferi protecție la nivel de anti-phishing, anti-malware şi anti-spam.

În **Tabelul nr. 1** este examinată evoluția alarmantă a unor e-mailuri de tip phishing transmise de atacatori care pretindeau a fi personal abilitat din partea unei bănci (Santander Bank, Wells Fargo Bank), companii de servicii financiare (American Express), de curierat (FedEx) sau streaming video (Netflix), software-ului de transmitere şi primire e-mailuri (Outlook, Global E-mail Server) sau din partea unui operator al unui sistem de plăți online (PayPal). Aceste alerte de phishing sunt doar câteva exemple din milioanele primite şi raportate de victime (i.e. organizații, indivizi) din întreaga lume. Riscurile asociate cu aceste amenințări generate de apariția modalităților de plată online, de servicii de curierat disponibile, de descărcare a informațiilor sau de vizualizare a acestora variază în modalitatea şi diversitatea atacului, scopul final fiind infestarea dispozitivului şi furtul de date personale. Confidențialitatea datelor nu mai este respectată de atacatorii cibernetici, aceştia căutând să pătrundă în toate sectoarele de activitate, prejudiciind drepturile utilizatorilor de tehnologie. Leaderul în protecție anti-phishing, Fraud Watch International, notifică asupra celei mai recente activități de phishing (**Tabelul nr. 1**).

Tabelul nr. 1. Evoluția alertelor phishing pentru luna martie 2020

Incidente Phishing	Subiectul e-mailului	Data
Microsoft - File "Lewis Invoice 076689.pdf" Has Been Shared With You	Instalare Update pentru Microsoft Outlook	26 Martie 2020
Netflix - Please Verify Your Account?	Verificare cont Netflix	24 Martie 2020
Global E-mail Server (Webmail Login) - Urgent Account Verification Needed!!!	Verificare urgentă a contului	20 Martie 2020
PayPal - Your Account cannot be used until you verify it	Verificare urgentă a contului pentru a-l folosi	18 Martie 2020
Outlook - Notification: Release Your 12 held E-mails	Notificare e-maluri	17 Martie 2020
1 New Security Message from Wells Fargo Bank	Mesaj de securitate din partea Wells Fargo Bank	17 Martie 2020
Banco Santander S.A - Aviso Santander Way (41855)	Informare din partea băncii Santander S.A.	03 Martie 2020
American Express - ***Your Account Has Been Flagged***	Contul American Express necesită atenția dumneavoastră	02 Martie 2020
FedEx - FedEx Support on Coronavirus	Suport Coronavirus	02 Martie 2020

Sursa: Proiecția autorului, bazată pe https://fraudwatchinternational.com

Alerta de tip phishing a fost identificată şi de compania de curierat FanCourier, sub numele căreia sunt transmise de către hackeri mesaje de plată sau de deschidere a unor ataşamente, utilizatorilor ce au plasat comenzi sau care au avut cel puțin o comandă operată de această companie (FanCourier, 2019). Pentru evitarea riscului infestării sau prejudicierii datelor personale, este recomandată o atenție sporită acestor e-mailuri, identificării adreselor de e-mail necunoscute ce transmit informații cu privire la aşa-zisele expediții operate de FanCourier. E-mailurile nu provin de la compania FanCourier, ci din partea unor atacatorilor cibernetici specializați în campanii rău intenționate de tip phishing. Hackerii se folosesc de numele FanCourier pentru a distribui fişiere infestate cu Trojan. Riscul de infestare este uriaş, recomandându-se evitarea deschiderii fişierelor primite de la expeditori necunoscuți sau accesării unor oferte online ce par neadevărate, indiferent de forma ce a stat la baza primirii acestora (de ex. mesaj primit pe telefon, link transmis online). În urma atenționării emise de ING Bank, FanCourier, Europol, CERT.RO se recomandă ca device-urile conectate non-stop la Internet şi folosite în scopul navigării să fie updatate şi să dețină soluții de securitate eficiente.

