The Impact of Delivering E-Banking Services on the Traditional Banking Risks

Drd. Mihaela Carmen TRUFAŞU
IT Project Manager – WYLOG ROMANIA

Technological innovation and competition among existing banking organizations have allowed a wider array of banking products and services to become accessible and delivered through the Internet. The rapid development of e-banking capabilities carries risks as well as benefits. The bankers are to recognize, address and manage banking institutions in a prudent manner according to the fundamental characteristics and challenges of e-banking services.
Keywords: *e-banking risks, traditional banking risks, operational risk, strategic risk.*

Societăţile bancare din toată lumea au furnizat servicii la distanţă pentru clienţii lor cu mult înaintea apariţiei termenului de e-banking. Transferul electronic de fonduri pentru plăţi de nivel redus, sistemele de gestiune al cash ului la nivel de corporaţie, cât şi maşini de unde se pot retrage sume de bani de către public au fost şi sunt o prezenţă uzuală în ţările cu tradiţie bancară şi în România. Ce toate acestea, furnizarea de servicii financiare utilizând reţele publice ca Internetul - prin Internet înţelegând toate tehnologiile ce permit accesul la reţea, inclusiv accesul wireless - a produs schimbări masive în industria de servicii financiare.

Problemele şi tendinţele care se manifestă ca purtătoare de risc din punct de vedere al caracterului electronic al furnizării de servicii financiare pe Internet sunt cauzate de diverşi factori cum ar fi viteza cu care sunt introduse pe piaţă produse şi servicii financiare noi, din dorinţa de a devansa concurenţa, viteza de procesare a tranzacţiilor ca urmare a evoluţiei spectaculoase în domeniul telecomunicaţiilor, în domeniul software şi hardware. Această frenezie în adoptarea noului şi implementarea noilor tehnologii este rareori dublată de cunoştinţe şi experienţă de lucru cu noile tehnologii si a riscurilor aduse de utilizarea acestor tehnologii.

Noi surse de risc sunt reprezentate şi de serviciile care provin din exteriorul întreprinderilor bancare pentru furnizarea de servicii bancare, de la terţi care nu au nici un fel de experienţă sau cunoştinţe legate de gestiunea riscului.

In aceste noi condiţii ce impun viteză în tranzacţii şi procesare se manifestă şi o cerere crescută pentru implementarea unei infrastructuri tehnologice scalabile, flexibile şi care să permită interoperabilitatea atât între întreprinderi cât şi în interiorul lor şi care să poată asigura securitatea, integritatea şi disponibilitatea informaţiilor şi serviciilor.

Potenţialul de fraudă a crescut datorită absenţelor standardelor operaţionale de verificare a clienţilor şi de autentificare a lor pe reţele deschise ca şi Internetul iar ambiguitate sau absenţa de reglementări legislative care să se adapteze activităţilor e-banking în continuă evoluţie creează vulnerabilităţi serioase în sistemele bancare.

Colectarea, stocarea şi partajarea frecventă a unor cantităţi semnificative de date cu privire la clienţi poate duce la apariţia unor probleme legate de confidenţialitatea datelor clientului ce pot crea băncii riscuri de natură prudenţială, ca de exemplu risc legal şi reputaţional.

Proceduri online de autentificare lungi sau complicate pot face clientul să renunţe la utilizarea paginii web prin intermediul căreia dorea acces la servicii bancare; mai mult, operaţiunile laborioase de lucru cu un client pot afecta performanţa generală a aplicaţiei web.

Organizaţiile bancare se concentrează din ce în ce mai mult pe activităţile de e-banking şi îşi extind, în prezent aceste activităţi, explorând utilizarea reţelelor wireless şi extinzându-şi activitatea şi în arii noi de comerţ electronic.

Internetul oferă de asemenea posibilitatea extinderii clientelei şi în afara graniţelor ţării în care operează. Cu toate acestea, natura deschisă a reţelei şi evoluţia comerţului electronic expun băncile la o concurenţă semnificativă întreţinută atât de alte bănci cât şi de companii nebancare.

Toţi aceşti factori reprezintă noi provocări pentru instituţiile financiare în procesul de management al securităţii, integrităţii şi disponibilităţii serviciilor oferite pentru a rămâne şi profitabile, în acelaşi timp.

In cele ce urmează voi prezenta pe scurt impactul asupra riscului strategic si a celui operaţional, riscuri al căror profil se modifică semnificativ datorită e-banking.

Riscul strategic este unul din cele mai importante riscuri pe care activităţile de e-banking îl prezintă pentru organizaţiile bancare. Riscurile strategice diferă de celelalte categorii de risc prin faptul că sunt mai generale şi au o natură mai largă.

Dată fiind cererea în creştere şi acceptarea de către clienţi pe scară largă a serviciilor de e-banking cât şi a eficienţei potenţiale aduse de aceste servicii, băncile au fost puse în faţa necesităţii adoptării unei strategii de utilizare a canalelor de livrare de servicii financiare mijlocite de Internet pentru oferirea către clienţi a acestor servicii. Schimbările rapide survenite în tehnologie, ritmul competiţiei cu alte bănci sau cu organizaţii nonbancare şi natura strategiei adoptate pot expune banca la riscuri substanţiale dacă planificarea şi implementarea strategiei nu este corectă sau dacă strategia în sine nu este bine gândită.

