

Despre valoarea reală a cunoștințelor, capitalul intelectual și reziliența în noua economie a cunoașterii

Lect.univ.dr. Călin Mihai Rangu*

Director, Autoritatea de Supraveghere Financiară, București, România

Rezumat

Societatea în care trăim este definită ca o societate a cunoașterii, iar economia este o economie post-cunoaștere, care este un amestec de cunoștințe și rețele. În termeni de capital intelectual (IC) acest lucru înseamnă de fapt capitalul structural (SC) ce este derivat din capitalul uman (HC) și capitalul relațional sau strategic alianței (SAC) care devin aspectele cheie.

Persoanele posedă IC bazat pe active necorporale cunoscute, explicite sau tacite. Dețin unele valori, recunoscute informal, dar adesea ignorate formal. Atacurile cibernetice vizează exact aceste valori.

Cuvântul „cunoaștere” are multe valențe. El fiind unul dintre cele vizate de infracțiunile informatice (bani, identități, proprietate intelectuală etc.).

Una dintre principalele probleme este faptul că cunoștințele nu oferă abilități, iar ruptura dintre abilități și cunoștințe lasă atacuri libere, practici frauduloase, pierderi astronomice aduse de infracțiunea informatică.

Standardele contabile rămân un tribut adus principiilor clasice neadaptate realității societății cunoașterii. Din acest motiv, valoarea activelor diminuate ca urmare a pierderilor cibernetice este dificil de cuantificat. Acest lucru este parțial cauzat de faptul că firmele au inventariat imobilizările corporale, în timp ce cele mai multe infracțiuni informatice se concentrează pe imobilizări necorporale, care rareori au inventar. Acest lucru poate fi parțial rezolvat prin utilizarea tehnologiilor de activare, cum ar fi învățarea automată, inteligența artificială și robotica. Acest lucru se observă cel mai bine la nivelul extrem de scăzut al asigurării de risc cibernetic. Ar trebui să implementăm politici, strategii pentru a acoperi acest decalaj.

La nivel uman este necesară trecerea de la acumularea cunoștințelor la dezvoltarea abilităților, la cunoaștere.

La nivel contabil este necesară crearea sistemului de evaluare și înregistrare a activelor intangibile ale cunoștințelor și rețelilor, capitalului uman, structural și relațional.

Cuvinte cheie: capital intelectual, risc cibernetic, active

Clasificare JEL: D81, G22, H56, M15

*Autor de contact, **Călin RANGU** - Calin.RANGU@asfromania.ro
Articol republicat din Revista "Considerations on challenges and future directions in cybersecurity", RAISA 2019, cu permisiunea editorului.

1. Despre riscul cibernetic și activele (ne) cunoscute sau (ne) acoperite

Dacă ne uităm tehnic, atacurile cibernetice duc la perturbarea activităților / afacerilor, prin înghețarea infrastructurilor publice sau private, a infrastructurilor productive, financiare etc., care afectează oamenii și proprietățile, prin compromiterea confidențialității, disponibilității sau integrității datelor sau serviciilor¹. Dar acesta este efectul. Cauza este umană, vorbim despre oameni și despre bunurile lor care sunt afectate, oameni care își asumă responsabilități și iau măsuri sau cei care îi ignoră cu bună știință sau ignoranță.

Conform analizei tematică a Autorității de Supraveghere Financiară (A.S.F.) cu privire la asigurarea de risc cibernetic², conducerea instituțiilor și companiilor în același timp cu angajații sunt responsabile, rolul oamenilor fiind esențial.

Instituțiile sau companiile au nevoie de o strategie globală de gestionare a riscurilor cibernetice pentru a reveni la operațiunile normale cât mai repede posibil, cu cel mai mic cost. Oamenii trebuie să dezvolte și abilități pe lângă educația tehnică necesară pentru a le oferi cunoștințe de bază. Aceste cunoștințe, experiența acumulată trebuie să fie monetizate. Educația nu trebuie găsită doar la limita cheltuielilor, ci și a imobilizărilor necorporale acumulate în urma educației, pentru a implementa structuri, proceduri, mecanisme bazate pe cunoaștere.

Când vorbim despre riscuri, vorbim despre amenințări (externe, din partea celor care au interes, cunoștințe și abilități), pe de o parte, și vulnerabilități pe de altă parte (cei care au valori intangibile de tipul datelor, informații, valoare monetară sau identitară) care nu știi, nu pot sau nu au abilități, cunoaștere și nu au capacități de apărare. Toate câștigurile obținute prin atacarea imobilizărilor necorporale sunt, de asemenea, achiziții ilegale prin afectarea imaginii companiilor sau a oamenilor, scurgeri de informații, perturbări ale activităților. Dacă cineva câștigă, unde se înregistrează pierderea, unde sunt acele active care dispar, unde o vom vedea în contabilitate? Cert este că acestea nu se regăsesc în contabilitate ca pierderi directe, ca active distruse. Poate că bunăvoința va fi afectată. Creează probleme în dimensionarea pierderii reale. Există probleme implicite în asigurarea acestei pierderi. Un asigurător nu se poate asigura că nici proprietarul acului activ nu îl evaluează înainte de riscul de afectare a produsului.

Amenințările pot fi intenționate (penale, teroriste, ostile, activism, șantaj sau motive personale) sau pot reprezenta evenimente accidentale (ștergeri de date, întreruperi de serviciu).

Stabilirea costului incidentelor cibernetice este o provocare, companiile evitând raportarea pierderilor, indiferent dacă nu pot calcula ei sau nu doresc ca imaginea lor să fie afectată (un alt activ intangibil al capitalului intelectual). Daunele cauzate de riscurile cibernetice sunt estimate la aproximativ 0,5% din PIB-ul mondial și aproape de două ori mai mult decât media anuală a pierderilor cauzate de calamitățile naturale³.

