Managementul riscurilor asociate instrumentelor de marketing online

Autor: **Mihai Orzan**

Abstract: Managementul riscurilor reprezintă procesul de implementare şi actualizare a unor metode şi instrumente de minimizare a riscurilor asociate sistemului informaţional al unui organizaţii, precum Politicile de Securitate Informaţională, procedurile şi practicile formalizate asociate acesteia, precum şi alte mijloace adoptate cu scopul aducerii acestor riscuri la niveluri acceptabile. Acest proces implică identificarea, analiza, evaluarea, tratarea şi monitorizarea riscurilor asociate securităţii informaţionale la nivel organizaţional.

Cuvinte cheie: managementul riscurilor, evaluare calitativă, evaluare cantitativă, VAR, OCTAVE, UCRA

Keywords: risk management, quantitative evaluation, qualitative evaluation

Pentru a se asigura succesul managementului riscurilor asociate securităţii informaţionale este vitală implicarea conducerii superioare a organizaţiei, prin promovarea activă a procesului şi asigurarea resurselor necesare acestuia. De asemenea, această practică s-a dovedit de succes în special în situaţiile în care managementul riscurilor a fost realizat de către echipe mixte, care au inclus administratori ai sistemelor informatice şi manageri din sistemul de producţie al organizaţiei.

Având în vedere că activităţile şi activele organizaţionale sunt într-o permanentă restructurare, că tehnologia informaţiei este unul dintre cele mai efervescente domenii ale economiei moderne şi că resursele umane şi tehnologice ale unei organizaţii sunt ajustate frecvent, şi activităţile asociate minimizării riscurilor informaţionale trebuie revăzute şi actualizate periodic, pentru a se analiza aceste modificări şi pentru a se determina gradul curent de eficienţă a controalelor implementate.

Evaluarea riscurilor, în conformitate cu definiţia dată de standardul BS7799:1 reprezintă „identificarea ameninţărilor la adresa securităţii informaţionale şi a vulnerabilităţilor fizice şi logice care le-ar putea cauza, impactul pe care materializarea acelor ameninţări l-ar avea asupra performanţelor organizaţiei analizate, ca şi probabilitatea producerii acestor ameninţări.” Pe scurt, riscul este tratat prin prisma ameninţărilor, activelor şi a vulnerabilităţilor cu care este asociat. De-a lungul timpului, a existat o modificare de paradigmă în tratarea riscurilor, în acest moment atenţia specialiştilor în securitate informaţională fiind concentrată asupra managementului riscurilor şi nu în evitarea acestora.

În general, riscurile pot fi transferate, respinse, reduse sau acceptate. Un exemplu de transfer al riscurilor este achiziţionarea unei polițe de asigurare de la o societate specializată pentru riscul identificat. Respingerea unui risc presupune ignorarea sa de către organizaţiei, ceea ce poate fi, pe termen lung, o politică extrem de periculoasă. De asemenea, riscurile pot fi reduse, prin implementarea sau îmbunătăţirea metodelor şi instrumentelor de minimizare a riscurilor (controale), luându-se însă tot

timpul în considerare atât beneficiile, cât şi costurile asociate acestor metode şi instrumente. Astfel, în cazul în care costul acestor controale depăşeşte beneficiile de care se va bucura organizaţia, atunci se poate decide acceptarea riscurilor în dauna securizării suplimentare a sistemului informaţional al organizaţiei.

Controalele asociate securităţii informaţionale a organizaţiei sunt în general clasificate ca şi acţiuni, proceduri, tehnici sau echipamente. Robustatea unui control este asociată în general cu robusteţea sa implicită sau obţinută prin intervenţie umană, ca şi de eficienţa în prevenirea riscurilor. De asemenea, controalele sunt clasificate din perspectiva documentării şi explicitării lor în controale formale şi controale ad-hoc, din perspectiva modului de declanşare se discută despre controale manuale, respective automate, iar din perspectiva momentului în care sunt aplicate, controalele sunt clasificate în preventive şi detective.

Nivelul de risc pe care o organizaţie, în mod inevitabil, îl va menţine după implementarea unui program de management al riscurilor, poartă denumirea de risc rezidual. Acesta poate fi ulterior utilizat de către echipa de management al riscurilor sau de către conducerea organizaţiei pentru a identifica acele zone în care nivelul controalelor nu este corespunzător şi întărirea acestora, pentru a reduce în continuare nivelul de risc informaţional la care este supusă organizaţia în cauză. În general, conducerea stabileşte o ţintă (nivel maxim) pentru riscul rezidual, iar colectivul de management al riscurilor face tot ce-i va sta în putinţă pentru atingerea acestei ţinte. Acceptarea unui anumit nivel al riscului rezidual în general se bazează pe politica organizaţiei, un proces formal de identificare şi măsurare a riscurilor, nivelul de incertitudine asociat însuşi procesului de evaluare a riscurilor, ca şi analiza cost-beneficiu a controalelor identificate.

Realizarea unui program de management al riscurilor presupune, într-o primă fază, stabilirea scopulurilor acestei activităţi, acestea putând include reducerea costurilor de asigurare a riscurilor sau reducerea scurgerii de informaţii sensibile în afara organizaţiei. Prin determinarea intenţiilor sale înainte de iniţierea unui program de management al riscurilor, instituţia poate evalua rezultatele şi le poate determina eficienţa.

De asemenea, în mod necesar realizarea activitatea de planificare pentru programul de management al riscurilor presupune desemnarea unei persoane sau a unei echipe responsabile pentru implementarea acestuia. O echipă de succes presupune integrarea tuturor nivelelor oranizaţionale la nivelul acestei echipe, sau cel puţin o bună colaborare a membrilor echipei cu toate nivelele semnificative ale organizaţiei, colaborare în general facilitată de implicarea şi suportul conducerii organizaţiei.