Decizia de pionierat în materie de tehnologie utilizată pentru furnizarea de servicii e-banking poate constitui un factor important de risc strategic mai ales dacă sistemul nu este suficient de rapid dezvoltat şi implementat iar tehnologiile nou apărute anulează starea de pionierat pe care se bazau iniţial strategii băncii. In contradicţie cu pionieratul se găseşte decizia de a folosi tehnici deja testate pentru dezvoltarea şi implementarea serviciilor e-banking, tehnici ce se pot dovedi uzate moral la sfârşitul procesului de implementare.

Înaintea Internetului, băncile utilizau reţele de tip proprietar pentru a face legătura între unităţile corporaţiei distribuite din punct de vedere geografic sau chiar şi cu un număr limitat de alte bănci. Aceste reţele de tip proprietar au ajutat la construirea unei apărări strategice împotriva noilor intraţi pe piaţă şi au generat o protecţie individuală prin intermediul francizei – necesitatea cumpărării dreptului de a participa la reţelele private de tip proprietar.

Internetul, însă este o reţea publică la care accesul este nelimitat atât pentru întreprinderile bancare cât şi pentru cele nonbancare, ele fiind libere să-şi extindă aria de operaţiuni fără a fi necesară extinderea prezenţei fizice. In consecinţă a crescut competiţia în industria financiară şi este foarte probabil ca această competiţie să crească şi în continuare.

Majoritatea bancherilor consideră canalul de distribuţie e-banking ca mijloc de reducere a cheltuielilor operaţionale. Cu toate acestea, mulţi dintre clienţii e-banking doresc să-şi menţină relaţiile tradiţionale cu banca, ceea ce face dificil abandonul infrastructurii existente, în vederea reducerii costurilor operaţionale.

Aceasta înseamnă că, cel puţin în viitorul apropiat, băncile vor trebui să-şi ofere serviciile pe multiple canale de distribuţie iar implementarea e-banking va constitui în mod cert o cheltuială în plus pentru bancă. Reducerile în cheltuielile operaţionale prin implementarea e-banking se pot înregistra totuşi în timp, dar numai pe orizonturi de timp medii sau mari.

Apariţia *agregării*[1] şi a sistemului de *screen scrapping* constituie atât o oportunitate strategică pentru bănci dar şi o ameninţare. In funcţie de natura şi evoluţia relaţiei dintre agregator, banca afectată şi consumator, băncile pot fi şi mai dezintermediate datorită "ruperii" relaţiei tradiţionale directe dintre bancă şi client iar agregatorii pot limita accesul direct pe care băncile îl aveau la clienţii online. In plus, activitatea de agregare agre-

[1] *Agregare* şi *screen scrapping* = culegerea direct de pe ecran a informaţiilor cu privire la client de pe un site. Agregatorul acţionează la cererea clienţilor şi oferă informaţii consolidate cu privire la datoriile şi disponibilităţile financiare ale clienţilor. Clienţii agregatorului îi furnizează acestuia parola şi identificatorul unic pentru a accesa informaţiile sale la diferite bănci sau instituţii nebancare şi pentru a-i putea prezenta o imagine consolidată a situaţiei financiare.

sivă atât de către bănci cât şi de către instituţiile nebancare pot duce la o mare răspândire a produselor şi serviciilor bancare reducând însă profitul băncii şi aducând cu sine riscuri potenţiale de natură legală sau legată de securitate.

Datorită legăturii dintre tehnologie şi e-banking, ***riscul operaţional*** este cel mai afectat de furnizarea de servicii e-banking.

Pentru a limita riscul operaţional, organizaţiile bancare sunt nevoite să ia în considerare implementarea unei arhitecturi tehnologice operaţionale integrate, la nivel corporativ care să faciliteze interoperabilitatea, să asigure securitatea, integritatea şi disponibilitatea datelor şi să permită gestiunea relaţiilor cu terţi furnizori de servicii. Mai mult, cum tehnologia se schimbă dramatic modelul de business şi procesele operaţionale, băncile se întâlnesc cu necesitatea implementării şi întreţinerii unor proceduri de control adecvate – inclusiv pentru controlul implementării schimbărilor, şi a unor procese de audit.

Infrastructura tehnologică - e-banking ul a adus cu sine problema integrării sistemelor tehnologice şi a aplicaţiilor cu operaţiunile şi cu procesele existente. Multe bănci se confruntă acum cu problema integrării sistemului e-banking cu sistemul informatic aflat în funcţiune şi cu sistemul multiplu de furnizori de servicii şi parteneri. Aceste bănci sunt expuse unor riscuri operaţionale semnificative datorită erorilor ce pot apare în procesul de procesare a tranzacţiilor datorată unei incorecte integrări a sistemului e-banking cu sistemul de procesare existent.