Pe baza unui barometru de risc, realizat prin interviuri pe 968 de participanți, principalele cauze ale pierderile generate de incidentele cibernetice au fost stabilite în anul

¹ L. Badea, C.M. Rangu, „Asigurarea riscului cibernetic - o mare provocare cu care se confruntă economiile moderne”, RSF nr. 6, mai 2019

² https://asfromania.ro/files/analize/Asigurari_risc_cibernetec.pdf [Accesat mai. 09, 2019]

³ L. Badea, C.M. Rangu, „Asigurarea riscului cibernetic - o mare provocare cu care se confruntă economiile moderne”, RSF nr. 6, mai 2019

2019 (Fig.1)⁴: 1. Întreruperea afacerilor; 2. Pierderea reputației; 3. Daune cauzate de pierderea datelor; 4. Costuri de restaurare a datelor; 5. Amenzi și penalități. Vulnerabilitățile pot fi acoperite cu resurse interne sau prin externalizarea riscului. Riscul rezidual, care costă prea mult să fie acoperit intern, poate fi preluat de sistemul de asigurare. Dar acest lucru duce, de asemenea, la o multitudine de cunoștințe și de cunoaștere pentru a o recupera. Acoperirea de risc cibernetic de numai 2025 va acoperi 1% din totalul asigurărilor, potrivit Swiss Re, în timp ce pierderile neacoperite sunt imense.

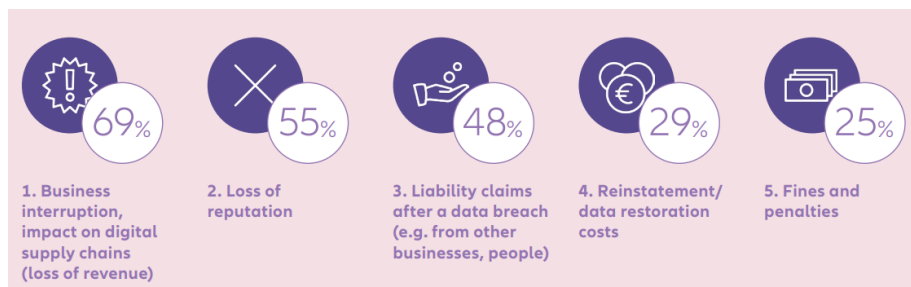


Fig.1 Principalele cauze ale pierderilor economice cauzate de incidente cibernetice

Sursa: Allianz Risk Barometer, 2019

Potrivit lui L. Badea (2019) "Cantitatea de pierderi financiare generate de riscul cibernetic este dificil de estimat, cu un deficit de informații. Unele activități de criminalitate cibernetică nu au un cost direct sau nu pot fi cuantificate. Industria încearcă să estimeze costurile totale, costurile pe incident și costul înregistrării unei încălcări a datelor conform tabelului 1. Fig. 2 prezintă estimări ale costurilor medii informatice anuale pe zone și țările principale afectate"⁵.

Tabelul 1. Costuri determinate de infracțiuni informatice

GLOBAL COSTS (IN BILLION USD, PER ANNUM)		COSTS PER INCIDENT (IN MILLION USD)		COST PER RECORD (IN USD)		COSTS BY COUNTRY (IN % OF GDP; MCAFEE; 2014)	
Symantec (2013)	113	Ponemon Institute (2015)	3.8	Symantec (2013)	298	U.S.	0.64
McAfee (2014)	445 (375-575)	Geschonnek et al. (2013)	2.1	Ponemon Institute (2015)	217	China	0.63
Kshetri (2010)	100-1'000	Kaspersky Lab (2013)	2.4	NetDiligence (2014)	956	Japan	0.02
						Germany	1.60

Sursa: Asociația Geneva, 2016

⁴ Allianz Global Corporate & Specialty, „Allianz Risk Barometer” 2019

⁵ Ten Key Questions on Cyber Risk and Cyber Risk Insurance, Geneva Association, Nov 2016

Conform Accenture, cele mai mari daune informatice sunt înregistrate în domeniul pierderilor de informații stocate electronic, urmate de pierderi de afaceri, pierderi de afaceri și daune echipamentelor (Fig. 2):

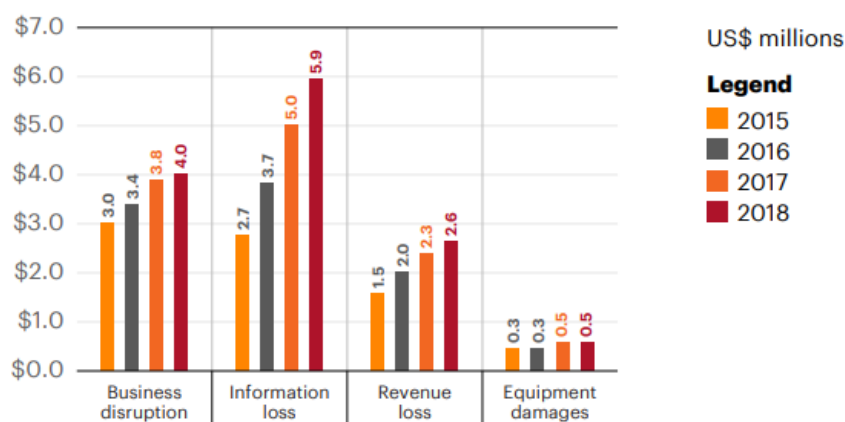


Fig. 2 Acoperirea anuală a costurilor legate de criminalitatea cibernetică pe principalele domenii ale pierderilor

Sursa: Accenture, 2019

Potrivit lui L. Badea și C. Rangu (2019), asigurarea pentru riscuri informatice poate juca un rol esențial în preluarea/transferul riscurilor la care sunt expuse companii și persoane. „Acesta poate fi un instrument care completează (și nu înlocuiește) cadrul de gestionare a riscurilor pe care fiecare organizație ar trebui să îl aibă și ar trebui să fie un element de stabilitate economică și socială, atât pentru infrastructurile critice, atât comerciale, cât și personale, inclusiv pentru sectorul financiar. Asigurarea riscului cibernetic ar trebui să fie utilizată în evaluarea solidității financiare / a activității de susținere a forței de muncă prin recuperarea rapidă a pierderilor și continuarea activității”. Dar cum să facem aceasta este cea mai mare provocare, în care metodologiile IC sunt esențiale.

