Audit financiar, XVII, Nr. 2(154)/**2019**, *204-211*
ISSN: 1583-5812; ISSN on-line: 1844-8801

Securitatea informațiilor contabile – o analiză a percepției practicienilor din România

Drd. Sînziana-Maria RÎNDAŞU,
Academia de Studii Economice din Bucureşti,
e-mail: sinziana_rindasu@yahoo.com

Rezumat

Riscurile asociate tehnologiilor informatice utilizate în prezent în domeniul contabil, referitoare la dificultatea securizării datelor, continuă să fie tot mai semnificative din cauza complexității sistemelor folosite care, pe lângă beneficiile pe care le aduc în cadrul proceselor contabile, generează şi o serie de provocări în menținerea caracteristicilor fundamentale ale datelor. Pentru a adresa problema lipsei practicienilor suficient de bine pregătiți astfel încât să poată reduce aceste riscuri, organismele profesionale internaționale susțin necesitatea dezvoltării unui set suficient de abilități profesioniştilor contabili prin creşterea gradului de conştientizare asupra impactului pe care incidentele de securitate le pot avea. Totodată, se evidențiază existența unui decalaj între abilitățile pe care studenții le dobândesc şi cerințele din partea mediului de afaceri, aspect ce favorizează creşterea numărului şi impactului atacurilor cibernetice. Scopul acestei lucrări este de a cerceta care este percepția practicienilor din domeniul contabilității şi auditului cu privire la securitatea datelor şi măsura în care aceştia consideră că informațiile pe care le primesc sunt suficiente, analizând în acelaşi timp şi diferite tipuri de acțiuni ale profesioniştilor care pot afecta securitatea informațiilor contabile. Rezultatele cercetării efectuate demonstrează că profesioniştii cunosc bunele practici de menținere a caracteristicilor fundamentale ale datelor şi înțeleg impactul generat de gestionarea incorectă a informațiilor, dar o parte semnificativă a participanților studiului consideră că nu primesc suficiente informații despre securitatea datelor din partea companiilor şi organizațiilor profesionale din care fac parte.

Cuvinte-cheie: *securitatea informațiilor, percepția practicienilor, phishing, riscuri, responsabilitate*

Clasificare JEL: *M14, M15, M41, M42*

Vă rugăm să citați acest articol astfel:
Rîndaşu, S-M. (2019), The Security of Accounting Information – A Perception-Based Analysis of the Practitioners from Romania, *Audit Financiar*, vol. XVII, no. 2(154)/2019, pp. 298-305, DOI: 10.20869/AUDITF/2019/154/012

Link permanent pentru acest document:
http://dx.doi.org/10.20869/AUDITF/2019/154/012
Data primirii articolului: 22.02.2019
Data revizuirii: 24.02.2019
Data acceptării: 11.03.2019

1. Introducere

Securitatea informațiilor a devenit una dintre principalele provocări ale organizațiilor, odată cu creşterea gradului de digitalizare a activităților şi automatizarea proceselor. Accesul continuu la informații şi raportarea în timp real a datelor contabile au devenit de-a lungul anilor principalele obiective ale companiilor, pentru a dovedi transparență şi a creşte nivelul de încredere al investitorilor.

Pentru a rămâne competitivi şi a putea menține desfăşurarea normală a activităților în condiții optime, în contextul actual în care fluxul de informații este continuu şi volumul acestora creşte exponențial, majoritatea companiilor mari aleg să utilizeze o serie de soluții tehnologice pentru automatizarea proceselor şi reducerea timpului necesar practicienilor pentru a gestiona informațiile, aspect ce a condus la o creştere a riscului de expunere a datelor confidențiale şi sensibile, ce poate avea ca efect pierderi financiare.

La nivel internațional organismele profesionale au urmărit în ultimii ani să sporească gradul de conştientizare asupra riscurilor generate de expunerea datelor prin introducerea conceptelor şi metodelor de reducere ale riscurilor referitoare la securitatea datelor în planurile de studii ale viitorilor practicieni certificați (ACCA, 2018).

