Audit financiar, XIV, Nr. 5(137)/**2016**, *505-515*
ISSN: 1583-5812; ISSN on-line: 1844-8801

Considerații privind selectarea şi ierarhizarea soluțiilor de securitate informațională

Maria Cristina RĂDULESCU,
Academia de Studii Economice din Bucureşti,
E-mail: maria.radulescu@cig.ase.ro

Rezumat

Lucrarea propune un set de repere utile pentru a prescrie o metodologie sau un proces detaliat pentru selectarea sau ierarhizarea proiectelor şi soluțiilor de securitate. Pornind de la ideea că nivelul costurilor unei soluții trebuie justificat prin prisma contribuției la asigurarea unei protecții adecvate pentru resursele informaționale ale organizației care o implementează. Articolul abordează problematica generală a riscurilor şi costurilor privind securitatea, argumentând necesitatea raportării explicite la obiectivele de securitate asociate resurselor informaționale, pentru validarea deciziilor de implementare a proiectelor de securitate. Într-o astfel de abordare, exigențele de securitate asociate resurselor informaționale se constituie într-un sistem de referință pentru cuantificarea beneficiilor şi limitelor soluțiilor definite ca răspunsuri alternative sau complementare la anumite riscuri de securitate şi a căror implementare este supusă restricțiilor de buget.

Cuvinte-cheie: *Securitate informațională; soluție de securitate; resursă informațională; risc de securitate; eficiență.*

Clasificare JEL: *M15, O33, M40, D81*

Vă rugăm să citați acest articol astfel:
Rădulescu, M.C. (2016), Considerations on the selection and prioritization of information security solutions, Audit Financiar, vol. XIV, no. 5(137)/2016, pp. 564-574, DOI: 10.20869/AUDITF/2016/137/564

Link permanent pentru acest document:
http://dx.doi.org/10.20869/AUDITF/2016/137/564

1. Introducere

În condițiile în care eficiența este un factor-cheie în procesele decizionale, iar obiectivul securizării corespunzătoare a sistemelor informaționale trebuie permanent conciliat cu restricțiile de buget, este necesar ca fiecare model de securitate să urmărească maximizarea beneficiilor concomitent cu minimizarea costurilor asociate (Scholtz, 2011). Posibilitățile de fundamentare economică a politicilor de securitate sunt investigate în diverse materiale ce recurg la repere şi tehnici de tip cantitativ (Böhme, 2010; Gordon şi Loeb, 2002; Gordon şi Loeb, 2005; Pontes ş.a., 2011), însă majoritatea modelelor vizează sistemul informațional în ansamblu, fără a ține seama de complexitatea sa structurală, care determină riscuri şi cerințe de securitate diverse.

În mod frecvent, identificarea şi analiza riscurilor de securitate are ca punct de start aplicațiile şi echipamentele ce asigură suportul proceselor de afaceri, soluțiile de securitate având o determinare preponderent tehnică şi fiind concepute pentru un segment bine delimitat al infrastructurii informaționale a unei organizații. Raportate la diversitatea tipologică a informației de afaceri care face obiectul protecției, soluțiile de securitate reprezintă structuri compozite, care vizează multiple categorii de date, cu exigențe de securitate distincte.

Lucrarea de față defineşte atât eficiența, cât şi limitele soluțiilor de securitate, din perspectiva efectului de protecție pe care acestea îl exercită asupra resurselor informaționale ale unei organizații. Pornind de la ideea că soluțiile de securitate nu constituie scopuri în sine, ci mijloace prin care trebuie să se asigure un nivel de protecție adecvat resurselor informaționale, lucrarea îşi propune furnizarea unui set de repere pentru validarea deciziilor de implementare a soluțiilor de securitate dintr-o perspectivă complementară celei economico-financiare şi indicatorilor asociați (pierderile anuale aşteptate, rata rentabilității, valoarea actualizată netă a investițiilor etc.).

2. Metodologia cercetării

Articolul este rezultatul unei cercetări de tip calitativ, care a avut ca scop definirea unui set de repere pentru analiza şi compararea soluțiilor de securitate prin prisma impactului asupra sistemului informațional al unei organizații. Cercetarea are la bază un studiu extins al literaturii ce tratează problematica riscurilor de securitate şi a eficienței soluțiilor de contracarare a acestora, care a permis argumentarea relevanței şi utilității abordării propuse în lucrarea de față. Demersul teoretic vizează următoarele aspecte: delimitarea conceptuală a resurselor informaționale şi a soluțiilor de securitate ca elemente-cheie ale modelului de analiză, adaptarea reperelor furnizate de managementul riscurilor pentru definirea unui sistem de evaluare a impactului soluțiilor de securitate, identificarea corelațiilor conceptuale care permit cuantificarea acestui impact. Rezultatele prezentei cercetări pot fi integrate într-un model formal de asistare a deciziei de investiții privind securitatea informațională. O astfel de abordare facilitează extinderea cercetării printr-un demers de tip cantitativ, pentru analiza datelor privind soluțiile de securitate de la nivelul sistemelor organizaționale reale.

3. Costurile şi beneficiile securității informaționale

Într-o abordare completă, securitatea informațională vizează atât datele gestionate cu mijloace informatice, cât şi pe cele disponibile în format non-digital, securitatea fiind în prezent percepută ca domeniu de graniță, care transcende procesele şi subdomeniile organizaționale. Necesitatea gestionării acestei complexități, sub aspect tehnic şi organizațional, a condus la standarde precum ISO27k *Information Security* (ISO – International Organization for Standardization) şi NIST SP800 *Computer Security* (NIST – National Institute of Standards and Technology) sau la modele de referință şi coduri de bune practici, precum COBIT – Control Objectives for Information and Related Technology sau ITIL – Information Technology Infrastructure Library. Securitatea informațională face şi obiectul anumitor norme şi reglementări sau este influențată de acestea; referințe frecvent menționate în literatură sunt acordurile Basel II şi III, pentru domeniul bancar, sau legea Sarbanes-Oxley, în SUA. Astfel de reglementări sau aderarea la anumite standarde influențează strategia şi politicile de securitate ale unei companii şi, inevitabil, nivelul investițiilor asociate. Impactul reglementărilor care vizează securitatea este analizat de Lee ş.a. (2016), pe baza unor scenarii privind desfăşurarea paralelă sau secvențială a controalelor de securitate normate şi a celor decise la nivel organizațional.