2. Despre capitalul intelectual (CI)

Conform F. Stibli⁶ „capitalul intelectual al unei organizații este împărțit în patru categorii: active centrate pe oameni, infrastructuri de ansamblu, active de proprietate intelectuală și active de piață”. Se poate observa că toate aceste active pot avea impact asupra ciber-spățiului și pot genera profituri atacatorilor. Fiecare dintre ele trebuie evaluat, inclusiv din punct de vedere monetar pentru a putea stabili imaginea riscului și pentru a le proteja deoarece „cunoștințele pot fi transformate în valoare”, în conformitate cu Leif Edvinsson și Sullivan Pat.

⁶ F. Stibli, Intellectual capital -the key resource for expanding organisational intelligence, <https://intelligence.sri.ro/capitalul-intelectual-resursa-cheie-pentru-extinderea-inteligenței-organizationale/> [Accessed: May. 10, 2019]

Thomas Davenport (Davenport, 1999) construiește un model de angajat ca investitor în capitalul uman (educațional)⁶. El observă că, în ultimii ani, numărul de locuri de muncă extrem de specializate a crescut la toate nivelurile de învățământ, în detrimentul muncii necalificate, slab specializate, precum și a managerilor de niveluri inferioare (majori, lideri de echipă etc.). Astfel, investiția în învățare pe tot parcursul vieții apare ca o prioritate pentru indivizi și asigurare împotriva riscurilor șomajului și sărăciei. Pe de altă parte, companiile pot obține un profit mai mare investind, mai degrabă, în educația angajaților lor, decât în creșterea stocului de capital economic".

Începând cu 1999⁷ s-a observat că ar fi timpul să definească conceptele de imobilizări necorporale, capital uman și cunoștințe. Comitetul internațional de contabilitate internațională - Contabilitatea internațională STANDARD IAS 38 definește o imobilizare intangibilă ca un activ non-monetar identificabil, fără substanță fizică, activ identificabil, fără sprijin material și reținut pentru utilizare în procesul de producție sau furnizarea de bunuri sau servicii, pentru a fi închiriat altor persoane sau în scopuri administrative. Particularitățile sunt reprezentate de natura identificabilă, controlul asupra unei resurse și existența viitorului, beneficii economice.

Capitalul intelectual (CI) care ne interesează în această analiză este capitalul uman (referindu-ne la cunoștințe, abilități, motivație, relații de echipă, pe scurt toți factorii în raport cu angajații care promovează performanța pe care clienții sunt dispuși să o plătească) și capitalul structural, referindu-se la „tot ce a rămas când oamenii au plecat noaptea” (Edvinsson & Malone, 1997, p. 17), cum ar fi baze de date, structura procedurilor detaliate transpuse în software etc.⁸ Gestionarea eficientă a IC constă în gestionarea hibrizilor în special HC -SC, SC-SAC, SC-CC, HC-SAC și HC-CC.

Valoarea umană este definită de OECD⁹ ca fiind cunoștințele, abilitățile, competențele și atributele încorporate în indivizi care facilitează crearea unei bunăvoințe personale, sociale și economice. Educația nu este singura sau principala formă de dezvoltare a HC. Experiența, ideile și rețelele pot fi la fel de importante. Însă educația este importantă pentru dezvoltarea capitalului uman. În înregistrările companiei avem doar cheltuielile studiilor, nu activul uman ca valoare umană suplimentară. Bărbatul / femeia este singurul activ care trebuie apreciat continuu, în comparație cu celelalte active care se amortizează continuu. Există cercetători precum Ludo Pyis de la Areopa care propune, de asemenea, formula pentru calcularea valorii umane. Atunci când activul uman este evaluat, îl va găsi plasat în bilanțul / bilanțul contabil al companiei, apoi omul va fi poziționat corect în companie, în societate. Însă, pentru aceasta, registrele generale și metodele contabile trebuie actualizate și există metodologii specifice.

Un exemplu este Wissensbilanz-declarația privind intelectualul-capitală - dezvoltată de Fraunhofer Institut¹⁰ care este „un instrument esențial pentru menținerea

⁷ 10 June 1999 HOLISTIC MEASUREMENT OF INTELLECTUAL CAPITAL COUNTRY covered: AUSTRIA RESEARCH TEAM: Manfred Bornemann, Karl Franzens University Adolf Knapp, Karl Franzens University

⁸ Edvinsson Malone Intellectual Capital, Realizing your Company's true Value by finding its hidden Brainpower. New York: Harper Business, 1997, p. 17

⁹ Human Capital-The Value of People <https://www.oecd.org/insights/humancapital-thevalueofpeople.htm>

¹⁰ Wissensbilanz, https://www.academy.fraunhofer.de/en/continuing-education/technology-innovation/intellectual_capital_statement.html

avantajului competitiv și menținerea cu succes a activității lor în economia bazată pe cunoaștere."

O clasificare generală recunoscută împarte KBC¹¹ în trei categorii: "Informații despre computer (software și bază de date), proprietăți inovatoare (brevete, drepturi de autor, design, mărci comerciale) și abilități economice (inclusiv capital de marcă, capital uman specific companiei, rețele și instituții ale oamenilor și cunoștințe organizaționale care cresc eficiența întreprinderii (Corrado, Hulten, și Sichel, 2005) ". Astfel apare a treia componentă importantă a capitalului intelectual, capitalul relațional / client.

Ca rezumat, Tabelul 2 definește principalele categorii de fenomene ale IC.

Conform AREOPA¹², „în afară de capitalul structural, clasele IC de bază sunt de fapt capitalul social. De exemplu, Capitalul uman (HC) este împărțit cu „proprietarii” săi: atunci când un membru al personalului decide să părăsească organizația, acesta își ia abilitățile și competențele, reputația și potențialul. Reguli similare se aplică atât Clientului Capital (CC), cât și Strategic Alliance Capital (SAC): atunci când clientul își duce afacerea în altă parte sau o alianță se desparte, potențialul de venit al clientului și efectul parteneriatului au dispărut. Consecința acestui fapt este că capitalul intelectual poate trece de la un sector la altul. Și aici intră în joc managementul IC. Este important ca firmele să realizeze unde se află IC-ul lor și ce acțiuni trebuie întreprinse pentru a transforma IC care riscă să fie pierdută în IC care a devenit structurală, adică să-și structureze capitalul uman, al clienților și alianței strategice către măsura maximă posibilă ”.