Pentru a realiza o identificare şi evaluare a riscurilor asociate securităţii informaţionale, este esenţială identificarea ameninţărilor asupra sistemului şi vulnerabilităţile pe care acestea le pot exploata. Pentru fiecare pereche ameninţare/vulnerabilitate, se determină gravitatea impactului asupra activelor informaţionale ale organizaţiei (pierderea confidenţialităţii, a integrităţii sau a disponibilităţii acestora) şi se determină probabilitatea exploatării acelei vulnerabilităţi, în condiţiile controalelor de securitate implementate la nivelul sistemului.

Standardul BS7799 conţine nu mai puţin de 127 de instrumente de minimizare a riscurilor (controale). Însă, în mod evident, nu toate acestea sunt aplicabile tuturor organizaţiilor, iar standardul sugerează că un sistem de analiză a riscurilor ar trebui utilizat pentru clasificarea riscurilor relevante pentru fiecare situaţie în parte.

Analiza riscurilor reprezintă acea parte a procesului de management al riscurilor care este preocupată de minimizarea riscurilor asociate producerii unor ameninţări din mediul intern sau extern al organizaţiei care să exploateze vulnerabilităţi asumate sau necunoscute ale sistemului informaţional şi astfel să afecteze securitatea activelor informaţionale. De asemenea, analiza riscurilor presupune asocierea unor frecvenţe cu care ameninţările asociate acestor riscuri se pot produce, ca şi impactul pe care acestea îl pot avea asupra desfăşurării optime a activităţilor normale ale organizaţiei analizate.

După ce conducerea organizaţiei a înţeles informaţiile legate de mediul tehnologic şi informaţional care conduc la formarea riscurilor identificate şi a impactului lor potenţial asupra organizaţiei, se recomandă prioritizarea acestor riscuri, în funcţie de gravitatea pe care producerea lor le-ar putea avea asupra organizaţiei. Probabilitatea producerii şi magnitudinea impactului reprezintă elementele de bază ale acestei prioritizări, care mai poate include elemente precum nivelul costurilor asociate implementării respectivelor controale sau costul presupus de îndepărtarea efectelor negative produse de către producerea lor.

De-a lungul timpului, un număr ridicat de metodologii de identificare a riscurilor asociate securităţii informaţionale au fost propuse şi adoptate, iar o simplificare a modului de abordare a diferitelor metodologii a dus la o clasificare a acestora în cantitative şi calitative, în special din perspectiva metricilor utilizate pentru cuantificarea riscurilor. În practică însă se utilizează aproape întotdeauna o combinaţie a acestor metode, în funcţie de caracteristicile organizaţiei investigate şi gradul de incertitudine asociat metodei de analiză şi management al riscurilor. Astfel, dacă toate elementele acestei analize (valoarea activelor, severitatea impactului, frecvenţa ameninţărilor, eficienţa controalelor, inceretitudinea şi probabilitatea materializării ameninţării) sunt exprimate în termeni cantitativi, atunci procesul poate fi caracterizat ca fiind unul în totalitate cantitativ. Altfel, în funcţie de modalitatea de exprimare a acestor măsurători, managementul riscurilor este parţial sau în totalitate unul calitativ.

Evaluarea riscurilor informaţionale pleacă de la şase elemente distincte considerate în managementul riscurilor: valoarea activelor informaţionale, frecvenţa ameninţărilor, gravitatea exploatarii vulnerabilităţilor organizaţionale cu ocazia producerii ameninţărilor, eficienţa modalităţilor de minimizare a riscurilor (controalelor), costul acestora, ca şi nivelu de incertitudine asociat procesului de management al riscurilor informaţionale. Măsura în care aceste variabile sunt cuantificate cu ajutorul unor modalităţi de măsurare independente şi obiective, precum costul înlocuirii pentru valoarea activelor informaţionale, sau frecvenţa anuală asociată ameninţărilor de securiate informaţională, metodologia de evaluare a riscurilor este considerată una cantitativă. Dacă toate cele şase variabile sunt măsurate cantitativ, atunci metodologia este una cantitativă.

Evaluarea cantitativă a riscurilor

Numai valoarea activelor informaţionale şi costul implementării şi menţinerii elementelor de minimizare a riscurilor (controalele) pot fi asociate unor valori monetare. Astfel, sunt utilizate metrici precum Frecvenţa Anuală de producere a ameninţarilor (FA), exprimată sub forma x/y (x reprezintă număr de apariţii ale activităţilor, evenimentelor sau acţiunilor considerate ameninţări pentru sistemul informaţional în perioada y), Ponderea Pierderilor (PP) generate de materializarea unui risc în relaţia cu

un anumit bun (activ) informaţional, exprimată procentual, indicele eficienţei controalelor sau nivelul de incertitudine.

Frecvenţa Anuală (FA) de producere a producere a ameninţărilor caracterizează probabilitatea ca o anumită ameninţare să se manifeste într-un an. Astfel, o ameninţare care se poate produce o dată la 10 ani are o FA de 1/10, sau 0,1.

Factorul de Expunere (FE) reprezintă o modalitate de reprezentare a gravităţii impactului unei anumite ameninţări asupra sistemului informaţional organizaţional. Este exprimat sub forma unui procent din valoarea activului afectat în cazul producerii ameninţării considerate.

Eficienţa Controlului (EC) reprezintă gradul, exprimat procentual, în care un anumit control previne riscul de exploatare al unei vulnerabilităţi de către o ameninţare.