Despre impactul Inteligenței Artificiale în prezent se poate afirma că această tehnologie nu poate înlocui în totalitate sarcinile de lucru umane. Cercetând mai îndeaproape acest fenomen, se cunosc detalii despre crearea unui robot GPT-2, ce poate genera paragrafe de text coerente, poate traduce din diverse limbi şi poate fi capabil să răspundă la diverse întrebări şi chiar să conceapă rezumate (Prangate, 2019). Compania OpenAI, fiind cea care l-a conceput, evidențiază faptul că robotul poate scrie în mediul online ştiri false şi poate crea confuzie, pretinzând că poate fi oricine altcineva. Nu se poate contesta capacitatea acestui robot, arătând cât de avansat este, dar nici faptul că rezultatul obținut este unul perfect. Este adus în discuție un risc asociat tehnologiei disruptive, Inteligența Artificială, un risc cu care omenirea se poate confrunta, prin crearea stării de confuzie. Acesta este un risc ce nu ar trebui subestimat, chiar dacă în primă instanță efectul este neaşteptat de bun.

O altă situație transpusă de Inteligența Artificială o constituie generarea imaginilor prin algoritmul de tip GAN (eng. Generative Adversarial Network) de Deep Learning. Rezultatele acestui algoritm ar putea fi folosite atât în scop pozitiv, cât şi negativ. Pozitiv, prin scutirea unor costuri pentru creatori de modă, agenții de publicitate sau producători de haine, aceştia folosindu-se de GAN pentru crearea de modele necesare şi promovarea articolelor vestimentare. Negativ, actorii rău intenționați ar putea folosi algoritmul pentru o amplă propagandă, imaginile obținute în urma rulării acestui soft subminând încrederea publicului față de aceste instrumente digitale.

Şeful departamentului de cercetare de la Microsoft, Eric Horvitz, este de părere că dezvoltarea Inteligenței Artificiale aduce în discuție anumite riscuri sau probleme

de natură legală, psihologică şi etică (Bellini, 2018). Datele personale de identificare ale unei persoane trebuie să rămână personale. Se poate considera că Inteligența Artificială, printr-o formă sau alta, poate avea acces la date confidențiale despre o persoană (de ex. adresă de domiciliu, cont bancar, traseu zilnic casă - serviciu, boli cu care se confruntă, stare emoțională). Întrebarea va fi în ce măsură Inteligența Artificială va pătrunde în viețile oamenilor, dar şi care vor fi drepturile şi libertățile într-o lume a Inteligenței Artificiale.

Odată cu dezvoltarea acestei tehnologii disruptive, trebuie luate în considerare şi aspecte privind redefinirea locurilor de muncă şi crearea altora noi. Este bine cunoscut faptul că a patra revoluție industrială va conduce la înlocuirea a milioane de locuri de muncă (Kaeser, 2018; Borak, 2018), omenirea necesitând o mai bună pregătire în educație, formare profesională şi academică, inovare şi adaptare la tot ce-i nou. Începând cu anul 2022, Singapore va introduce autobuzele fără şofer (BBC, 2017), pe când în Suedia există încă din 2018, implicând riscul dispariției treptate a locurilor de muncă ce necesită şoferi. O altă întrebare ce derivă din toate aceste invenții şi implicit, riscuri, generate de Inteligența Artificială, este dacă antreprenorii vor prefera roboții sau personalul uman în lucrul de zi cu zi. Se pare că există deja companii ce s-au îndreptat către acest trend (The Guardian, 2017), preferând să lucreze cu Inteligența Artificială, din perspectiva unor costuri mai mici, o eficiență ce creşte considerabil, nefiind necesare pauze, concediu de odihnă sau salariu lunar.

Un robot devine şi o problemă legală, unde pentru prima dată a fost prezentată Sophia, un robot ce a primit cetățenia statului Arabia Saudită (Weisberger, 2017), fiind considerată cetățean cu drepturi depline şi cu personalitate proprie. În România se pare că va exista pentru prima dată ca ambasador o formă de Inteligență Artificială, ce va recomanda locuri de vizitat, va răspunde la diverse întrebări despre România în vederea satisfacerii interesului străinilor, va vorbi despre obiceiuri şi modul de viață al românilor (EMEA, 2017).