Faptul că securitatea constituie o dimensiune distinctă a managementului organizațional este confirmat de PricewaterhouseCoopers – PwC (2015) printr-un studiu amplu (10.000 de decidenți, din 127 de state) care arată că 58% dintre organizații dispun de strategii de securitate. În pofida creşterii cu 38% a numărului incidentelor de securitate comparativ cu anul 2014, PwC (2015) constată diminuarea cu 5% a pierderilor financiare cauzate de acestea, o astfel de evoluție atestând utilitatea strategiilor de securitate informațională. Pe de altă parte, în condițiile în care 24% dintre companii au raportat creşteri ale bugetului alocat securității, se ridică problema eficienței strategiilor. Importanța acestui aspect este subliniată de un alt studiu realizat la nivel global de Ernst&Young – EY (2015), care a indicat restricțiile de buget drept principal obstacol (pentru 67% dintre companii) pentru un nivel adecvat al securității informaționale. În condițiile unui buget în mod invariabil limitat, apare necesitatea optimizării modelului de securitate prin considerarea beneficiilor obținute şi potențiale, raportate la costurile asociate (Scholtz, 2011).

Managementul riscurilor este indispensabil pentru alocarea unui buget corespunzător securității informaționale. În primul rând, se ridică întrebarea „Cât de mult este într-adevăr suficient?" (Hoo, 2002), după care se pune problema unei repartizări adecvate a bugetului pe destinații care corespund controalelor definite în contextul managementului riscurilor. O repartizare judicioasă impune estimarea realistă a costurilor incidentelor de securitate, inclusiv a prejudiciilor indirecte cauzate de indisponibilitatea sistemelor informatice. De asemenea, trebuie avute în vedere toate tipurile de răspunsuri la riscurile de securitate. Spre exemplu, Zhao ş.a. (2009) compară opțiunile de transfer al riscurilor, *outsourcing*-ul fiind prezentat drept o alternativă mai avantajoasă la soluțiile oferite de sistemul de asigurări; pe de altă parte, *outsourcing*-ul IT ridică problema unor costuri ascunse (Barthélemy, 2001), identificarea şi estimarea acestora fiind esențiale pentru o fundamentare corectă a deciziei de *outsourcing*.

Managementul riscurilor de securitate nu se limitează la infrastructura informatică a unei organizații; spre exemplu, Goettelmann ş.a. (2014) propune un model de analiză a riscurilor asociate proceselor de afaceri care au suportul soluțiilor de tip *cloud-computing*. În NIST (2012) managementul riscurilor de securitate este abordat stratificat: la nivel tehnic, al proceselor de afaceri şi la nivel strategic; acestea corespund unor planuri de identificare şi analiză a riscurilor, dar şi unor niveluri decizionale care vizează măsurile de contracarare a riscurilor. Tratată de regulă în plan operațional şi tehnic, problema riscurilor de securitate este mai puțin abordată din perspectiva deciziilor strategice privind politicile de securitate şi susținerea lor financiară. Spre exemplu, în Gordon şi Loeb (2006) sau Hamill ş.a. (2005) bugetele se prezumă a fi cunoscute; o abordare diferită propun Anderson şi Choobineh (2008), care tratează în mod explicit problema dimensionării bugetului securității informaționale. La nivel strategic sunt puse în balanță riscurile de securitate şi costurile asociate, inclusiv cele de oportunitate (Gordon şi Loeb, 2006), bugetul alocat securității depinzând, în mod esențial, de percepția pe care decidenții o au asupra riscurilor, respectiv de toleranța la risc. Aceasta poate să difere considerabil de la organizație la alta şi, pentru aceeaşi organizație, de la o perioadă la alta, în funcție de obiectivele companiei şi contextul economic; în această cheie poate fi interpretată şi abordarea propusă de Gordon ş.a. (2003) – amânarea unor investiții costisitoare până la producerea primului incident de securitate care justifică o reacție concretă.

Posibilitățile de fundamentare economică a politicilor de securitate sunt investigate prin recurgerea la modele, tehnici şi repere de tip cantitativ. De exemplu, Böhme (2010) tratează relația dintre valorile indicatorilor de securitate şi modelele de investiții, iar Gordon şi Loeb (2002) prezintă un model economic pentru determinarea unui nivel optim al investițiilor privind securitatea informațională. În mod uzual, eficiența investițiilor este apreciată pe baza analizelor de tip cost-beneficiu, ceea ce implică estimări ale pierderilor evitate prin realizarea respectivelor investiții. Gordon şi Loeb (2005) furnizează un ghid de aplicare a analizei cost-beneficiu în contextul securității IT; sunt vizate direcționarea şi dimensionarea corespunzătoare a investițiilor, dar şi aspecte complementare, precum strategiile de minimizare a impactului incidentelor de securitate sau relația dintre riscuri şi resursele alocate securității. De asemenea, Pontes ş.a. (2011) abordează rentabilitatea investițiilor în securitate prin raportarea la managementul riscurilor de acest tip.