Pierderile Provizionate (PP) individuale sunt calculate pentru fiecare activ informaţional includ în programul de management al riscurilor, ca produs al Valorii de Schimb (VS) sau de înlocuire a respectivului activ şi Factorul de Expunere. Pierderile provizionate individuale apar în general ca rezultat al analizei de impact a ameninţărilor şi tind să fie exagerate de către analişti, pentru a se atrage atenţia conducerii asupra importanţei lor.

Pierderile Anuale Previzionate (PAP) reprezintă o modalitate de determinare a costurilor asociate materializării diferitelor tipuri de ameninţare, calculată ca produs al Pierderilor Previzionate (PP) individuale şi al Frecvenţei Anuale (FA) a acestora. Exprimarea sa anuală are rolul facilitării utilizării sale în calculele financiar-contabile ale organizaţiei. Astfel, pentru o ameninţare care poate genera pierderi de 100.000 Euro pentru o anumită organizaţie, cu o FA de 1/100, valoarea PAP va fi de 1.000 de euro.

Factorul de Incertitudine (FI) reprezintă gradul, de asemenea exprimat procentual, în care rezultatele procesului de evaluare a riscurilor sunt sigure. Incertitudinea este în general măsurată invers proporţional cu nivelul de încredere (atunci când nivelul de încredere este scăzut FI este ridicat, şi invers).

Distribuţia Marginală (DM) reprezintă o modalitate de centralizare a metricilor cantitative sub o formă care include incertitudinea inerentă procesului de evaluare prin utilizarea unor intervale (ex.: Există o probabilitate de 80% ca baza de date cu clienţii organizaţiei să aibă un cost de înlocuire de 175.000 – 200.000 de euro, sau Centrul Naţional de Seismologie apreciază că există o şansă de 60% de producere a unui cutremur cu magnitudine de peste 7 grade Richter în zona Vrancea în următorii 10 ani). DM prezintă şi avantajul facilitării consensului printre membrii echipei de management al riscurilor în ceea ce priveşte valorile diferitelor metrici.

Utilizarea metodologiilor cantitative de evaluare a riscurilor securităţii informaţionale presupun o serie de avantaje precum obţinerea unor informaţii obiective şi semnificative statistic, valoarea informaţiilor exprimată cantitativ este mult mai uşor inteligibilă de către persoanele cu o pregătire marginală în domeniile asociate tehnologiei informaţiei, rezultatele reprezintă o bază credibilă pentru analiza cost/beneficiu şi pentru activităţile bugetar-contabile, performanţa activităţilor de management al riscurilor este uşor evaluabilă şi exprimată într-o modalitate familiară conducerii organizaţiei.

Pe de altă parte însă, utilizarea metodelor cantitative presupune asumarea unor neajunsuri asociate acestora, precum complexitatea calculelor necesare determinării valorilor diferitelor variabile (iar lipsa unor explicaţii clare poate duce la lipsa de încredere a conducerii pentru nişte valori obţinute pe baza unor metode de tip „cutie neagră"), utilizarea acestor metode în lipsa unui instrument automatizat este extrem de

dificilă şi îndelungată (s-a estimat că timpul necesar realizării unei astfel de analize fără aportul instrumentelor automatizate este de 10-20 de ori mai mare decât o analiză calitativă similară), informaţiile necesare analizei sunt mult mai numeroase şi mai complexe şi nu există un standard universal acceptat şi dezvoltat de către o organizaţie independentă, ceea ce scade credibilitatea şi acurateţea instrumentelor automatizate disponibile pe piaţă.

Evaluarea calitativă a riscurilor

Având în vedere că toate metricile calitative conţin un anumit grad de subiectivism, utilizarea unor scale de tipul diferenţialelor semantice („Foarte ridicat", „Ridicat", „Mediu", „Scăzut", „Foarte Scăzut") poate fi adaptat fiecăreia dintre elementele identificării şi evaluării riscurilor informaţionale. Astfel, diferitele metodologii calitative sau parţial calitative au dus la implementarea unor instrumente specifice de recoltare a informaţiilor necesare procesului de evaluare a riscurilor informaţionale, fără a exista însă un standard general acceptat.

Astfel, pentru determinarea **probabilităţii de exploatare a unei anumite vulnerabilităţi** a sistemului presupune asocierea unei frecvenţe cu care ameninţare asociată acesteia se produce. Această probabilitate este asociată unui număr de factori care includ arhitectura sistemului, mediul extern, modalitatea de control a accesului la activele informatice protejate, ca şi de eficienţa controalelor implementate. Astfel, Tabelul 1 prezintă o serie de niveluri asociate frecvenţei materializării ameninţărilor, în condiţiile controalelor existente:

Tabelul 1: Probabilitatea de materializare a ameninţărilor

Probabilitate	Descriere
Neglijabilă	Improbabilă realizarea
Foarte redusă	Ameninţarea se manifestă o dată la 2 sau 3 ani
Redusă	Ameninţarea se manifestă anual sau mai rar
Medie	Ameninţarea se manifestă binanual sau mai rar
Ridicată	Ameninţarea se manifestă lunar sau mai rar
Foarte ridicată	Ameninţarea se manifestă de mai multe ori pe lună
Permanentă	Ameninţarea se manifestă zilnic sau chiar mai des

Determinarea **magnitudinii sau severităţii impactului unei anumite ameninţări** presupune identificarea pierderilor potenţiale la nivelul fiecărei categorii de securitate (confidenţialitate, integritate şi disponibilitate), în condiţiile probabilităţii asociate producerii acesteia. Impactul poate fi asociat cu pierderea funcţionalităţii sistemului sau altor active ale organizaţiei, degradarea acestora, reducere timpului de răspuns pentru utilizatorii legitimi, pierderea încrederii publice în organizaţie sau divulgarea neautorizată a datelor sensibile. Gravitatea impactului acestor ameninţări este în general evaluat pe baza informaţiilor prezentate în Tabelul 2.