Tabelul 2. Blocurile de calcul ale calculului ICIC

	Human Capital	Customer Capital	Structural Capital (Organizational Capital)
GUTHRIE (2001)	<ul style="list-style-type: none"> • Know-how; • Education; • Vocational qualification; • Work-related knowledge; • Work-related competencies; • Entrepreneurial spirit • Innovativeness, • Proactive and reactive abilities • changeability 	<ul style="list-style-type: none"> • Brands • Customers • Customer loyalty • Company names • Distribution channels • Business Collaborations • Licensing agreements • Favourable contracts • Franchising agreements 	<ul style="list-style-type: none"> • Patents • Copyrights • Trademarks • Management Philosophy • Corporate Culture • Management processes • Information Systems • Networking Systems • Financial Relations

Sursa: Diapozitive Areopa, Guthrie, 2001

¹¹ OECD (2013), "Introduction and Overview", in Supporting Investment in Knowledge Capital, Growth and Innovation, OECD Publishing, <http://dx.doi.org/10.1787/9789264193307-4-en>

¹² Ludo Pyse, NO CURE, NO PAY? Would applying this rule bring IT projects failure statistics down? ... and how do we measure sure success?, ww.areopa.com

Concluzia lor este următoarea „compania de cunoștințe călătorește ușor. ... Nu numai că activele cheie ale unei companii de cunoștințe sunt intangibile, nu este clar cine le deține sau este responsabil pentru îngrijirea acestora.”

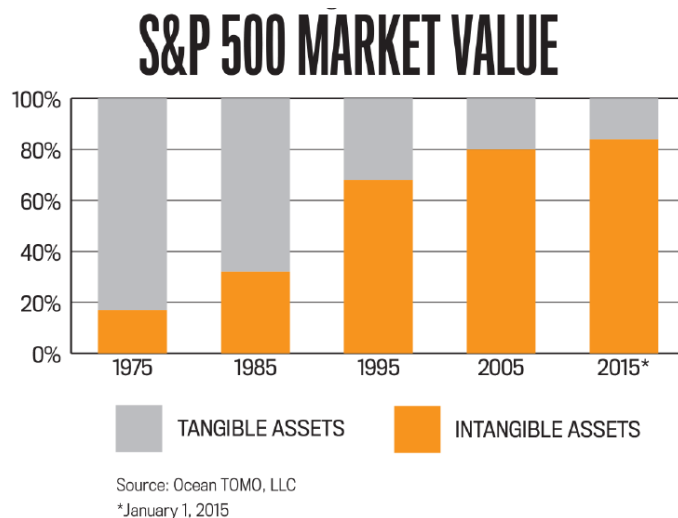


Fig. 3. Evaluarea immobilizărilor necorporale în valoarea de piață S&P 500
Sursa: G. Cokins, 2017

Potrivit lui Cokins, G. și Shepherd, N. (2017), figura 3 arată modul în care „valoarea ascunsă” poate fi făcută vizibilă. Partea din stânga a figurii reprezintă situațiile financiare dezvăluite public întocmite în conformitate cu principiile de contabilitate general acceptate (GAAP) sau cu Standardele internaționale de raportare financiară (IFRS). Mai întâi luați în considerare bilanțul publicat în partea de sus. Eforturile timpurii de înțelegere și cuantificare a diferenței dintre valoarea contabilă și valoarea ajustată cu active adăugate necorporale pot fi urmărite până la începutul anilor 1990 și creșterea managementului cunoștințelor și a capitalului intelectual. O lucrare mai recentă în știința evaluării capitalului intelectual a fost întreprinsă și publicată de AREOPA, o firmă de consultanță lider în gândire, specializată în acest domeniu¹³.

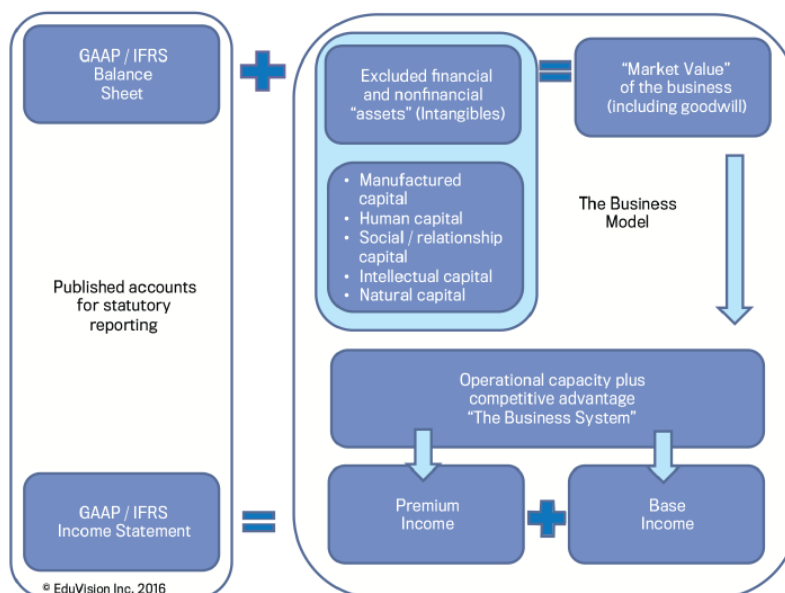
Gary Cokins¹⁴ (2017) arată clar în fig. 4 că noua lume rezultă din immobilizările necorporale și „bilanțul tradițional subliniază valoarea economică a unei companii, deoarece nu include o mare parte din immobilizările necorporale ... Acum patruzeci de ani, mai mult de 80% din media evaluarea companiilor la S&P 500 a fost reprezentată de active corporale, cum ar fi immobilizări corporale, echipamente - majoritatea fiind reflectate în bilanțul unei organizații. -numărul este acum inversat cu peste 80% din valoarea atribuită a unei organizații reprezentată de intangibile, cum ar fi capitalul său intelectual, forța de muncă, lanțurile de aprovizionare și alte relații cheie.