Brecht şi Nowey (2012) realizează o analiză detaliată a problematicii costurilor şi investițiilor privind securitatea informațională şi a indicatorilor asociați, comparând

contribuțiile semnificative din literatura de specialitate. O problemă a majorității modelelor este percepția de tip „cutie neagră" asupra sistemului informațional şi ignorarea complexității sale structurale, care determină riscuri şi exigențe de securitate diverse. Pe termen scurt, un astfel de tratament permite reducerea costurilor cu analiza şi clasificarea datelor sub aspectul exigențelor de securitate, respectiv cu adaptarea corespunzătoare a politicilor de securitate. Pe termen lung însă, opacitatea modelului de securitate poate conduce la bugete inadecvate sau repartizate necorespunzător, supradimensionarea anumitor alocări şi subdimensionarea altora favorizând incidente de securitate a căror soluționare implică noi costuri. O abordare mai nuanțată este oferită de Gordon şi Loeb (2002), care propun un model economic pentru determinarea nivelului optim al investițiilor pentru securizarea datelor sub aspectul integrității, confidențialității, disponibilității, autenticității şi non-repudierii; în acest scop, se recurge la o versiune ajustată a modelului de calcul al pierderilor anuale aşteptate, adaptat situațiilor în care cel mult una dintre tentativele de subminare a obiectivelor de securitate va avea succes. Exigențele de securitate asociate resurselor informaționale ale unei organizații sunt vizate în mod explicit şi în articolul de față, fiind tratate drept sistem de referință uniform şi stabil, pentru cuantificarea beneficiilor şi limitelor oricărui proiect de securitate, independent de aspectele financiare, anvergura operațională sau orizontul său de timp.

4. Resursele informaționale din perspectiva securității

Deşi obiectivele de securitate pot fi aplicate, în funcție de context, datelor propriu-zise şi aplicațiilor care asigură prelucrarea şi gestionarea acestora, lucrarea de față adoptă o perspectivă mai largă şi se poziționează la un nivel de abstractizare relevant pentru logica de afaceri. Resursele informaționale sunt percepute ca entități conceptuale stabile, care transcend atât aplicațiile, cât şi procesele de afaceri; cu alte cuvinte, este vizată informația de afaceri, respectiv reperele tipologice şi de clasificare ce pot fi utilizate pentru structurarea acesteia, inclusiv sub aspectul obiectivelor de securitate asociate.

Rezultatul abstractizării entităților cu proprietăți comune se prezintă sub forma unor tipuri generice, care permit tratarea întregului sistem informațional al unei organizații la nivel pur conceptual, în optica specifică bine-cunoscutului model *Entitate-Asociere*, propus de Chen (1976). Cel mai frecvent însă, un astfel de model se plasează la un nivel de detaliu inadecvat analizei şi tratamentului riscurilor de securitate, impunându-se regrupări ale entităților la nivelul unor categorii relevante din perspectiva securității informaționale. Spre exemplu, contractele, clienții şi încasările pot fi alocate categoriei *Desfaceri*; ca alternativă, se poate opta pentru definirea unei categorii unice care să includă atât furnizorii, cât şi clienții şi operațiunile asociate; într-o altă abordare, contractele aferente partenerilor companiei pot fi plasate într-o categorie distinctă de cea a operațiunilor financiare asociate. Resursele informaționale pot să difere considerabil sub aspectul importanței strategice şi operaționale, la care se pot adăuga şi alte criterii de diferențiere, precum gradul de actualitate sau regimul impus de diferite reglementări (durata minimă de păstrare, condițiile în care acestea pot fi distruse etc.). Prin urmare, analiza şi clasificarea datelor din perspectiva importanței pe care o prezintă pentru organizație este un pas obligatoriu pentru identificarea resurselor informaționale critice şi a riscurilor de securitate asociate.

Deşi informațiile din aceeaşi categorie pot face obiectul unor scenarii ce implică utilizatori multipli şi diverse aplicații sau medii de exploatare, cu exigențe distincte în planul securității, abordarea informației de afaceri în mod sistematic şi coerent, în contextul managementului riscurilor, permite stabilirea unui prag minimal al cerințelor de securitate care să fie adecvat tuturor scenariilor impuse de logica de afaceri. Definirea tipologiei resurselor informaționale impune analize detaliate ale sistemului informațional, pentru fiecare dintre categoriile identificate specificându-se procesele, aplicațiile şi tipologia utilizatorilor, cu prerogativele şi restricțiile de securitate asociate.

Nivelul de protecție adecvat fiecărei categorii informaționale este expresia agregată a exigențelor de securitate care vizează un set particular de cerințe şi obiective. Chiar dacă natura acestora este influențată de aplicarea unor standarde ca ISO27k sau de aderarea la anumite platforme de control şi guvernanță IT, precum ISACA-COBIT, uzual se recurge la tripleta confidențialitate-integritate-disponibilitate; aceasta poate fi completată de criterii suplimentare, ca non-repudierea, autenticitatea, reziliența etc. Chiar şi în condițiile în care pentru fiecare obiectiv de securitate se aplică aceeaşi

scală descriptiv-cantitativă, este posibil ca exigențele de securitate asociate unei categorii de resurse informaționale să fie semnificativ diferite, în funcție de criteriul considerat. De exemplu, Oberlaender (2011) trece în revistă o serie de scenarii care reclamă niveluri diferite ale cerințelor specifice privind securizarea informației de afaceri.

Deşi problematica modelării informației de afaceri depăşeşte cadrul acestui material, s-a urmărit o delimitare conceptuală adecvată a resurselor informaționale, ca elemente esențiale pentru analiza soluțiilor de securitate.

5. Analiza soluțiilor de securitate prin raportarea la resursele informaționale

În cele ce urmează vor fi prezentate elementele generale ale unui model de analiză a proiectelor sau a soluțiilor de securitate, prin raportarea la exigențele de protecție asociate resurselor informaționale. Un astfel de model permite fundamentarea deciziilor de selectare sau ierarhizare a soluțiilor definite ca răspunsuri alternative sau complementare la anumite riscuri de securitate, în condițiile în care implementarea lor este supusă restricțiilor de buget. Ca atare, setul soluțiilor de securitate şi costurile aferente se prezumă cunoscute, devenind inputuri ale modelului de analiză. În plus, întrucât nivelul riscurilor este criteriul prioritar în raport cu care se apreciază necesitatea tratamentelor pentru contracararea acestora, comparația se limitează la soluțiile definite ca răspunsuri particulare la riscurile de un anumit nivel, evaluat în prealabil prin demersuri specifice managementului riscurilor.