În literatura de specialitate există studii care tratează problematica securității informațiilor contabile prin prisma aplicațiilor şi soluțiilor IT utilizate, dar mai puțină atenție a fost acordată nivelului de înțelegere despre necesitatea de securizare a informațiilor şi despre modul în care practicienii contribuie la scăderea sau la creşterea riscului generat de digitalizarea proceselor. Obiectivul prezentei lucrări este de a cerceta măsura în care contabilii şi auditorii din România înțeleg şi protejează datele şi cunosc aşteptările companiilor pentru care lucrează şi ale organismelor profesionale.

2. Analiza literaturii de specialitate

Schimbarea rolului practicienilor odată cu evoluția sistemelor şi a aplicațiilor utilizate pentru desfăşurarea activităților presupune o realiniere a abilităților de lucru ale practicienilor contabili pentru a putea gestiona eficient volumul de date atât prin prisma conținutului datelor financiare, cât şi prin prisma menținerii şi îmbunătățirii caracteristicilor fundamentele ale datelor: confidențialitate, integritate şi disponibilitate. Schimbările modului de raportare financiară, dar şi modificările proceselor au generat nevoi diferite din partea investitorilor şi a managementului, iar asigurarea asupra securității optime a sistemelor şi procedurilor de lucru utilizate nu este opțională (No şi Vasarhelyi, 2017).

Literatura de specialitate din domeniul securității informațiilor contabile propune metode prin care practicienii din acest domeniu pot să mențină confidențialitatea datelor (Hawker, 2005; Seetharaman et al., 2017; Bawaneh, 2018) prin revizuirea drepturilor de acces ale utilizatorilor la aplicații, utilizarea soluțiilor criptografice, implementarea unor controale interne eficiente pentru a reduce vulnerabilitățile şi a crea un set de proceduri pentru menținerea securității informațiilor. Dar, ca urmare a complexității tehnologiilor actuale şi emergente care pot fi adoptate în contabilitate, aceste metode nu reuşesc să acopere în totalitate varietatea de riscuri.

Datorită faptului că viitorii şi actualii profesionişti îşi dezvoltă abilitățile necesare practicării acestei profesii prin intermediul a două surse, organismele profesionale şi mediul universitar, trebuie luat în considerare modul în care ambele contribuie la dezvoltarea şi formarea continuă a contabililor şi auditorilor financiari. Pentru a-i pregăti pe viitorii şi actualii practicieni să răspundă corespunzător nevoilor mediului de afaceri, organismele profesionale internaționale au început în ultimii ani să atragă atenția atât asupra necesității dobândirii unui set suficient de competențe de lucru cu actualele şi viitoarele tehnologii utilizate, dar şi să protejeze datele, prin evitarea manipulărilor incorecte sau a expunerii şi crearea unor controale suficient de riguroase pentru a reduce riscurile de securitate a informațiilor (ACCA, 2016). Cu toate acestea, în cadrul raportului ACCA regăsim doar foarte puține informații despre modul în care practicienii pot să acopere aceste riscuri, astfel sfera de cunoştințe care trebuie dezvoltate nu este pe deplin definită. În opinia autorului, organismele profesionale ar trebui să ofere un set clar de atribuții pe care practicienii contabili este necesar să îl dezvolte pentru a reuşi să reducă impactul vulnerabilităților existente.

ICAEW (2015) îi îndeamnă pe practicieni să îşi dezvolte competențele digitale pentru a înțelege şi utiliza noile

tehnologii pentru a gestiona volumul tot mai mare de informații din cadrul proceselor contabile şi a trage un semnal de alarmă pentru a evidenția riscurile asociate manipulării incorecte a informațiilor, care poate avea ca finalitate periclitarea confidențialității datelor. Totodată, ICAEW propune o nouă reprezentare, în care rolul contabilului se distanțează de aparența tradițională spre un nou rol, bazat mai mult pe activități de analiză financiară şi previziuni pentru management.