Cu referire la dinamica incidentelor de securitate, studiul efectuat de Kaspersky Lab relevă cel mai de temut incident de securitate, Advanced Persistance Threats (APT-urile), ce ocupă primul loc din top 5 pentru anii 2018 şi 2019, pe când în 2017 atacurile de tip malware erau raportate pe primul loc. APT-urile reprezintă o clasă recentă de amenințări, ce pare să fi câştigat un impact mai ridicat, un maxim de 68% pentru anul 2019, față de malware şi ransomware, cu un procent de 66%, respectiv 70%. Acest clasament al APT-urilor s-a menținut pentru ultimii doi ani, 2018 şi 2019, şi se datorează noilor mijloace de atac găsite de hackeri, de complexitatea atacurilor şi de atacul exact la țintă (**Tabelul nr. 2**).

Tabelul nr. 2. Dinamica celor mai frecvente 5 incidente de securitate între anii 2017-2019

Incidente de securitate	2017	2018	2019
APT-uri	32%	66%	68%
Malware	56%	65%	66%
Atacuri Ransomware	33%	64%	70%
Sabotaj din partea actorilor externi	41%	56%	35%
Amenințări din partea terților / partenerilor	44%	44%	44%

Sursa: Proiecția autorului, bazată pe rapoartele de securitate Kaspersky Lab

În cazul malware, evoluția înregistrează valori mai mari în fiecare an. Scopul acestor atacuri de tip malware este furtul de informații, situație cu care se confruntă îndeosebi sectorul financiar-contabil. Hackerul caută slăbiciuni în sistemul informatic al entităților, în vederea punerii în aplicare a unui plan de atac, prin instalarea programului malware şi finalizarea atacului perfect (e.g. furtul de parole, date bancare, informații financiare, date ce vizează programe de investiții, planuri de audit sau alte informații confidențiale). Un exemplu de software rău intenționat îl constituie Calul Troian (de ex. Poweliks, FakeAV), un program malware ce se deghizează într-un soft ce pare legitim. Acest tip de infestare reprezintă o adevărată provocare în depistarea tipului de atac, înşelând utilizatorii cu privire la adevărata intenție. După ce acest soft infecțios pătrunde în sistem, se activează, fapt ce permite hackerului extragerea datelor din dispozitivul victimei. Atacurile Ransomware ocupă