5.1. Inventarierea soluțiilor de securitate supuse analizei

În contextul lucrării de față, sintagma *soluție de securitate* desemnează un set de elemente de natură tehnică şi organizațională, menite să limiteze riscurile privind securitatea informațională. În funcție de complexitatea sa, fiecare soluție de securitate permite implementarea unor controale şi mecanisme de securitate ce acționează pe unul sau mai multe planuri:

- *Logic*: autentificare şi autorizare a accesului la aplicații, monitorizare, audit, *backup*, criptare, antivirus, *firewall* etc.;
- *Fizic*: securizarea unui anumit perimetru fizic, gestiune echipamente etc.;
- Operațional-administrativ: training, screening angajați, proceduri de lucru, help-desk etc.

O astfel de abordare a soluțiilor de securitate are o dublă argumentare:

- Raportarea la managementul riscurilor determină complementaritatea şi interdependența măsurilor şi controalelor privind securitatea;
- Limitările de ordin financiar impun selectarea controalelor de securitate şi ordonarea investițiilor după criteriul eficienței.

Potrivit enunțurilor de mai sus, fiecărei soluții de securitate îi va corespunde un anumit decupaj de elemente tehnice şi operaționale considerat relevant pentru managementul riscurilor. Soluțiile de securitate pot fi definite la diferite niveluri de granularitate, cu condiția să fie implementabile de sine stătător şi să poată face obiectul analizelor cost-beneficiu; cu alte cuvinte, o anumită soluție poate fi concepută drept versiunea mai simplă a alteia, diferența de granularitate având consecințe directe în planul costurilor. Din perspectiva unui buget limitat, costurile asociate unui set predefinit de soluții de securitate sunt, în diferite proporții, aditive şi totodată exclusive; se impune deci identificarea combinației de soluții ce permite furnizarea unui răspuns optim la riscurile de securitate, cu respectarea restricției de buget.

De la caz la caz, soluțiile de securitate pot viza un set mai amplu sau mai restrâns al resurselor informaționale, după cum aceleaşi resurse pot face obiectul mai multor soluții de securitate. Pe de altă parte, cerințele de securitate ale resurselor sunt independente de soluțiile supuse analizei, fiind determinate de natura intrinsecă a informației de afaceri şi de importanța pe care aceasta o prezintă pentru organizație. Drept urmare, pentru a cuantifica impactul global al unei soluții de securitate este necesar să se evalueze aportul său la atingerea nivelului de protecție predefinit ca optim pentru fiecare criteriu de securitate asociat resurselor informaționale pe care le vizează.

Chiar dacă prezintă cerințe de securitate identice, resursele informaționale pot fi semnificativ diferite sub aspectul importanței operaționale sau strategice, criteriul importanței relative a fiecărei categorii informaționale fiind esențial pentru aprecierea în termeni cantitativi a obiectivelor de securitate şi a aportului soluțiilor de securitate la atingerea lor. Într-o abordare mai pragmatică, ce permite simplificarea acestor evaluări,

sistemul de corespondențe soluții-resurse poate fi definit pe baza subsetului resurselor informaționale apreciate drept critice, prin prisma efectelor unor potențiale incidente de securitate. Dintr-o astfel de perspectivă au fost exemplificate şi corespondențele generice din **Tabelul 1**, limitate la ansamblul ipotetic al resurselor critice vizate de soluțiile de securitate.

5.2. Cuantificarea impactului soluțiilor de securitate

Întrucât obiectivelor de securitate trebuie să le corespundă criterii clare pentru specificarea fiecărui nivel al exigențelor de securitate asociate resurselor informaționale, în cazul celor din urmă se poate discuta despre un anumit nivel de conformitate, respectiv de neconformitate cu cerințele de securitate predefinite; spre exemplu, NIST (2005) recurge la un indicator de neconformitate ce vizează sistemul informațional în ansamblul său. Lucrarea de față propune o abordare mai nuanțată, prin izolarea exigențelor de securitate ale resurselor informaționale. Astfel, un nivel de protecție superior celui predefinit ca adecvat nu este considerat necesar şi nici posibil, fără a antrena costuri suplimentare disproporționate în raport cu beneficiile aşteptate.

Conformitatea cu cerințele de securitate nu reprezintă un obiectiv absolut, ci se evaluează prin raportarea la nivelul considerat optim în cazul fiecărui criteriu de securitate. Ca atare, eficacitatea unei soluții de securitate poate fi percepută drept un indicator agregat al valorilor individuale, ce atestă gradul în care aceasta permite creşterea conformității cu obiectivele de securitate asociate resurselor informaționale pentru care prezintă interes. În cazul fiecărei soluții, raportarea la nivelul de exigență predefinit ca optim (100%) pentru un anumit obiectiv de securitate conduce la următoarele repere cantitative:

- *Neconformitatea anterioară implementării soluției de securitate (NA)*
- *Neconformitatea ulterioară implementării soluției de securitate (NU)*

Tabelul 1. Exemplificarea sistemului de corespondențe soluții securitate - resurse informaționale