Aşteptările pe termen lung sunt ca tot mai multe tehnologii emergente să fie integrate şi utilizate de către departamentele de contabilitate pentru a putea răspunde competiției din piață. Astfel, setul de abilități referitoare la tehnologiile informatice pe care actualii şi viitorii profesionişti contabili trebuie să îl dezvolte este într-o continuă schimbare, dar, conform literaturii de specialitate, în prezent există un decalaj între cerințele mediului de afaceri şi programele de studiu ale universităților, din cauza lipsei unei comunicări active (Blount, 2016). Datorită faptului că planurile de studii din mediul academic sunt fundamentul pregătirii profesionale, este vitală reanalizarea programelor de studiu, pentru ca universitățile să îi păstreze pe studenți activi şi să îmbunătățească posibilitatea de a se integra în câmpul muncii. Facultățile trebuie astfel să răspundă urgent schimbărilor generate de adopția tot mai frecventă a tehnologiilor emergente, în caz contrar existând riscul ca tot mai mulți potențiali studenți să aleagă alte programe de studii, care le vor oferi o bază suficientă de cunoştințe.

În România, conform studiului efectuat de Stanciu şi Rîndaşu (2017), majoritatea facultăților publice de contabilitate oferă o dublă specializare atât în domeniul contabil, cât şi în domeniul informaticii de gestiune, dar, cu toate acestea, autorii au concluzionat, după analizarea planurilor de studii ale programelor de master şi licență, că doar în puține cazuri erau incluse materii precum sisteme informatice de gestiune, securitatea datelor, audit IT şi tehnologii emergente, care sunt actualmente printre cele mai cerute competențe de către piața muncii şi mediul de afaceri. Acest rezultat confirmă ideea decalajului dintre abilitățile pe care practicienii le dezvoltă în cadrul mediului academic şi aşteptările companiilor, iar nealinierea pregătirii universitare la noile cerințe ale profesiei şi mediului de afaceri va determina pe termen mediu şi lung neacoperirea aptitudinilor cerute de către angajatori ca urmare a revizuirii cerințelor de angajare şi a creşterii numărului de incidente de securitate, din cauza diversității şi importanței informațiilor. Cu toate acestea, conform studiului efectuat de Stanciu şi Tinca (2018), lipsa personalului bine pregătit reprezintă doar o parte a cauzelor incidentelor, cealaltă parte fiind reprezentată de lipsa bugetelor şi complexitatea implementării unor controale eficiente.

3. Metodologia cercetării

Scopul acestei lucrări este de a analiza percepția practicienilor din domeniul contabil în legătură cu securitatea informațiilor şi de a afla dacă aceştia se consideră suficient de bine pregătiți pentru a face față provocărilor de a menține caracteristicile fundamentale ale informațiilor contabile. Totodată, în cadrul cercetării sunt incluse şi elemente care să determine dacă practicienii manifestă un comportament corect pentru reducerea riscurilor securizării datelor şi dacă au suficiente informații astfel încât să acționeze corespunzător în cazul depistării unui atac cibernetic. Pentru a îndeplini acest obiectiv, am realizat o cercetare empirică calitativă, sub forma unui chestionar cu 20 de întrebări cu una sau mai multe variante şi de tipul matrice de răspunsuri.

Acest chestionar a fost adresat exclusiv practicienilor din domeniul contabil, în particular celor din contabilitate şi audit financiar, fiind transmis potențialilor respondenți prin intermediul rețelelor profesionale de socializare şi în cadrul grupurilor online de practicieni. Răspunsurile au fost colectate în perioada ianuarie – februarie 2019, fiind primite 137 de răspunsuri şi un răspuns a fost eliminat, deoarece participantul nu era parte din grupul țintă, având astfel în final 136 de răspunsuri valide.

Din punct de vedere al experienței în domeniu, media anilor de activitate în domeniu este de 10 ani, iar acest rezultat reprezintă una dintre primele concluzii ale acestei cercetări, faptul că există o maturitate a participanților, care ar trebui să dețină suficiente cunoştințe despre securitatea informațiilor şi să manifeste un comportament corect de protecție a datelor. Analizând răspunsurile oferite de participanți referitoare la apartenența în cadrul organismelor profesionale, 73 de practicieni, ce reprezintă 53,67% din totalul respondenților chestionarului, sunt membri în cadrul a cel puțin unei organizații profesionale.