Tabelul 2: Niveluri ale severităţii materializării ameninţărilor

Severitatea impactului	Descriere

Nesemnificativă	Producerea amenințării şi exploatarea vulnerabilității nu vor avea aproape nici un impact asupra organizației.
Minoră	Organizația va fi doar uşor afectată. Va fi necesar un efort mimin pentru remedierea problemelor generate.
Semnificativă	Va avea ca rezultat efecte negative tangibile, deşi neglijabile şi remarcate doar de un număr redus de angajați sau parteneri. Ar putea duce însă la publicitate negativă şi va fi necesară afectarea unui număr semnificativ de resurse pentru remediere.
Importantă	Ar putea avea ca rezultat pierderea încrederii în capacitatea conducerii şi a sistemului de securitate informațională al organizației. Vor fi necesare resurse importante pentru remedierea problemelor cauzate.
Ridicată	Ar putea duce la pierderi semnificative de active informaționale, ca şi la pierderea unor clienți sau parteneri, ca şi la diminuarea credibilității externe a organizației.
Critică	Producerea acestor amenințări ar avea ca rezultat compromiterea extensivă a sistemului informațional sau chiar deteriorarea permanentă a acestuia, mergându-se până la distrugerea acestuia.

În sfârşit, determinarea **nivelului riscurilor** este în general făcută pe baza probabilității ca o anumită amenințare să exploateze o vulnerabilitate a sistemului şi pe gravitatea pe care materializarea acelei amenințări o are asupra activelor informaționale ale organizației. Matematic, nivelul riscului este determinat ca produs al probabilității de manifestare a amenințărilor şi severitătii impactului acestora asupra confidențialității, disponibilității şi integrității sistemului informațional al organizației. Tabelul 3 prezintă nivelul riscurilor bazate pe cei doi parametri, nivel ce poate fi incrementat în anumite condiții (nivelul de securitate asociat sistemului informațional, compromisurile pe care le presupune materializarea riscurilor, etc.) de către echipa de management al riscurilor.

Tabelul 3: Nivelul riscurilor

Probabilitatea producerii	**Severitatea impactului**					
	Nesemnificativă	**Minoră**	**Semnificativă**	**Importantă**	**Ridicată**	**Critică**
Neglijabilă	Redus	Redus	Redus	Redus	Redus	Redus
Foarte redusă	Redus	Redus	Redus	Redus	Moderat	Moderat
Redusă	Redus	Redus	Moderat	Moderat	Ridicat	Ridicat
Medie	Redus	Redus	Moderat	Ridicat	Ridicat	Ridicat
Ridicată	Redus	Moderat	Ridicat	Ridicat	Ridicat	Ridicat
Foarte ridicată	Redus	Moderat	Ridicat	Ridicat	Ridicat	Ridicat
Permanentă	Redus	Moderat	Ridicat	Ridicat	Ridicat	Ridicat

Printre avantajele utilizării metodelor calitative este inclus faptul că, în general, nu este nevoie de stabilirea exactă a valorii financiare a activelor, ci mai degrabă a efectelor asupra acestora în termenii generali ai securității informaționale (confidențialitate, disponibilitate, integritate). De asemenea, eventualele calculele prespuse de aceste metode sunt simple şi rapide, nu necesită calculul exact al costului implementării şi menținerii controalelor şi al diferitelor modalități alternative de minimizare a riscurilor şi sunt mult mai rapid dezvoltate ş implementate decât metodologiile cantitative.

Evaluarea calitativă a riscurilor asociate securităţii informaţionale presupune însă şi o serie de dezavantaje, printre care faptul că evaluarea riscurilor şi rezultatele acestui proces sunt esenţial subiective, influenţate de calificarea şi experienţa analiştilor. De asemenea, lipsa unor valori numerice asociate costurilor presupuse de riscurile identificate tinde să ducă la o percepţie inexactă a acestora. În plus, acest tip de evaluare nu oferă informaţii utile analizei cost/beneficiu şi nu permite urmărirea obiectivă a performanţelor activităţilor de management al riscurilor, în cazul în care toate metricile sunt de natură subiectivă.

Metoda OCTAVE

Metodologia **OCTAVE** (Operationally Critical Threat, Asset and Vulnerability Evaluation – Evaluarea Ameninţărilor, Activelor şi Vulnerabilităţilor Organizaţionale Critice) pleacă de la definirea complexă, sistematică şi contextuală a componentelor estenţiale ale unui sistem informaţional, folosind o organizare în trei etape pentru a determina riscurile asociate confidenţialităţii, integrităţii şi disponibilităţii activelor informaţionale critice pentru buna desfăşurare a activităţilor organizaţiei considerate. Metoda abordează atât aspectele organizaţionale, cât şi cele tehnologice necesare asigurării securităţii informaţionale, dintr-o perspectivă modernă, ce prevede un proces continuu de evaluare.

Etapa 1: **Construirea unor profile ale activelor bazate pe ameninţările asupra acestora**. Această etapă presupune evaluarea întregii organizaţii, zonele cheie fiind identificate şi analizate în scopul extragerii acelor active informaţionale relevante, ameninţările asociate acestora, controalele (curente şi potenţial necesare) pe care minimizarea acestor ameninţări le prespun, ca şi puncte slabe la nivelul abordării Politicii şi practicilor de securitate informaţională la nivelul organizaţiei. La rândul ei, această etapă este divizată în patru paşi.