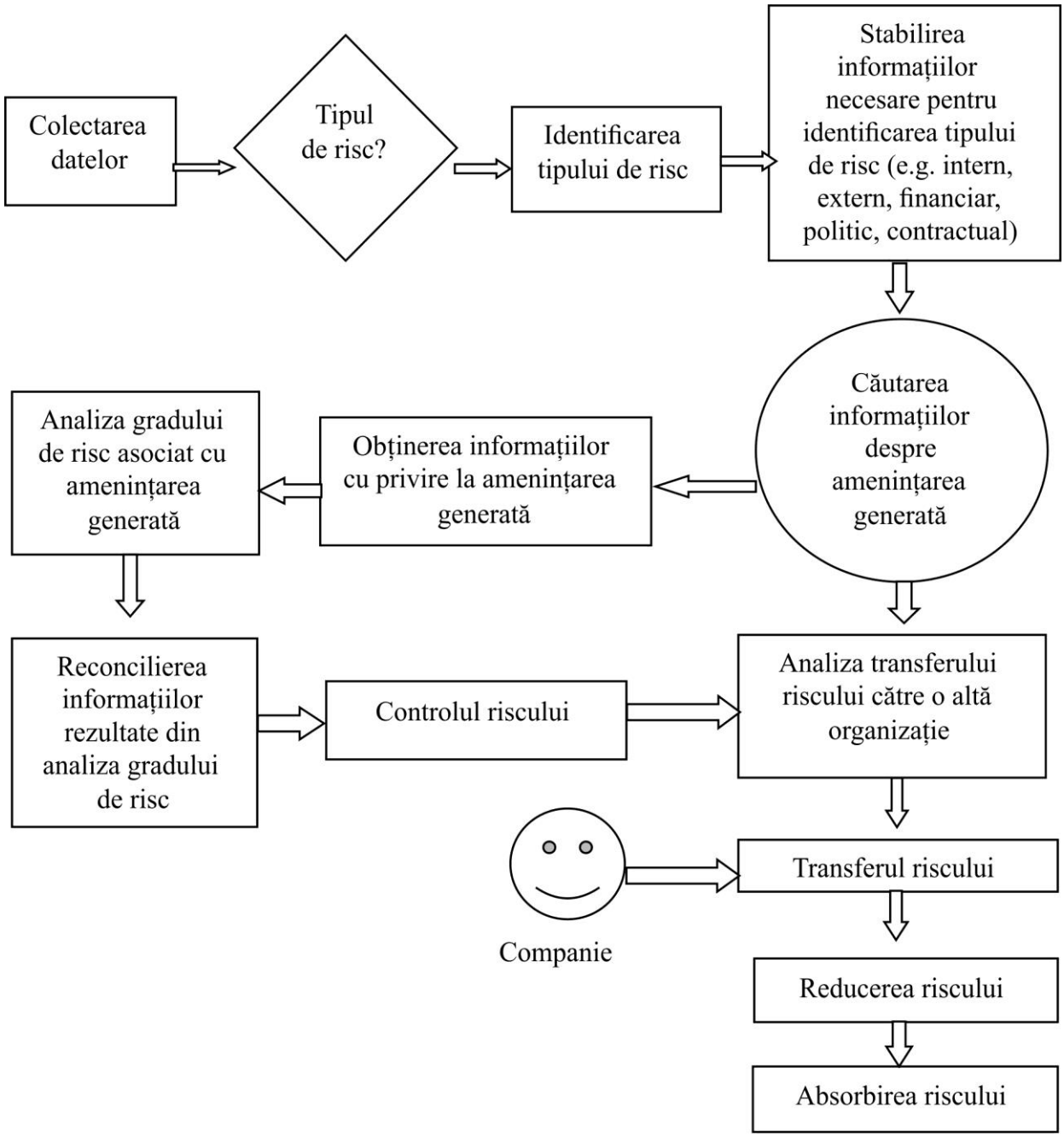
locul 3 în clasamentul Kaspersky Lab şi continuă să înregistreze creşteri. Ransomware reprezintă o nouă formă de malware ce urmăreşte instalarea unui soft rău intenționat pe dispozitivul victimei (de ex. calculator, telefon, tabletă), urmărind criptarea datelor. În schimbul redării accesului, hackerul cere o anumită sumă de bani. În cazul în care victima nu plăteşte la timp sau nu face obiectul plății, există riscul ca datele să nu mai poată fi recuperate, accesul la date realizându-se numai după ce hackerul încasează suma cerută. Din categoria ransomware, CryptoWall 3.0 este un virus ransomware foarte periculos ce a generat încasări de 325 milioane de dolari din schemele de răscumpărare.

Sabotajul din partea actorilor externi se situează pe locul 4 în evoluția incidentelor de securitate. Evoluția acestui tip de atac cunoaşte o evoluție pentru anul 2018, unde pentru 2019 sabotajul din partea actorilor externi înregistrează un declin de 21 de procente. Totuşi, acest incident, întâlnit destul de frecvent în companii din întreaga lume, continuă să înregistreze riscuri cauzate de o insuficientă protecție informatică. Companiile ar trebui să analizeze riscurile cu care se confruntă şi să adopte strategii de implementare pentru o protecție mai sigură a sistemelor informatice. Nici amenințările din partea terților sau partenerilor nu prezintă o popularitate mai scăzută în top 5 incidente de securitate, înregistrate pentru 2017-2019 (**Tabelul nr. 1**). O menținere constantă de 44% defineşte fiecare an raportat (**Tabelul nr. 2**). Ținta atacurilor poate fi reprezentată de orice tip de companie, indiferent de mărime sau de industria în care aceasta operează. Se recomandă o atenție sporită contractelor încheiate cu parteneri necunoscuți sau activi recent pe piață, precum şi cu furnizorii de Cloud, considerată cea mai importantă tehnologie în viitorul securității informațiilor (Cloud-ul). Companiile ar trebui să testeze, înainte de semnarea contractului, capacitatea partenerilor şi terților cu privire la securitatea promisă, având în vedere dependența majoră ulterioară.