Companiile mari adoptă mult mai uşor tehnologii noi deoarece au la dispoziție bugete mai mari pentru

investiții, motiv pentru care am considerat oportun să se ia în considerare şi mărimea companiilor, plecând astfel de la premisa că participații din organizațiile cu peste 250 de angajați au mai multe cunoştințe despre securitatea datelor. Analizând rezultatele obținute, majoritatea respondenților (44,8%) lucrează în companii mari, 39% în companii medii cu mai puțin de 250 de angajați şi 16,2% activează în organizații cu mai puțin de 10 angajați.

4. Rezultatele cercetării

Chestionarul cuprinde patru secțiuni, prima fiind cea referitoare la experiența în domeniu şi apartenența la organismele profesionale. În a doua parte a chestionarului studiul s-a axat pe analiza calității şi cantității de cunoştințe privind securitatea informațiilor pe care participanții le primesc atât din partea companiilor pentru care lucrează, cât şi din partea organismelor profesionale. Majoritatea practicienilor (88,2%) care au răspuns la chestionar consideră că organizațiile ar trebui să ofere programe de formare pentru a îmbunătăți securitatea datelor, dar numai 63,2% au afirmat că au urmat un astfel de curs. În urma acestui rezultat, se poate constata faptul că organizațiile trebuie să acorde un grad mai mare de atenție acestui aspect, deoarece vulnerabilitățile IT nu sunt universale, fiecare infrastructură informatică având propriile caracteristici şi provocări.

Datorită faptului că factorul uman continuă să reprezinte un element semnificativ ce poate diminua sau accentua riscurile de expunere sau pierdere a informațiilor, companiile trebuie să realizeze importanța pe care programele de formare le pot avea în reducerea riscurilor având ca efect atât pierderi financiare, cât şi scăderea gradului de încredere al investitorilor (Colwill, 2009). De-a lungul timpului, metodele de inginerie socială s-au îmbunătățit şi au generat mai multe atacuri din cauza lipsei de personal bine pregătit pentru a le recunoaşte, iar cea mai sigură soluție de combatere este reprezentată de sesiuni de instruire eficiente (Greitzer et al., 2014).

Dintre cei 53,7% participanți care sunt membri ai organizațiilor profesionale naționale şi internaționale, 54,79% consideră că primesc suficiente informații referitoare la securitatea datelor, 31,50% afirmă că primesc anumite informații, dar consideră că nu sunt suficiente, iar restul participanților au răspuns că nu primesc nicio informație în acest sens. Acest rezultat indică existența unui decalaj între planurile de formare ale organismelor profesionale pe termen lung şi aşteptările mediului de afaceri. Securitatea informațiilor este într-adevăr un subiect complex, ce presupune o învățare continuă, dar în lipsa unei baze suficiente de abilități pentru a proteja datele sensibile şi confidențiale, impactul şi frecvența atacurilor cibernetice vor creşte semnificativ.