Pasul 1: *Determinarea competenţei la nivelul securităţii informaţionale pentru managementul superior al organizaţiei*.

Pasul 2: *Determinarea competenţei în domeniul securităţii informaţionale pentru nivelul operaţional al organizaţiei*.

Pasul 3: *Determinarea competenţei angajaţilor în domeniul securităţii informaţionale*.

Primii trei paşi sunt dedicaţi întâlnirilor cu angajaţii de pe toate nivelurile organizaţionale în scopul identificării activelor asociate sistemului informaţional şi a modalităţii în care acestea pot fi afectate. Astfel, în cadrul acestor întâlniri participanţilor li se solicită identificarea priorităţii/importanţei acestor active şi nivelul de sigurantă care există/ar trebui obţinut pentru protejarea acestora.

Pasul 4: *Crearea profilului ameninţărilor*. În acest pas participanţii sunt în exclusivitate membrii echipei de management al riscurilor informaţionale, care pe baza documentaţiei şi a informaţiilor obţinute în primii trei paşi selectează activele critice în buna desfăşurare a activităţilor organizaţionale, grupează şi clasifcă aceste active, împreună măsurile de securitate asociate, în conformitate cu nivelul organizaţional pe care îl deservesc, creînd o imagine de ansamblu asupra activelor organizaţionale şi identifică ameninţările asupra acestor clase de active şi asupra activelor individuale.

Etapa 2: **Identificarea vulnerabilităţilor structurale**. Această etapă presupune evaluarea sistematică a structurii informaţionale a organizaţiei pentru a determina eficienţa soluţiilor de securitate informaţională curentă, a identifica deficienţele şi vulnerabilităţile sistemului (clasificate ca vulnerabilităţi conceptuale, de implementare şi de configurare). În general, aspectele tehnologice sunt identificate prin compararea cu standardele de profil stabilite fie de producători, fie de organisme independente. În general, în această fază punctele slabe ale sistemului sunt determinate pe baza unei multitudini de instrumente automatizate, incluzând instrumente pentru testarea integrităţii fişierelor, programe antivirus, eficienţa sistemului de limitare a accesului prin parole, siguranţa comunicaţiilor, precum şi multe alte instrumente.

Pasul 5: *Identificarea componentelor cheie*.În această fază membrii echipei de management al riscurilor implică şi personalul departamentului informatic al organizaţiei analizate şi cu ajutorul acestora identifică principalele clase de componente ale sistemului informatic pe baza analizei căilor de acces la resursele informatice, în contextul unor scenarii de materializare a ameninţărilor.

Pasul 6: *Evaluarea componentelor cheie*. Acest pas, de asemenea realizat în colaborare cu personalul departamentului informatic al organizaţiei analizate, presupune determinarea vulnerabilităţii tehnologice, cu ajutorul instrumentelor automatizate, care determină vulnerabilitatea în faţa unor ameninţări provenite din exteriorul, din interiorul şi din exteriorul organizaţiei. Apoi rezultatele acestei investigaţii sunt analizate şi pe baza lor sunt formulate concluzii prealabile în ceea ce priveşte cauzale fenomenelor constatate (vulnerabilităţile sistemului informaţional).

Etapa 3: **Dezvoltarea Planului şi Strategiei de Securitate Informaţională**. Odată ce activele, ameninţările şi vulnerabilităţile au fost identificate, se trece la identificarea riscurilor la care este supus sistemului informaţional. Scopul acestei etape este de a determina modul în care anumite riscuri sunt asociate anumitor active organizaţionale. Din perspectiva OCTAVE riscul este considerat un rezulatat al pierderilor cauzate de absenţa sau inadecvarea unor modalităţi de prevenire sau minimizare a acestora. Măsurarea pierderilor, severităţii impactului sau nivelului riscurilor poate fi atât calitativă, cât şi cantitativă, în funcţie de neceistăţile organizaţionale şi resursele disponibile colectivului de management al riscurilor sistemului de securitate informaţională. Determinarea riscurilor asociate securităţii informaţionale este în general mai dificilă datorită faptului că informaţiile despre ameninţări şi valoarea activelor sunt în general mai greu de obţinut şi cuantificat, iar factorii de risc sunt în permanentă schimbare. Analiza riscurilor pe baza metodologiei OCTAVE presupune utilizarea unor scenarii de risc, asociate fiecărui activ critic al organizaţiei.

Pasul 7: *Identificarea riscurilor securităţii informaţionale*. Scopul acestui pas este de a definitiva un profil al riscurilor, în urma analizei gravităţii impactului ameninţărilor identificate asupra fiecărui activ informaţional. De asemenea, se utilizează o serie de criterii de evaluare calitativă (scala diferenţială semantică) a riscurilor pentru stabilirea importanţei şi impactului riscurilor, iar în final echipa de management al riscurilor informaţionale stabileşte costul materializării riscurilor identificate pentru organizaţia analizată.

Pasul 8: *Dezvoltarea modalităţilor de protejare a sistemului informaţional*. Scopul acestui ultim pas al metodologiei OCTAVE este de a dezvolta o strategie de protejare a organizaţiei prin intermediul unor controale pentru activele critice, ca şi o

listă de activităţi ce trebuie realizate pentru implementarea acestora, listă ce include termene de realizare şi nominalizarea persoanelor responsabile. De asemenea, la nivelul acestui pas se realizează o revizuire a documentaţiei adunate pe parcursul proiectului de management al riscurilor asociate securităţii informaţionale, concluziile fiind prezentate membrilor conducerii organizaţiei, în colaborare cu care este stabilită forma finală a strategiei de protejare a activelor informaţionale critice ale organizaţiei.