¹³ THE POWER OF INTANGIBLES BY GARY COKINS, CPIM, AND NICK SHEPHERD, FCPA, FCGA, FCCA, May 1, 2017, <https://sfmagazine.com/post-entry/may-2017-the-power-of-intangibles/>

¹⁴ THE POWER OF INTANGIBLES BY GARY COKINS, CPIM, AND NICK SHEPHERD, FCPA, FCGA, FCCA, May 1, 2017, <https://sfmagazine.com/post-entry/may-2017-the-power-of-intangibles/>

Fig. 4 Valoarea ascunsă Vizibilă

HIDDEN VALUE MADE VISIBLE



Sursa G. Cokins, 2017

Din perspectivă contabilă, acest lucru a determinat creșterea calculării unei sume de fond comercial, pe măsură ce organizațiile au fost cumpărate, vândute și amalgamate, iar excesul de achiziție plătit peste valoarea contabilă contabilă a fost raportat ca fond comercial. Un articol recent al lui Bloomberg a citat un studiu Goldman Sachs Global Investment Research care a arătat creșterea continuă a fondului comercial în companiile americane a ajuns la 2,5 miliarde de dolari în ansamblu până în 2015. (Vezi <https://bloom.bg/2pIcKNS>).

3. Evaluarea capitalului intelectual

Comisia Europeană menționează în Raportul de evaluare a proprietății intelectuale¹⁵, în 2013 „oportunitatea, dacă nu este nevoie, de a beneficia de intangibile și, în special, de cei care au o recunoaștere legală, cum ar fi mărcile și drepturile de proprietate intelectuală, pentru favorizarea inovatoare și forme mai consistente de cunoștințe de finanțare bancară pentru creșterea companiei și procesele de investiții. Acest lucru este valabil în special pentru IMM-urile europene intensiv în cercetare”.

¹⁵ https://ec.europa.eu/research/innovation-union/pdf/KI-01-14-460-EN-N-IP_valuation_Expert_Group.pdf

UE subliniază, necesitatea dezvoltării de noi segmente de piețe financiare dedicate evaluării, schimbului și finanțării DPI și a altor materiale intangibile, prin crearea pre-condițiilor și a infrastructurilor necesare. pentru ca aceste piețe să funcționeze într-un mod eficient și eficient la scară europeană”¹⁶

Lipsa măsurării intangibile la nivel micro (adică companie) este o altă prioritate politică recurentă care stă la baza multor probleme de mai sus. Metodele comune de evaluare și contabilitate sunt o problemă de bază relevantă care poate explica dificultatea de a vedea intangibile în situațiile financiare anuale ale companiei și dezvoltările. Această problemă este valabilă în special pentru produsele necorporale generate intern; astfel sunt - în multe cazuri - IPR-urile. După cum a menționat recent domnul Hans Hoogervorst, președintele Comitetului pentru standardele internaționale de contabilitate (IASB)¹⁷ „Imobilizările necorporale sunt neînregistrate (sau subînregistrate) în bilanț știm că standardul [contabilitate] [IAS 38] este rudimentar, deoarece se bazează pe costul istoric, care poate să nu reflecte adevărata valoare a imobilizării necorporale”.

O scurtă analiză a practicilor internaționale pentru elaborarea rapoartelor de capital intelectual¹⁸ poate fi menționată de Brooking¹⁹ care fragmentează în patru categorii: active centrate pe om; Seturi de infrastructură; Active active intelectuale; Active de piață.

Leif Edvinsson a realizat un model și un limbaj standardizate pentru prezentarea CI. Edvinsson concluzionează că rezultatul scăderii valorii contabile a valorii de piață a unei organizații semnifică efectiv CI-ul existent în organizația respectivă, conform formulei²⁰:

$$\text{Market value} = \text{Financial Capital} + \text{CI}$$

Leif Edvinsson²¹ a descompus CI în patru arii distincte: Capital uman; Capital client; Capital proces; Capital de inovație.

L. Pyis²² prezintă elocvent în Fig. 5 etapele prin care biții trec prin data datorată implementării unei sintaxe, informațiilor prin semantică, cunoștințelor reale datorate plasării în context, know-how, experiență și expertiză prin utilizare, prin practică și o abordare eficientă. Reținem că la fiecare nivel există riscul cibernetic, activele de capital intelectual sunt mai valoroase și interesate atât pentru companie, cât și pentru factorii externi.

¹⁶<http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=11602&no=1>

¹⁷ <https://magazine.lucbrates.com/intellectual-capital-and-knowledge-management>

¹⁸<http://www.incd2020.ro/sites/default/files//Analiza%20bune%20practici%20intl%20rapoarte%20CI.pdf>

¹⁹ Brooking A., 1996. Intellectual Capital: Core Asset for the Third Millennium Enterprise. New York: International Thomson Business Press

²⁰ Leif Edvinsson Intellectual Capital: Realizing Your Company's True Value by Finding Its Hidden Brainpower Hardcover, 1997

²¹https://www.researchgate.net/profile/Selcuk_Burak_Hasiloglu/publication/28263308/figure/fig1/AS:394353668313091@1471032649090/Edvinssons-Categorization-of-Capital-Resource-Leif-Edvinsson-and-M-S-Malone.png

²² Ludo PYIS, AREOPA GROUP, IS IT WORTH PROTECTING YOUR INTELLECTUAL CAPITAL FOR CYBER INTRUDERS (PPT presentation), 2013

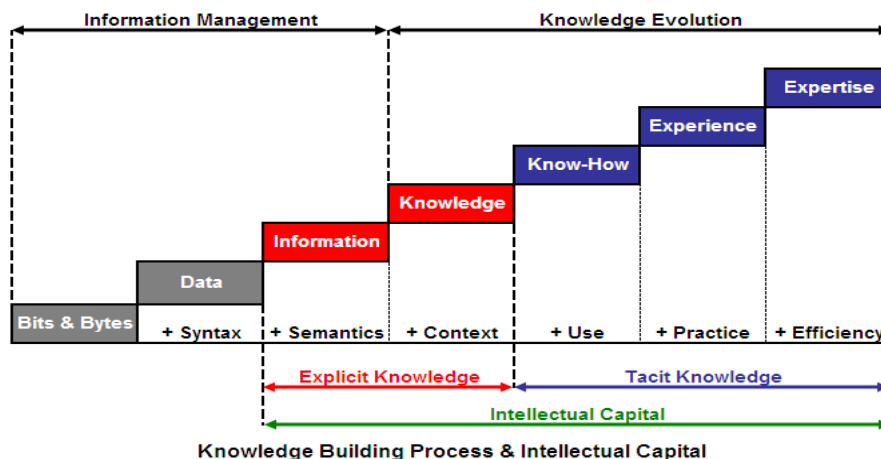


Fig. 5 Procesul de construire a IC

Sursa: Areopa, 2015

Dacă am analizat riscurile pe care le prezintă trunchiul cerebral, acestea sunt legate de riscurile operaționale ale celor generate de oameni, procese și sisteme.