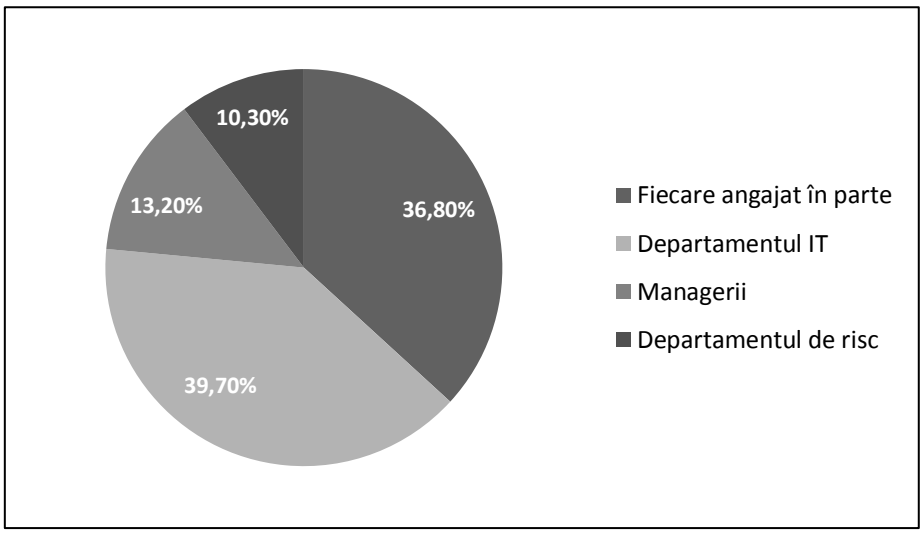
Din 25 mai 2018, la nivelul tuturor țărilor din cadrul Uniunii Europene, Regulamentul General Privind Protecția Datelor (GDPR) a intrat în vigoare şi se referă la protecția datelor personale. Având în vedere faptul că în domeniul contabil o parte semnificativă a datelor au aspect personal, acest regulament ar fi trebuit să determine companiile să ofere cursuri angajaților pentru a nu încălca principiile reglementării. Un studiu realizat de Stanciu şi Rîndaşu (2018), cu două luni înainte ca GDPR să intre în vigoare, a scos în evidentă faptul că în acel moment doar un procent destul de mic de practicieni din domeniul contabil din România a fost instruit. Pentru a analiza dacă într-adevăr s-au produs schimbări la un an de la aplicarea regulamentului, participanții studiului au fost întrebați dacă utilizează date personale şi dacă au primit din partea organizației sesiuni de formare. Analizând răspunsurile primite, se constată faptul că 77,9% dintre respondenți utilizează date personale, dar numai 66,03% dintre cei 103 participanți confirmă că au fost instruiți. Comparând acest rezultat cu cel al studiului menționat anterior, nu se identifică schimbări semnificative, fapt ce ar trebui să ridice un semnal de alarmă, mai ales din cauza faptului că, în cazul în care regulamentul nu este respectat, sancțiunile sunt semnificative din punct de vedere financiar.

Prin întrebările din a treia partea a chestionarului, s-a urmărit investigarea acțiunilor practicienilor ce pot afecta securitatea datelor. Astfel, respondenții au primit un set de întrebări referitoare la responsabilitatea securității datelor, gestiunea conturilor şi a parolelor. După analizarea răspunsurilor primite, s-a putut observa existența unor acțiuni ce cresc riscul gestionării incorecte a datelor: 4,4% dintre participanți au afirmat că folosesc aceleaşi parole pentru accesarea conturilor personale şi profesionale, iar 14% au confirmat că în cadrul echipelor în care lucrează, conturile şi parolele la aplicații nu sunt individuale, aspect ce poate duce inclusiv la fraudă, în

lipsa mijloacelor de identificare unică a utilizatorilor. Totodată, fiind întrebați dacă au împărtăşit datele de acces în cadrul echipei, 11% dintre respondenți au răspuns afirmativ, iar 3,7% au confirmat că le-au fost cerute parolele, dar nu le-au oferit. Astfel de acțiuni pot avea ca efect consecințe multiple şi majore, vizând chiar pierderi financiare, şi ar trebui să reprezinte un semnal de alarmă pentru companii.

Din punct de vedere al responsabilității pentru menținerea securității datelor, majoritatea respondenților consideră că departamentul IT este responsabil, fiind urmat de fiecare angajat în parte, managerii şi departamentul de risc (**Figura nr. 1**). Răspunsurile oferite arată că peste 60% dintre practicieni consideră că nu sunt responsabili de securitatea datelor, fapt ce sporeşte îngrijorarea cu privire la modul în care datele sensibile şi confidențiale sunt gestionate. Departamentele IT pot să impună nişte controale de prevenție pentru a evita accesul neautorizat şi expunerea datelor, dar aceste soluții nu reuşesc să evite complet astfel de riscuri, mai ales în situația în care personalul care utilizează datele nu are suficiente cunoştințe şi adoptă practici contrare menținerii securității.