Metoda VAR

O altă metodă mixtă (calitativă şi cantitativă de evaluare a riscurilor, cunoscută sub denumirea de VAR (VAloarea Riscurilor), pleacă de la identificarea celor mai drastice efecte pe care producerea riscurilor asociate securităţii informaţionale le-ar putea avea asupra organizaţiei, într-un orizont de tip şi un interval de încredere dat, scopul său fiind realizarea unei balanţe optime între nivelul asumat al riscurilor şi cheltuielile necesare minimizării acestora. Cele patru etape propuse de către metodologia VAR includ identificarea ameninţărilor, estimarea probabilităţii de producere a acestor ameninţări, calcularea indicatorului VAR (valoarea riscurilor), respectiv determinarea controalelor pentru prevenirea sau minimizarea efectelor riscurilor identificate.

Etapa 1: **Identificarea ameninţărilor**: În această primă etapă sunt identificate riscurile (curente sau potenţiale) cu care se poate confrunta sistemul informaţional analizat. Metoda VAR recomandă classificarea acestora ca şi fraude, activităţi rău intenţionate, glume, tentative de accesare a informaţiilor confidenţiale, dezastre naturale, sabotaj şi erori de utilizare. Modalităţile concrete de manifestare a acestor ameninţări pot include atacuri de tip DoS, furtul, ştergerea sau modificarea informaţiilor sau afectarea funcţionării normale a reţelelor. Aceste metode sunt concepute pentru a exploate vulnerabilităţile sistemelor informaţionale şi includ viruşi informatici, programe de tip troian, viermi, programe de „spargere” a parolelor, interceptarea poştei electronice şi a pachetelor tranzacţionate de diverse aplicaţii prin reţelele de comunicaţie informatice, ca şi asumarea unor false identităţi la nivelul acestor reţele (spoofing).

Etapa 2: **Estimarea probabilităţii de producere a ameninţărilor şi a riscurilor asociate acestora**. Activităţile din această etapă au ca obiectiv determinarea probabilităţii de producere a ameninţărilor identificate în etapa anterioară. Această activitate poate fi realizată pe baza metodelor calitative sau cantitative descrise anterior. În plus, metoda VAR recomandă utilizarea surselor secundare de informaţii (studii furnizate de către agenţii guvernamentale sau de către institute de sondare a pieţei) pentru obţinerea informaţiilor legate de frecvenţa producerii diferitelor tipuri de ameninţare. Astfel, un studiu publicat de Briney în anul 2000 (http://www.infosecuritymag.com/articles/september00/pdfs/Survey1_9.00.pdf) reallizat în Statele Unite asupra unui eşantion reprezentativ din rândul angajaţilor departamentele de tehnologia informaţiei ale unor organizaţii particulare şi guvernamentale a concluzionat că 80% dintre sistemele informatice pe care le folosesc s-au confruntat cu viruşi informatici în ultimul an, utilizarea abuzivă a resurselor informaţionale ale organizaţiei a fost raportată de 58% dintre aceştia, 42% s-au confruntat cu tentative de acces neautorizat din afara organizaţiei, iar 24% dintre ei au avut de remediat efectele

distructive ale activității rău intenționat sau accidentale ale colegilor lor. Surse suplimentare pentru aceste informații pot fi rapoartele publice/guvernamentale, jurnalele asociate diferitelor sisteme informatice sau aplicațiilor utilizate, date istorice sau interviuri în profunzime cu personalul relevant din departamentele de securitate informațională.

Etapa 3: **Estimarea VAR**. Pe baza riscurilor identificate în etapa anterioară şi a frecvenței cu care amenințările care le generează se produc, metoda VAR presupune calcularea variabilei cu aceiaşi denumire, plecând de la Valoarea de Piață (VP) a organizației investigate, orizontul de tip dorit şi intervalul de încredere (statistică) a rezultatului obținut, după formula:

$$VAR = \pm\alpha * \sigma * \sqrt{T}$$

unde α reprezintă intervalul de încredere a rezultatului (pentru 99% valoarea sa este 2,64, pentru 95% 1,96), σ reprezintă Valoarea de Piață estimată a organizației, iar T este numărul de zile pentru care se realizează calculul.

Etapa 4: **Modalități de minimizare a riscurilor identificate**. Ultima etapă a acestei metode presupune selectarea diferitelor metode de minimizare a riscurilor (pe baza standardelor existente în industrie şi pe baza surselor secundare de informare). Valoarea VAR este utilizată pentru a determina nivelul investiției, o companie pentru care această valoare este mai redusă necesitând o investiție mai modestă în asigurarea securității informaționale decât companiile cu o valoare similară mai ridicată.

Metoda UCRA

Metoda de evaluare a riscurilor intitulată **UCRA** (University of California Risk Assessment) dezvoltată de către teoreticienii de la University of California este o metodă esențial cantitativă, care urmăreşte îndeaproape recomandările standardului BS7799, realizarea sa presupunând urmărirea unui număr de nouă păşi.

Pasul 1: **Stabilirea echipei de evaluare a riscurilor**. Această echipă va fi responsabilă pentru colectarea, analiza şi raportarea rezultatelor către conducerea organizației. Este esențial ca toate elementele ciclului productiv al organizației să fie reprezentate la nivelul acestei echipe, incluzând la nivel minim forța de muncă, administrația, sistemele informatice şi securitatea fizică.