Soluții/ Resurse		Confidențialitate			Integritate			Disponibilitate		
		Scăzută	Medie	Ridicată	Scăzută	Medie	Ridicată	Scăzută	Medie	Ridicată
S1	R1		NA = 0,50 NU = 0,30 P = 0,20			NA = 0,70 NU = 0,50 P = 0,20				NA = 0,50 NU = (-0,25) P = 0,50 | SP = 0,25
	R2			NA = 0,75 NU = 0,50 P = 0,25		NA = 0,00 NU = (-0,50) P = 0,00 | SP = 0,50			NA = 0,50 NU = 0,00 P = 0,50	
S2	R2			NA = 0,75 NU = 0,00 P = 0,75		NA = 0,00 NU = 0,00 P = 0,00			NA = 0,50 NU = 0,50 P = 0,00	
S3	R1		NA = 0,50 NU = (-0,20) P = 0,50 | SP = 0,20			NA = 0,70 NU = 0,70 P = 0,00				NA = 0,50 NU = 0,30 P = 0,20
	R2			NA = 0,75 NU = 0,50 P = 0,25		NA = 0,00 NU = 0,00 P = 0,00			NA = 0,50 NU = 0,50 P = 0,00	
	R3	NA = 0,20 NU = 0,20 P = 0,00			NA = 0,00 NU = 0,00 P = 0,00					NA = 0,50 NU = 0,25 P = 0,25
S4	R1		NA = 0,50 NU = 0,5 P = 0,00			NA = 0,70 NU = 0,70 P = 0,00				NA = 0,50 NU = (-0,15) P = 0,50 | SP = 0,15
	R2			NA = 0,75 NU = 0,75 P = 0,00		NA = 0,00 NU = 0,00 P = 0,00			NA = 0,50 NU = 0,25 P = 0,25	

NA = Neconformitatea Anterioară (neconformitatea anterioară implementării soluției de securitate)
NU = Neconformitatea Ulterioară (neconformitatea ulterioară implementării soluției de securitate)
P = Efect de protecție SP = Efect de supraprotecție
Sursa: Prelucrările autorului

Neconformitatea anterioară este evaluată pe baza stării curente a sistemului informațional, în timp ce neconformitatea ulterioară corespunde unei potențiale stări viitoare, tranziția către aceasta fiind condiționată de implementarea unei anumite soluții de securitate. Dificultățile inerente evaluărilor privind nivelul de neconformitate trebuie gestionate în contextul managementului riscurilor de securitate; spre exemplu, trebuie apreciată posibilitatea de apariție a incidentelor de securitate şi de neutralizare a consecințelor acestora. Astfel de estimări implică statistici şi repere de ordin cantitativ, dar şi raționamentul profesional al experților în securitatea IT, managementul riscurilor şi audit intern. Limitele modelelor cantitative în scenariile complexe, în care rolul experților este determinant, sunt analizate de Devos ş.a. (2013). Acuratețea cuantificării nivelului de neconformitate este condiționată de un sistem coerent de management al riscurilor de securitate, care permite monitorizarea soluțiilor ce fac obiectul implementării şi evaluarea rezultatelor, preluate apoi ca inputuri într-un nou ciclu de gestiune a riscurilor.

Deşi creşterea neconformității în urma aplicării unei soluții de securitate (*NU* > *NA*) este, în general, neverosimilă, o excepție o constituie situațiile în care se urmăreşte înlocuirea unei soluții preexistente, care din perspectiva anumitor obiective de securitate se dovedeşte superioară unei potențiale soluții de substituție, care face obiectul evaluării. Scenariul uzual este însă acela în care soluțiile supuse analizei permit rezolvarea parțială sau, în mod ideal, integrală, a problemelor de conformitate cu cerințele de securitate asociate resurselor informaționale. Pe de altă parte, o analiză detaliată, care opune fiecărei soluții de securitate ansamblul resurselor informaționale pe care trebuie să le protejeze, poate evidenția şi soluții cu impact parțial nul (vizează un subset al obiectivelor de securitate, fără nicio contribuție la reducerea neconformității constatate în cazul celorlalte) sau soluții care asigură satisfacerea anumitor cerințe de securitate la un nivel superior celui predefinit ca adecvat pentru resursele considerate.

Valoarea negativă a neconformității ulterioare aplicării unei soluții de securitate (*NU* < *0*) indică supra-conformitatea cu obiectivele de securitate. Un astfel de impact trebuie deosebit de cel care permite atingerea nivelului de conformitate prestabilit ca optim, întrucât corespunde investițiilor supradimensionate sau controalelor excesive în raport cu beneficiile concrete în planul securității. Ca atare, cuantificarea impactului unei soluții de securitate se va realiza în mod distinct pentru cele două tipuri de efecte pe care aceasta le poate produce:

- Protecție, respectiv eliminarea neconformității sau reducerea ei parțială:

  Efect de protecție (P) = Neconformitatea ulterioară – Neconformitatea anterioară

- Supra-protecție, respectiv eliminarea neconformității şi asigurarea unei protecții suplimentare în raport cu pragul de conformitate definit ca optim din perspectiva exigențelor de securitate ale resurselor informaționale:

  Efect de protecție (P) = Neconformitatea anterioară

  Efect de supra-protecție (SP) = (- Neconformitatea ulterioară)

5.3. Impactul global al soluțiilor de securitate

În condițiile în care o soluție de securitate vizează resurse informaționale multiple, impactul său global va fi calculat ca medie a valorilor care cuantifică efectul respectivei soluții prin prisma exigențelor de securitate individuale ale resurselor ce-i corespund. În prealabil, mulțimea acestor valori trebuie separată în două subseturi de date, în funcție de natura efectului; distingem, deci, efectul mediu de protecție şi, dacă este cazul, pe cel de supra-protecție. Efectul mediu de protecție constituie o măsură a eficacității unei soluții de securitate, sub aspectul contribuției la securizarea corespunzătoare a resurselor informaționale. Pe de altă parte, un nivel mai ridicat sau mai redus al efectului mediu de supra-protecție este de aşteptat să genereze costuri fără acoperire din perspectiva necesităților reale de securizare a resurselor informaționale.