Capitaluri intelectuale cu: Controlul capitalului uman, controlul structural al capitalului, controlul capitalului relațional și alianțelor.

IT este intrarea în schimbare managementul și managementul cunoștințelor, managementul riscului, evaluarea, acoperirea și asigurarea.

Conform cu AREOPA:

- Cunoașterea este critică în timp, virtuală, relevantă, reflectantă, complexă, în evoluție, interactivă, neplăcută, creată cu un scop, dar bazată pe trecut, social, deseori experiență de autoorganizare, realizată prin întrebări, provocări și dezbateri, filtrantă, creativă, selectivă.
- Cunoștințele se găsesc în prezentări, rapoarte, reviste, licențe, brevete, licențe, proprietate intelectuală, baze de date, software, instrumente de risc, audituri, biblioteci, cataloage, arhive, manuale, documente de politică, memorii, capacitate individuală, memorie, know-how, experiență, echipe, comunități, grupuri, rețele.
- Cunoașterea explicită este ușor de identificat, reutilizabilă într-o manieră consistentă și repetabilă - pentru luarea deciziilor și / sau pentru exercitarea judecății, poate fi stocată ca procedură scrisă sau ca procesare într-un sistem informatic, stocată ca artefacte-entități artificiale, fizice sau virtuale care pot fi măsurate, identificate, distribuite și auditate.
- Cunoașterea tacită se prezintă ca lecții învățate, metodologii, cazuri, povești, personal, context specific, dificil de formalizat și comunicat, informații, reguli mentale, seturi de minte, nescrise reguli, valori inconștiența, filozofia fundamentală.

Karl-Erik Sveiby a propus un model pentru metodele de evaluare a IC în conformitate cu fig. 6, în patru categorii: capitalizare de piață, rentabilitate a activelor, IC direct, metode de scor.

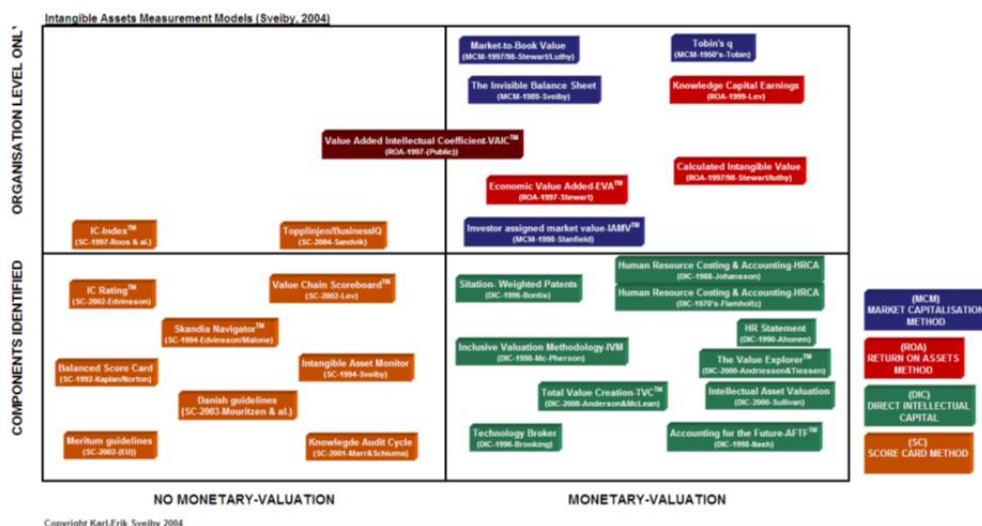


Fig.6 Modelul pentru metodele de evaluare a IC
Sursa: Diapozitiv Areopa, 2015

Pornind de la această abordare, Areopa propune un model de calcul, de la nestructurat la tipurile de capital intelectual foarte structurate.

AREOPA a dezvoltat un model pentru identificarea și cuantificarea intangibililor ca componente ale capitalului intelectual (IC). Acest model servește la evaluarea rentabilității companiei asupra întregului capital pe care îl folosește, contribuind la explicarea diferenței dintre valoarea contabilă și valoarea de piață. De asemenea, oferă îndrumări cu privire la modul în care managementul ar trebui să-și atragă atenția pentru a crește IC-ul global al organizației. Pornind de la noul IAS 38, Lucurbate Peter Walch menționează că „contabilizarea IC creează de fapt un bilanț suplimentar, de asemenea, bazat pe debit, și sistemul de credit în același mod ca standardele de contabilitate financiară. Astfel contabilitatea IC creează o recunoaștere a activelor care nu sunt raportate sau care nu sunt raportate în afara bilanțului. Graficele de mai jos trebuie studiate cu atenție”²³.

²³ Lucurbate Peter Welch October 12th, 2018 Magazine article No: 42, October 8th, 2018

International Accounting Standards (IAS)
IAS 36 Impairment of Assets / IAS 38 Intangible Assets

SUMMARY OF IAS 36

Objective
 To ensure that assets are carried at no more than their recoverable amount, and to def...

Scope
 IAS 36 applies to all assets except: [IAS 36 2]

- inventories (see IAS 2)
- assets arising from construction contracts (see IAS 11)
- deferred tax assets (see IAS 12)
- assets arising from employee benefits (see IAS 19)
- financial assets (see IAS 39)
- investment property carried at fair value (see IAS 40)
- certain agricultural assets carried at fair value (see IAS 41)
- insurance contract assets (see IFRS 4)
- assets held for sale (see IFRS 5)

Therefore, IAS 36 applies to (among other assets):

- land
- buildings
- machinery and equipment
- investment property carried at cost
- intangible assets
- goodwill
- investments in subsidiaries, associates, and joint ventures
- assets carried at revalued amounts under IAS 16 and IAS 38

the three critical attributes of an intangible asset are: [IAS 38 8]

- identifiability
- control (power to obtain benefits from the asset)
- future economic benefits (such as revenues or reduced future costs)

Identifiability: An intangible asset is identifiable when it: [IFRS 38 12]

- is separable (capable of being separated and sold, transferred, license)
- arises from contractual or other legal rights, regardless of whether those and obligations.