Figura nr. 1. Percepția respondenților despre responsabilii menținerii securității datelor



Sursa: Prelucrare proprie, bazată pe răspunsurile primite de la participanții la studiu

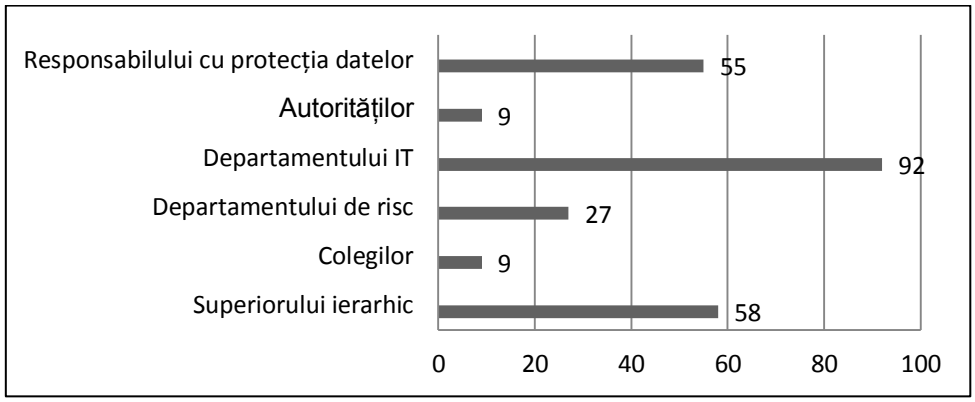
Prin ultima parte a chestionarului, obiectivul a fost de a studia percepția participanților cu privire la cunoştințele deținute referitoare la securitatea datelor. Având în vedere faptul că tehnicile de inginerie socială continuă să reprezinte una dintre cele mai importante vulnerabilități, participanții au fost întrebați dacă au cunoştințe despre atacurile de tipul phishing, iar majoritatea (68,4%) a răspuns pozitiv. Acest rezultat nu trebuie privit ca fiind pozitiv, din cauza faptului că există o populație semnificativă care nu are suficiente cunoştințe pentru a evita să devină victima unui astfel de atac. Pentru a reduce riscurile, companiile ar trebui să demareze campanii de instruire în acest sens prin care să le atragă atenția angajaților despre astfel de pericole, dar, chiar şi în astfel de cazuri, literatura de specialitate arată că rata de evitare nu este absolută, din cauza faptului că acest tip de atac este într-o continuă perfecționare şi reuşeşte să treacă nedetectat şi de personalul instruit (Alsharnouby et al., 2015).

Participanții au fost întrebați dacă sunt de părere că au suficiente cunoştințe pentru a detecta dacă laptopul sau calculatorul pe care îl folosesc a fost ținta unui atac cibernetic, iar 39,7% au răspuns afirmativ, 19,1% au afirmat că nu ar putea detecta, iar 41,2% nu au certitudinea că ar putea identifica o astfel de situație, deoarece consideră că nu au suficiente cunoştințe. Conform raportului publicat de

Ponemon Institute (2018), în medie existența unui atac se identifică în 196 de zile, timp suficient pentru ca datele confidențiale să fie expuse.

Întrebați cui se adresează în momentul în care detectează că au fost victima unui atac cibernetic, majoritatea a răspuns că se adresează departamentului IT, superiorului ierarhic şi departamentului responsabil de protecția datelor (**Figura nr. 2**). Chiar dacă angajații au suficiente cunoştințe pentru a detecta un atac cibernetic este important să ştie cui se pot adresa pentru a minimiza eventualele pierderi. Astfel, companiile trebuie să emită proceduri care să ofere indicații clare, pentru a putea acționa cât mai repede.

Figura nr. 2. Persoanele cărora se adresează practicienii contabili atunci când bănuiesc că au fost ținta unui atac cibernetic



Sursa: Prelucrare proprie, bazată pe răspunsurile primite de la participanții la studiu

În cadrul ultimei întrebări a chestionarului, participanții au autoevaluat pe o scară de 5 puncte (0 – dezacord total, 5 – acord total) gradul de conştientizare a impactului securității datelor, nivelul de cunoştințe, importanța datelor pe care le gestionează şi impactul pe care îl au în reducerea riscurilor, iar analiza statistică a răspunsurilor primite de la respondenți este detaliată în **Tabelul nr. 1**.