Identificarea şi cuantificarea efectului de supra-protecție atribuit soluțiilor de securitate sunt ghidate de ideea că doar un nivel de protecție apreciat ca necesar are justificare în planul costurilor. Pe de altă parte, în condițiile în care soluțiile de securitate vizează, în mod colectiv, mai multe categorii de resurse informaționale, asigurarea unui nivel de protecție adecvat anumitor resurse poate determina supra-protecția altora, fără ca aceasta să antreneze o creştere a costurilor de implementare a soluțiilor de securitate. O corespondență directă şi imediată între efectul de supra-protecție şi nivelul costurilor poate fi dificil sau chiar imposibil de stabilit,

având în vedere perspectivele şi reperele diferite utilizate pentru cuantificarea acestora: exigenţele de securitate ale resurselor informaţionale, respectiv valoarea economică a activelor şi serviciilor necesare pentru securizarea resurselor. În aceste condiţii, determinarea aritmetică a unei fracţiuni din cost care este imputabilă supra-protecţiei nu are nicio justificare economică, efectul de supra-protecţie fiind doar o premisă, nu şi o certitudine privind creşterea costurilor unei soluţii de securitate. Drept consecinţă, efectul de supra-protecţie nu va influenţa tratamentul costurilor, ca inputuri necesare pentru evaluarea eficienţei soluţiilor de securitate.

Tabelul 2. Repere cantitative asociate soluţiilor de securitate exemplificate

Soluţie	Nivel costuri	Efect mediu protecţie	Efect mediu supraprotecţie	Eficienţă costuri	Neconformitate ulterioară medie
S1	15.000	0,275	0,375	0,183	0,217
S2	5.000	0,250	0,500	0,500	0,167
S3	35.000	0,133	0,038	0,038	0,272
S4	17.500	0,125	0,150	0,071	0,367

Sursa: Prelucrările autorului

5.4. Eficienţa soluţiilor de securitate

Subiectul eficienţei soluţiilor de securitate este tratat pe larg în diverse materiale care analizează indicatorii specifici şi problemele pe care le ridică determinarea acestora - spre exemplu, Pontes ş.a. (2011). Făcând abstracţie de alte elemente de ordin economic şi financiar (valoarea echipamentelor şi aplicaţiilor care fac obiectul protecţiei, evoluţia estimată a productivităţii muncii sau a rezultatelor financiare etc.), NIST (2005) recurge la un indicator de eficienţă exprimat ca raport între nivelul neconformităţii cu obiectivele de securitate şi costurile proiectelor de securitate. Premisa unei astfel de abordări este aceea că soluţiile de securitate îşi vor atinge scopul, respectiv eliminarea neconformităţii; cu cât nivelul acesteia este mai ridicat şi al costurilor mai scăzut, cu atât este mai eficientă soluţia de securitate.

Deşi lucrarea de faţă tratează eficienţa soluţiilor de securitate în manieră similară („unităţi" de efect la o „unitate" de cost), considerarea explicită a exigenţelor de securitate ale resurselor informaţionale favorizează creşterea relevanţei indicatorilor. Cu alte cuvinte, pentru o acoperire cât mai bună a riscurilor, în condiţiile unui buget limitat, costurile fiecărei soluţii de securitate trebuie justificate prin prisma utilităţii sale reale, considerându-se efectul aşteptat şi necesar şi făcându-se abstracţie de un eventual efect de supra-protecţie a resurselor. Eficienţa unei soluţii de securitate va fi deci exprimată ca raport între efectul mediu de protecţie şi costurile pe care aceasta le generează. Întrucât ridică problema ordinului de mărime a costurilor, indicatorii de eficienţă sunt relevanţi doar în măsura în care soluţiile de securitate analizate prezintă niveluri comparabile ale costurilor de implementare. Acest scenariu trebuie însă considerat ca implicit, proiectele şi soluţiile cu impact semnificativ diferit la nivelul sistemului informaţional punând sub semnul întrebării relevanţa comparaţiilor şi utilitatea întregului demers de analiză. Indicatorii de eficienţă ai soluţiilor generice folosite pentru exemplificare sunt disponibili în **Tabelul 2**; pentru a simplifica utilizarea lor, valorile reale au fost multiplicate cu 10.000.

5.5. Selectarea şi clasificarea soluţiilor de securitate

Deşi eficienţa poate constitui un criteriu de selecţie a proiectelor de securitate, acest indicator ia în considerare doar impactul pozitiv al soluţiilor analizate, nu şi limitele lor în raport cu exigenţele de securitate ale resurselor pe care le protejează. Măsura în care o soluţie şi-a atins scopul este expresia agregată a valorilor neconformităţii rezultate în urma aplicării sale (*NU*), fiind cuantificată ca medie a acestora. Pentru soluţiile generice considerate pentru exemplificare, indicatorii neconformităţii medii ulterioare implementării sunt prezentaţi în **Tabelul 2**.

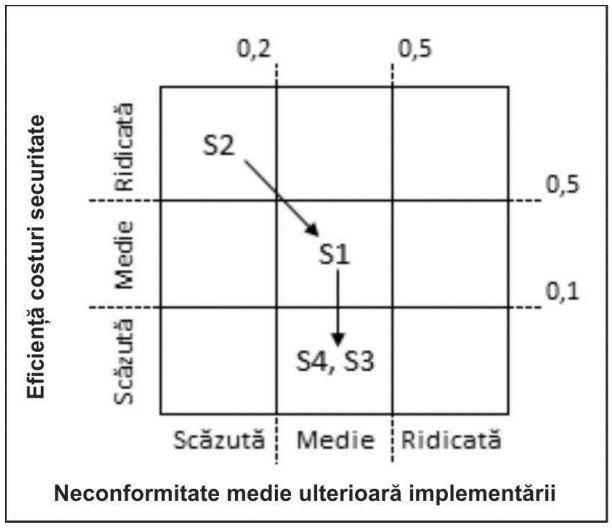
Un tratament particular se impune situaţiilor care corespund supra-protecţiei resurselor informaţionale. Deşi aceasta poate constitui premisa unei creşteri de costuri fără acoperire în planul necesităţilor reale de protecţie a resurselor, rămâne certitudinea faptului că

nivelul de protecție obținut permite eliminarea integrală a neconformității anterioare implementării soluțiilor de securitate. Drept urmare, la determinarea neconformității medii ulterioare implementării unei soluții, valoarea 0 va fi utilizată ca input pentru fiecare situație de supra-protecție a resurselor.