Riscurile asociate cu amenințările la adresa securității informației nu derivă doar din software-ul folosit, ci depind şi de modul în care utilizatorii îl gestionează. Deoarece angajații sunt cei care folosesc sistemele informatice, securitatea organizației riscă să fie amenințată de acțiunile acestora. O primă acțiune periculoasă ce poate expune sistemele informatice la incidente de securitate este vizitarea unor site-uri web ce includ un conținut rău intenționat sau site-uri web ce procesează informații privind cardurile de credit. Sunt entități ce desfăşoară activități financiar-contabile pe aceeaşi rețea, fără o segmentare a activităților profesionale. În cazul unui atac cibernetic, întreaga activitate operațională ar fi compromisă. De aceea, rețeaua ar trebui segmentată în domenii de activitate şi activele de mare valoare - izolate. Dispozitivelor necunoscute nu ar trebui să li se permită accesul la Wi-fi, prin setarea rețelei private sau publice (respectiv - private, public network). De altfel, conectările la Wi-fi nu sunt deloc sigure, mai ales atunci când se efectuează plăți online. Este recomandat să se evite conectarea la Wi-fi-ul public, deoarece s-au depistat modalități prin care hackerii se conectează la serverul Wi-fi-ului, însuşindu-şi datele. Mai apoi, utilizatorii conectându-se la rețeaua Wi-fi a hackerului, hackerul va avea acces la istoricul de navigare al victimei, implicit în cazul unei plăți - la date confidențiale ale acesteia (respectiv - nume şi prenume, număr card bancar, data expirării cardului, cod CVV) .

Gestionarea riscului (eng. Risk Management), un subiect controversat, are la bază o experiență vastă din partea managementului în identificarea riscului generat de tehnologiile disruptive sau ca urmare a riscurilor asociate proceselor de digitalizare. Primul pas este reprezentat de colectarea datelor în vederea stabilirii tipului de risc cu care se confruntă compania. Identificarea tipului de risc facilitează stabilirea informațiilor necesare în stabilirea tipului de risc (e.g. intern, extern, financiar, politic, contractual) în vederea analizei gradului de risc. În urma reconcilierii informațiilor survine controlul riscului, ce vizează transferul riscului sau mutarea acestuia către o altă organizație sau persoană. Transferul se realizează de obicei către asigurator (e.g. banca), contra unei prime de asigurare. În acest fel, riscul se reduce, compania urmând a gestiona riscul asumat rămas (***Figura nr. 1***).

Figura nr. 1. Model de analiză privind gestionarea riscului



Sursa: Proiecția autorului

5. Concluzii

Discuții privind amenințările generate de tehnologiile disruptive (cum ar fi Cloud Computing, Inteligența Artificială, Machine Learning prin subsetul Deep Learning) ce generează incidente de securitate frecvente (de ex. APT-uri, phishing, malware, ransomware, sabotaj din partea actorilor externi,

ameninţări din partea terţilor / partenerilor, pierderea accesului la dispozitivele mobile prin accesarea unor link-uri cu conţinut rău intenţionat) au fost incluse în această lucrare, alături de analiza impactului generat de tehnologiile disruptive pe baza rapoartelor de securitate emise de Kaspersky Lab pe o perioadă de 3 ani (2017, 2018, 2019) şi pe baza evidenţei frecvente de phishing, conform Fraud Watch International.

Progresul Cloud Computing, al Inteligenţei Artificiale şi al Deep Learning este un fapt real, ce nu poate fi contestat. Adoptarea Automatizării Robotice a Proceselor ar contribui la o Automatizare Inteligentă Robotizată, concretizată prin apariţia unor noi sarcini de lucru şi automatizarea unor activităţi de rutină (ce urmează de fiecare dată acelaşi flux), în procesele financiar-contabile şi de audit, având în vedere legătura dintre aceste profesii, creând o valoare adăugată sistemelor informatice folosite. Dat fiind rezultatul acestei investigaţii, unde incidentele de securitate figurează creşteri succesive, companiile vor investi din ce în ce mai mult în automatizări inteligente ale proceselor interne, vor cere o asigurare mai mare furnizorilor de Cloud, vor proiecta metodologii şi practici curente, ce la rândul lor vor necesita protecţie. Toţi aceşti paşi sunt necesari şi indivizibili în vederea păstrării reputaţiei companiei, menţinerii încrederii clienţilor în raportarea financiară şi investitorilor în continuarea plasării capitalurilor.