Tabelul nr. 1. Analiza statistică a răspunsurilor primite

	Modificarea gradului de conştientizare a impactului securității datelor	Suficiente cunoştințe pentru a asigura securitatea datelor	Existența activităților ce ar putea afecta securitatea datelor	Informațiile gestionate nu prezintă niciun risc
Medie	3.94	3.57	2.85	2.72
Deviație standard	1.24	1.14	1.32	1.33
Minimum	1	1	1	1
Nr. min.	12	9	31	36
Frecvență min.	8.82%	6.62%	22.79%	26.47%
Maximum	5	5	5	5
Nr. max.	59	30	16	13
Frecvență max.	43.38%	22.06%	11.76%	9.56%
Mediana	4	4	3	3
SKEW	-1.15	-0.63	-0.02	0.09

Sursa: Prelucrare proprie, bazată pe răspunsurile primite de la participanții la studiu

Conform analizei statistice, majoritatea participanților consideră că în ultima perioadă şi-a modificat gradul de conştientizare al impactului pe care securitatea incorectă a datelor îl poate avea asupra organizațiilor şi consideră că au un nivel mediu de cunoştințe pentru a asigura caracteristicile fundamentale ale datelor. Aceste rezultate sunt conforme cu răspunsurile primite de la respondenți la întrebările anterioare şi se poate evidenția faptul că majoritatea practicienilor manifestă un comportament relativ corect, chiar şi în lipsa unor sesiuni de instruire. De asemenea, din punct de vedere al existentei activităților care ar putea afecta securitatea datelor gestionate, majoritatea consideră că nu aduc un aport riscurilor deja existente şi sunt conştienți de impactul manipulării neadecvate a datelor, dar trebuie avut în vedere faptul că acest rezultat a fost obținut ca urmare a unei autoevaluări a participanților asupra propriilor aptitudini, scopul lucrării nefiind testarea nivelului real al cunoştințelor deținute.

Concluzii

În cadrul acestui lucrări s-a studiat percepția practicienilor din domeniul contabil cu privire la securitatea datelor, focalizând analiza pe următoarele aspecte: cantitatea şi calitatea informațiilor primite de la companiile pentru care lucrează şi de la organismele profesionale, responsabilitatea asupra menținerii calității datelor şi percepția asupra riscurilor.

Cu toate că organismele profesionale accentuează importanța securității informațiilor, un procent semnificativ de membri consideră că informațiile primite nu sunt suficiente sau chiar lipsesc cu desăvârşire, iar în cadrul companiilor unde activează nu toți beneficiază de o instruire adecvată care să le ofere o bază suficientă pentru a putea adresa problemele de securitate. Pentru a depăşi acest decalaj atât organizațiile profesionale, cât şi companiile trebuie să acorde un grad mai mare de atenție spre a putea gestiona eficient vulnerabilitățile datelor contabile şi ale sistemelor utilizate.

Din punct de vedere al responsabilității față de protecția datelor, majoritatea practicienilor manifestă un comportament relativ corect, dar din cauza faptului că nu primesc suficiente informații nu consideră că ar putea gestiona în totalitate riscurile generate de datele utilizate. Utilizarea conturilor comune şi a codurilor de acces reprezintă o practică ce creşte semnificativ riscul de afectare a integrității datelor, iar companiile ar trebui să revizuiască procedurile de lucru, pentru a evita continuarea menținerii acestor vulnerabilități.

Practicienii consideră că au suficiente cunoştințe pentru a gestiona corect datele şi consideră că de-a lungul timpului gradul de conştientizare asupra impactului a crescut, declarând că acesta se reflectă şi în comportamentul acestora. Vom reține aceste opinii cu un anumit scepticism, reprezentând doar opinii subiective ale respondenților, aceştia nefiind subiectul unei evaluării a nivelului de cunoştințe privind securitatea datelor. Există un număr semnificativ de respondenți care consideră că activitățile pe care le întreprind nu reprezintă un risc, cu toate că gestionează date personale fără a fi primit o instruire adecvată.