În absența unei corelații conceptuale care să conducă la un indicator relevant ce implică ambele criterii, eficiența şi neconformitatea ulterioară medie vor fi combinate pe baza unei matrice care permite delimitarea unor contexte generice pentru calificarea soluțiilor de securitate drept mai mult sau mai puțin avantajoase, prin raportarea la anumite combinații de valori. În **Figura 1**, pentru fiecare criteriu s-a apelat la categoriile descriptiv-cantitative uzuale în managementul riscurilor (scăzut, mediu, ridicat); scalele valorice la care se raportează acestea sunt definite prin prisma toleranței la risc, fiind independente de soluțiile de securitate ce fac obiectul analizei. Evident, vor fi preferate soluțiile care se plasează în secțiunea alocată eficienței ridicate şi neconformității scăzute sau în imediata proximitate a acesteia. Demersul concret de selectare a uneia sau a mai multor soluții ridică însă o serie de probleme, care se pliază pe următoarele scenarii:

- *Mai multe soluții de securitate poziționate în aceeaşi secțiune a matricei*. Eficiența, neconformitatea ulterioară implementării, nivelul costurilor sau efectul mediu de supra-protecție pot fi utilizate drept criterii de departajare, într-o ordine prestabilită, care depinde de importanța acordată acestora. Spre exemplu, în absența unor limitări foarte stricte legate de buget, este justificat să primeze neconformitatea, din cauza riscurilor de securitate pe care le comportă.
- *Soluții de securitate non-exclusive, care se pot implementa în paralel, cu respectarea restricției de buget*. Pornind de la extremitatea care corespunde combinației optime şi, dacă este cazul, continuând cu celulele adiacente, trebuie determinată combinația de soluții care permite respectarea limitei de buget.
- *Soluții de securitate non-exclusive, care se aplică secvențial*. În acest caz se presupune că toate soluțiile urmează să fie implementate, dar nu simultan; prin urmare, se va da prioritate celor mai avantajoase soluții, din perspectiva efectelor produse. Ierarhizarea debutează în extremitatea care corespunde combinației optime, însă direcția în care se avansează depinde de importanța acordată criteriilor ce exprimă efectele soluțiilor de securitate (eficiența cât mai ridicată sau neconformitatea ulterioară cât mai scăzută).

Figura 1. Matricea utilizată pentru selectarea şi ierarhizarea soluțiilor analizate



Sursa: Prelucrările autorului

În situația în care vizează un set comun de resurse, soluțiile de securitate non-exclusive ridică problema consistenței reperelor de analiză. Astfel, abordarea problemelor de conformitate cu cerințele de securitate ale resurselor informaționale în mod distinct, pentru fiecare soluție care face obiectul analizei, nu permite identificarea unei eventuale supra-conformități rezultată prin cumularea efectelor de protecție asociate fiecărei soluții de securitate selectate spre implementare. În varianta unei abordări integrate, în care post-condițiile implementării unei soluții devin pre-condiții pentru următoarea, nivelul neconformității anterioare în raport cu exigențele de securitate ale resurselor vizate de mai multe soluții de securitate nu este identic pentru fiecare dintre acestea şi nu rămâne cel estimat inițial, fiind actualizat după fiecare operație de selectare a unei soluții, cu respectarea criteriilor de clasificare descrise mai sus. Selectarea unei anumite soluții în vederea implementării determină refacerea machetei de corespondențe soluții - resurse prin restrângerea setului de soluții analizate şi reconsiderarea neconformității

anterioare pentru resursele partajabile (este preluată valoarea estimată a neconformității ulterioare aplicării soluției selectate). În pofida complexității, o astfel de abordare este mai adecvată scenariilor de implementare reale, permițând expunerea unor efecte de supra-protecție a resurselor informaționale şi, implicit, a riscului unor costuri nejustificate, ce nu pot fi sesizate şi estimate ignorând dimensiunea dinamică pe care logica ierarhizării soluțiilor de securitate o induce neconformității cu cerințele de securitate predefinite.

5.6. Limitele abordării propuse

Principala limită a abordării propuse pentru analiza şi compararea soluțiilor de securitate derivă din caracterul teoretic, impunându-se testarea utilității şi aplicabilității sale în mediile organizaționale reale. Transpunerea în practică a reperelor la care se recurge în lucrarea de față prezintă o serie de dificultăți specifice, prima dintre acestea vizând definirea coerentă, la un nivel de abstractizare potrivit, a resurselor informaționale şi a soluțiilor de securitate; de asemenea, acestea ridică problema granularității adecvate şi a tratamentului eventualelor suprapuneri şi dependențe. În plus, analiza şi clasificarea resurselor informaționale, la care se adaugă evaluarea neconformității cu cerințele de securitate, constituie un demers destul de laborios. Deşi uzuale în contextul managementului riscurilor de securitate, evaluările privind neconformitatea sunt complicate de abordarea detaliată, pentru fiecare obiectiv de securitate asociat resurselor informaționale.

6. Concluzii

Deşi nu prescrie un proces detaliat pentru selectarea sau clasificarea soluțiilor de securitate, lucrarea furnizează un set de repere utile unui astfel de demers, pornind de la ideea că nivelul costurilor fiecărei soluții trebuie justificat prin prisma contribuției la asigurarea unei protecții adecvate pentru resursele informaționale pe care le vizează. Sub rezerva că estimarea gradului de neconformitate cu obiectivele de securitate prezintă dificultăți inerente şi este condiționată de un management coerent al riscurilor de securitate la nivel organizațional, exigențele de securitate ale resurselor informaționale se constituie într-un sistem de referință non-monetar pentru cuantificarea eficienței şi a limitelor soluțiilor de securitate. Din această perspectivă, reperele propuse pentru analiză şi compararea soluțiilor de securitate prezintă avantajul caracterului generic, putând fi aplicate în mod uniform oricărui context organizațional, indiferent de maniera în care este gestionată securitatea informațională. Abordarea prezentată este complementară celor ce vizează dimensiunea economică şi financiară a securității, rezultatele demersului de selecție şi clasificare a soluțiilor de securitate putând servi la validarea analizelor privind impactul financiar al acestora.