Pasul 2: **Definirea obiectivului proiectului**. Echipa de evaluare a riscurilor ar trebui să clarifice încă de la început obiectivul proiectului de evaluare a riscurilor, cu specificarea departamentului, ariei sau funcției organizației ce va fi evaluată, responsabilitățile membrilor echipei, personalul ce va fi intervievat, standardele utilizate, documentația necesară în procesul de evaluare, ca şi operațiile sau funcțiile ce vor fi observate în acest proces.

Pasul 3: **Identificarea activelor implicate în procesul de evaluare**. Activele organizaționale pot include (fără a fi limitate la) personal, bunuri hardware şi software, date şi informații (inclusiv clasificări asupra datelor sensibile şi critice pentru buna funcționare a organizației), facilitățile în care se desfăşoară activitatea, ca şi controale implementate pentru protejarea acestora. Identificarea tuturor activelor asocitate cu obiectivele proiectului definite în pasul anterior este esențială pentru proiectul de management al riscurilor.

Pasul 4: **Clasificarea pierderilor potenţiale**. Această etapă presupune identificarea şi descrierea modului în care producerea situaţiilor de risc identificate ar afecta funcţionarea organizaţiei, precum şi pierderile (financiare sau de altă natură) pe care aceasta le-ar suport în acest caz. Astfel, aceste pierderi ar putea fi rezultatul afectării fizice a echipamentelor, împiedicarea utilizatorilor legitimi să acceseze bunurile organizaţionale, modificarea, accesul neautorizat sau divulgarea informaţiilor confidenţiale. Iar în unele cazuri pierderile pot fi necuantificabile, precum pierderea credibilităţii organizaţiei.

Pasul 5: **Identificarea ameninţărilor şi vulnerabilităţilor**. O ameninţare este definită ca fiind un eveniment, proces sau acţiune ce exploatează o vulnerabilitate pentru a afecta un activ informaţional al organizaţiei. Astfe, poate fi vorba de ameninţări naturale, umane accidentale sau rău intenţionate. Mai în detaliu, ameninţările se pot concretiza în evenimente de tipul căderilor de tensiune, contaminare biologică sau scurgerea unor produse chimice toxice, dezastre naturale, funcţionarea defectuoasă a echipamentelor hardware sau a produselor software, distrugerea sau afectarea integrităţii datelor, sabotaj, furt sau vandalism. La rândul lor, vulnerabilităţile se referă la puncte slabe în securitatea logică sau fizică a activelor organizaţionale, pe care o ameninţare le poate exploata pentru a le afecta. Vulnerabilităţile sunt în general clasificate ca şi vulnerabilităţi ale securităţii fizice, de meniu, de securitate a sistemelor, de securitate a proceselor de comunicaţie, asociate personalului, a planurilor, a politicilor, procedurilor, de conducere, de suport, precum şi alte tipuri.

Pasul 6: **Identificarea controalelor existente**. Diferitele modalităţi de minimizare a riscurilor de producere a evenimentelor cu efecte negative asupra securităţii informaţionale a organizaţiei sunt în general cunoscute sub denumirea de controale. Astfe, controalele sunt definite ca instrumente de siguranţă cu rolul de a reduce probabilitatea ca o anumită ameninţare să exploateze cu succes o vulnerabilitate a sistemului informaţional pentru a ataca cu succes un anumit activ al organizaţiei. Această etapă este preocupată de identificarea acelor controale care sunt deja implementate, ca şi de determinarea utilităţii şi eficienţei lor în contextul analizei curente.

Pasul 7: **Analiza datelor**. În această etapă toate datele colectate vor fi utilizate pentru a determina riscurile efective la care sunt supuse activele care fac obiectul proiectului curent de management al riscurilor. Tehnica de analiză UCRA presupune pregătirea unei liste (Tabelul 4) de active şi ameninţările asociate acestora, tipurile de pierderi cauzate de materializarea respectivelor ameninţări şi vulnerabilităţile care au facilitat atacurile. De asemenea, trebuie estimată frecvenţa cu care aceste ameninţări s-ar putea manifesta.

Pasul 8: **Determinarea unor modalităţi de minimizare a riscurilor eficiente din perspectiva costurilor de implementare**. Evaluarea trebuie să prezinte şi o estimare a costurilor asociate implementării controalelor propuse, a costurilor anuale de mentenanţă şi actualizare şi asupra ciclului de viaţă al acestora.

Pasul 9: **Raportul final**. Proiectul de management al riscurilor, în conformitate cu metodologia UCRA, presupune prezentarea unui raport final formalizat într-o formă inteligibilă şi utilă audienţei avute în vedere. În general este vorba despre un raport simplu şi uşor de citit şi asimiliat, care prezintă concluziile alături de analizele detaliate care au dus la formularea lor. De asemenea, raportul ar trebui să includă datele identificate la nivelul organizaţiei şi lista completă de active, ameninţări şi

vulnerabilităţi asociate, ca şi determinarea riscurilor, controalele recomandate şi o analiză cost-beneficiu.

Avantajele implementării unui proces de management al riscurilor

Conducerea organizaţională ignoră, în majoritatea cazurilor, procesul de management al riscurilor, ca şi riscurile asociate securităţii informaţionale a organizaţiei, în ansamblul lor. În general, activităţile care nu sunt în mod direct cuantificabile şi pentru care un nivel al profitului generat nu poate fi în mod direct prezentat, tind să fie ignorate de către conducerea superioară, motiv pentru care activităţile de management al riscurilor necesită o activitate de conştientizare, atât printre managerii organizaţiei, cât şi la nivelul angajaţilor. De asemenea, există şi teama ca aceste proiecte să scoată la lumină neconcordanţe şi lipsuri legate de conducerea sistemului informatic al organizaţiei sau al nivelului superior de conducere ca motivant al rezistenţei întâmpinată de acest tip de activitate. Şi cu toate că un nivel ridicat al securităţii informaţionale poate părea costisitor, lipsa unei securităţi adecvate se va dovedi cu siguranţă, pe termen lung, catastrofală pentru organizaţie. În sfârşit, atunci când acest proces este realizat în întregime manual, sau nu poate fi făcut decât prin utilizarea unor metrici calitative, faptul că acest proces poate dura luni de zile şi că nu are ca rezultat o analiză de sensitivitate este un obstacol major pentru declararea sa ca un succes al organizaţiei.