Factorul uman reprezintă un element semnificativ în menținerea securității informațiilor, dar în lipsa suportului adecvat şi al procedurilor care să ofere suficiente informații pentru a gestiona eficient vulnerabilitățile, riscurile asociate datelor contabile continuă să reprezinte o provocare. În urma analizării tuturor răspunsurilor oferite de participanții la studiu, constatăm existența unui decalaj între nevoile companiilor şi suportul pe care acestea îl oferă practicienilor, pentru a răspunde cererilor şi a acționa ca protectori ai datelor.

BIBLIOGRAFIE

1. Alsharnouby, M., Alaca, F., & Chiasson, S. (2015), Why phishing still works: User strategies for combating phishing attacks, *International Journal of Human-Computer Studies*, 82, pp. 69-82.
2. Bawaneh S. (2018), Securing Information Technology for Banks and Accounting Information Systems, *International Journal of Applied Engineering Research*, Vol.13, 6 (2018) pp. 3291-3300
3. Blount, Y., Abedin, B., Vatanasakdakul, S., & Erfani, S. (2016), Integrating enterprise resource planning (SAP) in the accounting curriculum: a systematic literature review and case study, *Accounting Education*, 25(2), pp. 185-202

4. Colwill, C. (2009), Human factors in information security: The insider threat–Who can you trust these days?, *Information security technical report*, 14(4), pp. 186-196.
5. Greitzer, F. L., Strozer, J. R., Cohen, S., Moore, A. P., Mundie, D., & Cowley, J. (2014), Analysis of unintentional insider threats deriving from social engineering exploits, *IEEE Security and Privacy Workshops*, pp. 236-250
6. Hawker, A. (2005), *Security and control in information systems: A guide for business and accounting*, Routledge
7. ICAEW (2015), *Providing leadership in a digital world*, disponibil online la https://www.icaew.com/-/media/corporate/files/technical/information-technology/technol ogy/providing-leadership-digital-full-report.ashx (accesat 17 februarie 2019)
8. No, W. G., & Vasarhelyi, M. A. (2017), Cybersecurity and continuous assurance, *Journal of Emerging Technologies in Accounting*, 14(1), 1-12.
9. Ponemon Institute (2018), *2018 Cost of Data Breach Study: Global Overview*, disponibil online la https://www.ibm.com/downloads/cas/861MNWN2 (accesat 17 februarie 2019)
10. Regulation (EU) 2016/679 (General Data Protection Regulation) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, which repeals Directive 95/46/EC
11. Seetharaman, A., Patwa, N., & Niranjan, I. (2017), Role of Accountants and Auditors in Mitigating Digital Crimes, *Journal of Applied Economics & Business Research*, 7(1).
12. Stanciu V. & Rîndaşu S. (2017), Emerging information technologies in accounting – are the aspiring professional accountants prepared to face the challenges? A case study of Romanian universities, *Proceedings of the 29th International Business Information Management Association Conference*, 2455-2467
13. Stanciu, V. & Rîndaşu, S., (2018), The Impact of General Data Protection Regulation in The Accounting Profession – Evidences from Romania, *Journal of Information Assurance & Cyber security*, Vol. 2018
14. Stanciu, V., & Tinca, A. (2017), Exploring cybercrime–realities and challenges, *Accounting and Management Information Systems*, 16(4), 610-632
15. The Association of Chartered Certified Accountants (2018), *Strategic Business Leader (SBL) Syllabus and study guide*, disponibil online la https://www.accaglobal.com /conte nt/dam/acca/global/PDF-students/acca/SBL/Strategic-Business-Leader-syllabus-and-study-guide-D17.pdf (accesat 17 februarie 2019)
16. The Association of Chartered Certified Accountants (2018), *Market change is faster than ever – is your finance function in the race?*, disponibil online la https://www.accaglobal.com /content/dam/ACCA_Global/Technical/fin/PI-Market-change-is-faster-than-ever%20-is-your-finance-function-in%20-the-race.pdf (accesat 17 februarie 2019)