BIBLIOGRAFIE

1. Anderson, E.E. şi Choobineh, J. (2008), Enterprise Information Security Strategies, *Computers & Security*, vol. 27, nr. 1/2, pp. 22-29, DOI:10.1016/j.cose.2008.03.002.
2. Barthélemy, J. (2001), The Hidden Costs of IT Outsourcing, *Sloan Management Review,* vol. 42, nr. 3, pp. 60-69.
3. Böhme, R. (2010), Security Metrics and Security Investment Models, In: *Advances in Information and Computer Security*. *Proceedings of IWSEC 2010*, LNCS vol. 6434, pp. 10-24, Belin/Heidelberg: Springer-Verlag.
4. Brecht, M., Nowey, T. (2012), A Closer Look at Information Security Costs, *11th Annual Workshop on the Economics of Information Security*, WEIS 2012, Berlin, [online], Disponibil la: http://www.econinfosec.org/archive/weis2012/papers/Brecht_WEIS2012.pdf, [Accesat pe 2 aprilie 2016].
5. Chen, P. (1976), The Entity-Relationship Model - Toward a Unified View of Data, ACM Transactions on Database Systems, vol. 1, nr. 1, pp. 9-36, DOI:10.1145/320434.320440.
6. Devos, J., Munteanu, A. şi Fotache, D. (2013), How Much Matter Probabilities in Information Security Quantitative Risk Assessment?, In: *International Business Information Management Conference (22nd IBIMA) - Creating Global Competitive Economies: 2020 Vision Planning & Implementation*, Noiembrie 2013, Roma, pp. 45-57.
7. EY - Ernst & Young (2015), *Creating Trust in the Digital World. EY's Global Information Security Survey 2015*, [online], Disponibil la: http://www.

ey.com/GL/en/Services/Advisory/ey-global-information-security-survey-2015-1, [Accesat pe 2 aprilie 2016].
8. Goettelmann, E., Dahman, K., Gateau, B., Dubois, E. şi Godart, C. (2014), A Security Risk Assessment Model for Business Process Deployment in the Cloud, *IEEE International Conference on Services Computing*, Iunie 2014, Anchorage, AK - SUA, pp. 307-314.
9. Gordon, L.A., Loeb, M.P. (2002), The Economics of Information Security Investment, *ACM Transactions on Information and System Security*, vol. 5, nr. 4, pp. 438-457.
10. Gordon, L.A., Loeb, M.P. şi Lucyshyn, W. (2003), Information Security Expenditures and Real Options: A Wait-and-See Approach, *Computer Security Journal*, vol. 9, nr. 2, pp. 1-7.
11. Gordon, L.A. şi Loeb, M.P. (2005) *Managing Cybersecurity Resources: A Cost-Benefit Analysis*, New York: McGraw-Hill Education.
12. Gordon, L.A. şi Loeb, M,P. (2006), Budgeting Process for Information Security Expenditures, *Communications of the ACM 2006*, vol. 49, nr. 1, pp. 121–125, DOI: 10.1145/1107458.1107465.
13. Hamill, J.T, Dekro, R.F. şi Kloeber, J.M. (2005), Evaluating Information Assurance Strategies, *Decision Support Systems*, vol. 39, nr. 3, pp. 463–484, DOI:10.1016/j.dss.2003.11.004.
14. Hoo, K.J.S. (2002): How Much is Enough? A Risk-Management Approach to Computer Security, In: *Workshop on Economics and Information Security (WEIS)*, University of California, Berkeley.
15. Lee, C.H., Geng, X. şi Raghunathan, S. (2016), Mandatory Standards and Organizational Information Security, *Information Systems Research,* vol. 27, nr. 1, pp.70-86, DOI:10.1287/isre.2015.0607.
16. Oberlaender, M.S. (2011), Data classification - A New Approach to Data Centric Security, (*IN)SECURE Magazine*, nr. 31, Septembrie 2011, pp. 35-42.
17. NIST (2005), National Institute of Standards and Technology - Special Publication 800-65, Version 1.0, *Integrating IT Security into the Capital Planning and Investment Control Process,* [online], Disponibil la: http://csrc.nist.gov/publications/nistpubs/800-65/SP-800-65-Final.pdf, [Accesat pe 2 aprilie 2016].
18. NIST (2012), National Institute of Standards and Technology - Special Publication 800-30, Revision 1*, Guide for Conducting Risk Assessments,* [online], Disponibil la: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf, [Accesat pe 2 aprilie 2016].
19. Pontes, E., Guelfi, A.E., Silva, A.A.A. şi Kofuji, S.T. (2011), A Comprehensive Risk Management Framework for Approaching the Return on Security Investment (ROSI), In: Savino, M. (Ed), *Risk Management in Environment, Production and Economy*, pp. 149-170, Intech, DOI: 10.5772/25911.
20. PwC - PricewaterhouseCoopers (2015), *The Global State of Information Security Survey*, [online], Disponibil la: http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html, [Accesat pe 2 aprilie 2016].
21. Scholtz, T. (2011), Articulating the Business Value of Information Security. Technical report, Gartner Inc., [online], Disponibil la: https://www.forrester.com/report/Articulating+The+Business+Value+Of+Information+Security/-/E-RES54908, [Accesat pe 2 aprilie 2016].
22. Zhao, X., Xue, L. and Whinston, A.B. (2009), Managing Interdependent Information Security Risks: A Study of Cyberinsurance, Managed Security Service and Risk Pooling, In: *Proceedings of the International Conference on Information Systems ICIS 2009*, Phoenix – Arizona, Paper 49, [online], Disponibil la: http://aisel.aisnet.org/icis2009/49, [Accesat pe 2 aprilie 2016].