Examples of possible intangible assets include:

- computer software
- patents
- copyrights
- motion picture films
- customer lists
- mortgage servicing rights
- licenses
- import quotas
- franchises
- customer and supplier relationships
- marketing rights

Intangibles can be acquired:

- by separate purchase
- as part of a business combination
- by a government grant
- by exchange of assets
- by self-creation (internal generation)

Fig.7.Rezumatul IAS 36
 Sursa: Welch, 2018

Pe baza acestui model, Areopapropus un model al bilanțului aferent capitalului intelectual, care să fie complementar, dar integrat cu cel clasic, așa cum s-a definit peste 400 de ani, un exemplu rafinând în Fig. 8.

		Closing Date		Balance Sheet			
		Assets		Liabilities and Capital			
LIQUIDITY	HIGH	Current Assets:		Current Liabilities:		SHORT	
		Total Current Assets	0.00	Total Current Liabilities	0.00		
		Fixed Assets:		Long-Term Liabilities:			
		Total Fixed Assets	0.00	Total Long-Term Liabilities	0.00		
	LOW	TOTAL ASSETS	0.00	TOTAL LIABILITIES AND CAPITAL	0.00	LONG	
<p>ABC COMPANY</p> <p>Closing Date</p> <p>Intellectual Capital Balance Sheet</p>							
		Intellectual Capital Assets		Intellectual Capital Liabilities and Equity			
STRUCTURED	HIGH	Structural Capital:		Intellectual Capital Liabilities:		LOW	
		Technological Capital	0.00	Tacit Internal Intellectual Capital Assets	0.00		
		Organisational Capital	0.00	Tacit External Intellectual Capital Assets	0.00		
		Total Structural Capital Assets	0.00	Total Intellectual Capital Liabilities	0.00		
	LOW	TOTAL IC ASSETS	0.00	TOTAL IC LIABILITIES AND EQUITY	0.00	HIGH	

Fig. 8 IC Bilanț: Urmează logica structurii BS FINANCIAR
 Sursa: Welch, 2018

Responsabilitatea ar trebui să fie conectată la cunoștințe și economia de rețea, la lumea cibernetică, pentru a face față amenințărilor cibernetice pentru că IC-ul real nu este protejat deloc, proprietatea intelectuală (brevete, drepturi de autor, mărci comerciale etc.) reprezentând doar câteva procente din IC. Cyber- atacurile scapă numai de IC-ul care este capturat, stocat și reutilizat prin computer, cunoștințele explicite, care se prezintă sub formă de date, informații, know-how etc., dar pot ataca și cunoștințele tacite, planurile de dezvoltare, care poate fi găsit în e-mailuri, cercetare și dezvoltare, la dezvoltatori, schimburi strategice de top management etc.

4. Rezolvarea rezilienței

Sabine Lautenschlager, membră a BCE, menționează²⁴ că pentru piața financiară informațiile, cunoștințele și expertiza instituțiilor publice și a industriei vor fi esențiale, deoarece:

-Închiderea interconectării și complexitatea sistemului financiar creează vulnerabilități care pot fi exploatare de cibernetici.

- Atacatorii par să obțină o înțelegere din ce în ce mai profundă a modului în care funcționează sistemul financiar. Acest lucru le permite să detecteze și să exploateze rapid punctele slabe într-un mod mai eficient și ar trebui să fie o preocupare pentru toți.

- Atât băncile, cât și infrastructurile pieței financiare se străduiesc să găsească personal cu abilitățile și experiența necesară pentru a preveni atacurile cibernetice. Lipsa de competențe se extinde mult dincolo de sectorul financiar. Toate părțile interesate relevante trebuie să lucreze urgent la strategii pentru a se asigura că forța de muncă are abilitățile necesare pentru viitoarele noastre economii și că societatea noastră este capabilă să profite de avantajele inovației.

- Adevărata inovație este întotdeauna perturbatoare. Fintech ar putea perturba piețele financiare în moduri pozitive. Dar vine și cu riscuri: o concurență mai violentă ar putea determina unii jucători de pe piață să adopte și să adopte noi tehnologii, servicii sau metode, înainte de a profita din plin de riscurile asociate riscurilor cibernetice în acest caz.

În martie 2017, Consiliul de conducere al FMI a aprobat strategia de rezistență cibernetică a Eurosistemului. De fapt, vorbim despre rezistența acestor imobilizări necorporale, date, informații, cunoștințe, active, identități, know-how. Aceste active au o valoare imensă. Trebuie să putem inventaria, evalua, măsura, apărea în sistemele de contabilitate, astfel încât să le putem asigura.

Conform L. Badea (2019), pentru a identifica riscul, trebuie să evaluăm:

-procese de afaceri relevante pentru riscul cibernetic, cu activele și valorile corespunzătoare ale acestora, trebuie să fie stabilite.

-datele privind punctele slabe trebuie colectate, întotdeauna în legătură cu activele, amenințările și metodele de protecție existente. Un prim indicator potențial de identificare a riscului poate fi asigurat prin autoevaluarea riscului cibernetic. De exemplu, metodele propuse de companiile specializate în distribuirea unei astfel de asigurări²⁵. Aceste instrumente pot ajuta la determinarea expunerii la risc și la conștientizarea riscului companiei și pot oferi indicații pentru riscurile încă neidentificate. Un alt aspect ar fi modul în care un atac de ciberspațiu poate fi detectat cât mai curând posibil din momentul în care

²⁴https://www.ecb.europa.eu/press/key/date/2019/html/ecb.sp190510_1~5803aca48c.en.html

²⁵ <http://www.marsh-stresstest.eu/>

s-a întâmplat. Un instrument pentru analiza consecințelor operațiunilor este desigur Analiza Impactului asupra Afacerilor (BIA).