Organisme profesionale, experţi în domeniu şi bănci se confruntă cu un fenomen cibernetic (i.e. criminalitatea informatică) ce pare a nu cunoaşte limite. Folosirea unui mix de metode de cercetare au contribuit la o investigare mai detaliată şi la un cadru mai amplu de analiză pentru contextul actual, marcat de riscuri ce rezultă din conectări non-stop la mediul online şi de ameninţări provocate de hackeri, dat fiind contextul economic actual, influenţat de pandemia COVID-19. Utilizatorii sunt bulversaţi de aceste ameninţări fără precedent, din două motive:

- Subiectul e-mailurilor pare a fi foarte credibil (de ex. „Măsuri împotriva COVID-19”, campaniile „Donaţi 2 euro pentru spitale”);
- Sursa (expeditorul) este bine cunoscută (OMS), utilizatorii pledând tot spre credibilitatea destinatarului.

Nivelul tot mai accentuat de transmitere, în frecvenţă şi impact, marchează un mediu extrem de vulnerabil pentru utilizatori şi companii de tehnologii disruptive. Pot fi luate în considerare şi riscurile la care factorul uman ar fi supus într-o eră a Inteligenţei Artificiale, concluzionând şi asupra unor aspecte etice, legale sau psihologice (de ex. cazul Sophia) sau robotul GPT-2, ce poate genera paragrafe de text coerente, poate traduce în diverse limbi şi poate fi capabil să răspundă la diverse întrebări şi chiar să conceapă ştiri false în mediul online, creând confuzie, dându-se drept altcineva. De altfel, conectările la un Wi-fi public ar trebui absolut evitate, mai ales dacă se efectuează plăţi online în acel moment, existând diverse modalităţi prin care hackerii pot fura datele confidenţiale.

Articolul prezent a enunţat şi unele măsuri neconvenţionale ce ar ajuta sectorul financiar, profesionişti contabili şi auditori în vederea atenuării riscurilor asociate cu ameninţările generate de tehnologiile disruptive. Este recomandată atenţia sporită asupra modului de lucru şi de gestionare software, sistemele informatice (chiar şi cele mai noi) fiind predispuse la atacuri cibernetice. Atât pe plan local, cât şi internaţional se pot lua în considerare numeroase campanii de informare ce vizează creşterea gradului de conştientizare asupra riscurilor asociate cu ameninţările discutate, în vederea asigurării calităţii auditului, sistemului de raportare financiar. În cazul primirii unor mesaje ce par a avea conţinut suspect sau cu un subiect prea popular (COVID-19) de la destinatari necunoscuţi şi chiar oficiali (OMS) este recomandată o documentare prealabilă înainte de a accesa sursa datelor. Pentru contabili şi auditori, aprofundarea noilor tehnologii (Inteligenţa Artificială, Deep Learning, RPA) este recomandată, având în vedere că în România aceste tehnologii sunt slab însuşite. În contextul sistemelor informatice actuale, a fost conturat şi un model de analiză ce are ca obiectiv gestionarea riscului de către organizaţiile preocupate de acest aspect, fiind detaliate fazele acestui proces, contribuind la o mai bună informare şi conştientizare, necesară într-o lume în continuă schimbare şi nesigură, din punct de vedere al securităţii informaţiei.

Ca direcţii pentru cercetările viitoare, autorul se angajează ca, într-un viitor material, să investigheze în ce măsură riscurile asociate cu ameninţările generate de tehnologiile disruptive impactează domeniul financiar, îndeosebi contabilitatea şi auditul.

BIBLIOGRAFIE

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