Dar procesul de management al riscurilor asociate securităţii informaţionale aduce o serie de avantaje majore pentru oricare organizaţie care depune eforturile necesare implementării sale. Astfel, la nivel minim, conducerea acelei organizaţii va fi sensibilizată asupra noţiunii de risc de securitate informaţională, va cunoaşte valoarea activelor şi pierderile pe care aceste riscuri le pot aduce organizaţiei (în ceea ce priveşte confidenţialitatea, integritatea şi disponibilitatea activelor informaţionale), va avea o analiză cost-beneficiu asociată acestor riscuri şi va şti care sunt măsurile necesare pentru a minimiza riscurile de exploatare a vulnerabilităţilor inerente de către ameninţările interne şi externe.

De asemenea, evaluarea riscurilor permite identificarea celor mai eficiente modalităţi de prevenire a efectelor negative asupra activelor informatice, înainte ca diferite fonduri să fie alocate către variante alternative de lucru. În plus, o echipă specializată în procesul de management al riscurilor poate realiza această activitate într-un timp redus, pornindu-se de la câteva zile până la câteva săptămâni, în funcţie de dimensiunea organizaţiei investigate.

Tabelul 4: Instrument de evaluare a riscurilor conform metodologiei UCRA

Proces, activitate sau acțiune	Procedură şi modalitate de stocare	Riscuri	Controale curente	Controale recomandate	Acțiuni recomandate (când şi de către cine)
Descriere generală a proceselor, activităților sau acțiunilor analizate. Sunt separate subactivitățile sau paşii care pot expune la diferite tipuri de riscuri, fiecăruia fiindu-i atribuit un rând propriu.	Descrierea tipurilor de informație stocate, nivelul de sensitivitate, modul de stocare şi drepturile de acces asupra acestora.	Care sunt evenimentele care ar putea afecta buna funcționare a activelor şi proceselor descrise? Care ar fi impactul acestora? Care sunt vulnerabilitățile exploatate?	Descrierea controalelor utilizate în prezent pentru minimizarea riscurilor de securitate identificate.	Evaluarea de către oamenii implicați asupra completitudinii proceselor, procedurilor, riscurilor şi controalelor identificate în analiză. În general, sunt răspunsuri din categoria Da sau Nu.	Dacă trebuie îmbunătățite sau adăugate controale, specificându-se efectele obținute, activitățile necesare, personalul implicat şi momentul realizării.

În plus, nivelul de integrare şi extindere a bunurilor informatice specifice economiei moderne permite specialiştilor în tehnologia informației să-şi prezinte recomandările pe baza unor analize statistice şi financiare bine fundamentate, care permit conducerii adoptarea unor decizii informate, nu bazate strict pe riscuri *presupuse*. Un program de management al riscurilor bazat pe un model strict de analiză, atât calitativ cât şi cantitativ, va putea să prezinte modalități tangibile de reducere a costurilor de asigurare a riscurilor şi a pierderilor asociate riscurilor securității informaționale.

Bibliografie

Amelinckx, I. şi van Grembergen, W., *Measuring and Managing E-business projects through the balanced scorecard*, apărută în *Proceedings of the International Conference on Electronic Commerce (ICEC)*, Viena, noiembrie 2001

Berghout, E şi Renkema, T. *Methodologies for IT investment evaluation: a review and assessment*, apărută în *Information Technology Evaluation Methods and Management*, Idea Group Publishing, 2001, pg. 78-97

Johner, H., Fujiwara, S., Yeung, A., Stephanou, A., Whitmore, J., *Deploying a Public Key Infrastructure*, IBM, 2000

McNamee, David, *Business Risk Assessment*, The Institude of Internal Auditors, 1998

Munteanu, Adrian, *Auditul sistemelor informaționale contabile*, Ed. Polirom, 2001

Orzan, Gheorghe, *Sisteme informatice de Marketing*, Ed. Uranus, Bucureşti, 2001

Orzan, M, Munteanu, A., Iliescu, F., şi Mincu, M., *Securitatea IT şi implementarea standardului ISO/IEC 17799*, Ed. Internews, 2005

Parasuraman, A., Zeithaml, V.A. şi Berry, L.L. R*eassessment of Expectations as a Comparison Standard in Measuring Service Quality: Implications for Further Research*, publicat în *Journal of Marketing*, Vol.58, ianuarie 1994

Parker, Michael, *Strategic Transformation and information technology*, Prentice Hall, Upper Saddle River, NJ, 1996

Seddon, P. B., *A Respecification and Extension of the DeLone and McLean Model of IS Success*, publicat în *Information Systems Research*, Vol. 8, No. 3, septembrie 1997.

Smith, Gordon, *Network Auditing: A Control Assessment Approach*, John Wiley & Sons, USA, 1999

Turban, E., Aronson, J.E., *Decision Support Systems and Intelligent Systems*, Prentice Hall, Englewood Cliffs, NJ, 2001

Vegheş, Călin, *Marketing Direct*, Ed. Uranus, 2003