Evitarea riscurilor ar însemna că stocarea electronică a informațiilor și restricția utilizării sistemelor informatice. În lumea de azi, acest lucru este greu de imaginat. Reducerea riscurilor și atenuarea sunt mai eficiente. Acestea sunt instrumente pentru reducerea probabilității de apariție (de exemplu, software antivirus, firewall etc.) sau care diminuează dimensiunea pierderilor (de exemplu, planuri de recuperare a dezastrelor).

În general, transferul riscului este posibil prin achiziționarea unui contract de asigurare.

Concluzii

Pentru a obține poziționarea corectă a capitalului intelectual al activelor economiei post-cunoaștere, parte a societății cognitive și pentru un spațiu cibernetic mai rezistent, sunt dezvăluite următoarele concluzii:

- Plecăm într-o altă economie, într-o economie a cogniției și ar trebui să o definim corect, incluzând noi instrumente și metodologii.
- Poziționarea stratului uman este esențială pentru o configurare corectă a lumii cibernetice și pentru a acționa împotriva atacurilor anti-cibernetice asupra seturilor de cunoștințe. Înființarea Centrului de excelență în domeniul capitalului intelectual va promova și ține în țară oameni cu cunoștințe, know-how, expertiză.
- Este esențial să formulăm și să ne asumăm politica și să susținem reglementarea riscului cibernetic prin reducerea impactului politic, social și economic²⁶. Aceste politici vor avea efecte benefice atât la nivel de cerere cât și la ofertă.
- Este esențial să se stabilească un nou cadru contabil pentru evaluarea economiei de cunoștințe și rețele. De asemenea, să se stabilească un sistem de raportare a pierderilor generate de infracțiuni informatice și polițe de asigurare de asigurare de forță.
- Este necesar pentru a dezvolta și utiliza modele de evaluare, bazate pe standarde și certificări recunoscute internațional, într-un mod auditiv, bazat pe noi abilități în ingineria riscurilor cibernetice.
- Riscurile cibernetice necesită realizarea unui front comun pentru creșterea nivelului cibernetic și maturității cibernetice, aplicarea principiilor de gestionare a riscurilor și pentru combaterea criminalității informatice.
- Capitalul uman, structural și relațional / client ar trebui reflectat în bilanțuri și calculate sunt cunoștințe activele capitalului intelectual al companiilor.

Bibliografie

- [1] Allianz Global Corporate & Specialty, „Allianz Risk Barometer” 2019
- [2] Brooking A., 1996. *Intellectual Capital: Core Asset for the Third Millennium Enterprise*. New York: International Thomson Business Press.

²⁶ L. Badea, C.M. Rangu, "Ensuring cyber risk - a great challenge facing modern economies", RSF No. 6, May 2019

- [3] Edvinsson Malone Intellectual Capital, Realizing your Company's true Value by finding its hidden Brainpower. New York: Harper Business, 1997P. 17
- [4] F. Stibli, Intellectual capital – the key resource for expanding organisational intelligence, <https://intelligence.sri.ro/capitalul-intelectual-resursa-cheie-pentru-extinderea-inteligentei-organizationale/> [Accessed: May. 10, 2019]
- [5] Human Capital-The Value of People <https://www.oecd.org/insights/humancapital-thevalueofpeople.htm>
- [6] L. Badea, C.M. Rangu, "Ensuring cyber risk – a great challenge facing modern economies", RSF No. 6, May 2019
- [7] Leif Edvinsson Intellectual Capital: Realizing Your Company's True Value by Finding Its Hidden Brainpower Hardcover, 1997
- [8] Lucubrate Peter Welch October 12th, 2018 Magazine article No: 42, October 8th, 2018
- [9] Ludo PYIS, AREOPA GROUP, *IS IT WORTH PROTECTING YOUR INTELLECTUAL CAPITAL FOR CYBER INTRUDERS (PPT presentation), 2013*
- [10] Ludo Pyse, NO CURE, NO PAY? Would applying this rule bring IT projects failure statistics down? ... and how do we measure sure success?, www.areopa.com
- [11] Manfred Bornemann, Karl Franzens University Adolf Knapp, Karl Franzens University, 10 June 1999 HOLISTIC MEASUREMENT OF INTELLECTUAL CAPITAL COUNTRY covered: AUSTRIA RESEARCH
- [12] OECD (2013), "Introduction and Overview", in Supporting Investment in Knowledge Capital, Growth and Innovation, OECD Publishing, <http://dx.doi.org/10.1787/9789264193307-4-en>
- [13] Ten Key Questions on Cyber Risk and Cyber Risk Insurance, Geneva Association, Nov 2016.
- [14] THE POWER OF INTANGIBLES BY GARY COKINS, CPIM, AND NICK SHEPHERD, FCPA, FCGA, FCCA, May 1, 2017, <https://sfmagazine.com/post-entry/may-2017-the-power-of-intangibles/>
- [15] Wissensbilanz , https://www.academy.fraunhofer.de/en/continuing-education/technology-innovation/intellectual_capital_statement.html
- [16] https://ec.europa.eu/research/innovation-union/pdf/KI-01-14-460-EN-N-IP_valuation_Expert_Group.pdf
- [17] <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=11602&no=1>
- [18] <https://magazine.lucubrates.com/intellectual-capital-and-knowledge-management/>
- [19] <http://www.incd2020.ro/sites/default/files//Analiza%20bune%20practici%20int%20rapoarte%20CI.pdf>
- [20] [HTTPS://www.researchgate.net/profile/Selcuk_Burak_Hasiloglu/publication/28263308/figure/fig1/AS:394353668313091@1471032649090/Edvinssons-Categorization-of-Capital-Resource-Leif-Edvinsson-and-M-S-Malone.png](https://www.researchgate.net/profile/Selcuk_Burak_Hasiloglu/publication/28263308/figure/fig1/AS:394353668313091@1471032649090/Edvinssons-Categorization-of-Capital-Resource-Leif-Edvinsson-and-M-S-Malone.png)
- [21] https://asfromania.ro/files/analize/Asigurari_risc_cibernetice.pdf [Accessed May. 09, 2019]
- [22] https://www.ecb.europa.eu/press/key/date/2019/html/ecb.sp190510_1~5803aca48c.en.html
- [23] <http://www.marsh-stresstest.eu/>