In consecinţă, multe bănci investesc cantităţi mari de bani in dezvoltarea infrastructurii tehnologice pentru a crea procese interne de control şi supraveghere extinsă a riscurilor ce provin din integrarea sistemelor. Prin aceste investiţii băncile încearcă să-şi crească flexibilitatea, scalabilitatea şi interoperabilitatea sistemelor şi operaţiilor atât în interiorul întreprinderii cât şi în relaţiile externe cu furnizorii de servicii.

In timp ce aceste evoluţii pot avea conotaţii pozitive pentru marile societăţi bancare, industria bancară mai are mult de evoluat pe calea îmbunătăţirii infrastructurii de management a riscurilor pentru a susţine eficient activitatea de e-banking.

Băncile de dimensiuni medii sau mici se confruntă cu provocări şi mai mari datorită necesităţii încadrării în bugete mult mai mici pentru achiziţionarea tehnologiei software şi hardware cât şi datorită necesităţii de atragere şi păstrare a personalului cu înaltă calificare tehnică solicitat de funcţionarea e-banking. Multe din aceste bănci apelează la serviciile unor terţi pentru a-şi procura infrastructura tehnologică necesară furnizării de servicii e-banking. In această situaţie, banca îşi va lua importanta responsabilitate de a asigura că aceste operaţiuni sunt bine conduse şi controlate iar supraveghetorul prudenţial va dori să se asigure că banca este capabilă să conducă aceste activităţi.

Securitatea - Majoritatea bancherilor intervievaţi de Electronic Banking Group consideră riscul de securitate ca o principală preocupare legată de e-banking. Ameninţări din afară cum ar fi atacurile de tip *hacking*[2], *sniffing*[3], *spoffing*[4] sau *denial of service*[5] expun banca la noi riscuri legate de securitate.

Canalele de furnizare deschise utilizate pentru e-banking creează noi probleme de securitate pentru bănci din punctul de vedere al respectării confidenţialităţii şi integrităţii informaţiilor, nerepudierii tranzacţiilor, autentificarea utilizatorilor şi controlul accesului.

Printre problemele principale pe care bancherii doresc să le rezolve cât mai rapid se numără dezvoltarea unor instrumente cât mai robuste de verificare a identităţii şi autenticităţii cererilor de tranzacţii de valoare mare. In plus, industria bancară trebuie să-şi continua munca de determinare a cerinţelor pentru elaborarea celei mai bune metode de criptare, care să includă şi legalitatea semnăturii electronice şi a documentelor electronice. S-a constatat de-a lungul vremii, în multe organi-

[2] *hacking* = practica de a intra fraudulos la datele stocate pe un computer, fără autorizare, din motive maliţioase pentru a demonstra că acest lucru poate fi realizat sau din alte motive personale

[3] *sniffing* = utilizarea unui program care este instalat în mod ilicit pe un calculator dintr-o reţea, program care să captureze datele de identificare şi parolele folosite de utilizatorii care intră în sistem.

[4] *spoofing* = încercarea de obţinere a accesului la un sistem prin "pozarea"/impersonarea ca user autorizat

[5] atac de tipul "*refuz de serviciu*" (*denial of service*) = încercarea de a suprasatura un server cu cereri astfel încât acesta să nu mai poată răspunde traficului legitim.

zaţii, că atacurile din interior, realizate de angajaţi sunt mult mai frecvente decât cele din exterior. O securitate cu deficienţe poate duce la afectarea reputaţiei şi chiar probleme de natură legală datorită incapacităţii băncii de a proteja datele personale ale clienţilor.

Integritatea datelor – este o componentă importantă a securităţii sistemului. Organizaţiile bancare se văd nevoite să-şi perfecţioneze interoperabilitatea în interiorul şi în afara întreprinderii pentru a gestiona eficient relaţiile cu clienţii, cu alte bănci sau cu furnizori de servicii. Până când se vor crea standarde pentru managementul informaţiilor stocate pe suport electronic, organizaţiile bancare vor continua să fie înscrise în cursa de stabilire a celor mai eficiente procese de asigurare a acurateţei şi integrităţii datelor transmise şi primite.

Dat fiind costul redus şi natura omniprezentă a Internetului, organizaţiile folosesc din ce în ce mai mult protocolul TCP/IP ca standard de protocol de comunicaţie. Există numeroase beneficii ca urmare a utilizării acestui protocol dar băncile trebuie să se asigure că datele transmise între sistemele electronice existente şi sistemele terţilor cu care intră în interacţiune sunt translatate şi integrate corespunzător pentru folosirea acestui standard de protocol de comunicaţie.

Mai mult, în timp ce introducerea nivelului *middleware* şi a limbajelor cum ar fi XML (*Extensible Markup Language*) facilitează acest efort, dezvoltarea de standarde la nivelul industriei bancare pentru a susţine aceste noi tehnologii este încă în faze incipiente.

Disponibilitatea sistemului - pentru asigurarea unei reţele interne securizate pentru activităţile de e-banking, planificarea eficientă a resurselor este critică în asigurarea continuităţii disponibilităţii produselor şi serviciilor e-banking.

Volumul tranzacţiilor poate avea o volatilitate mare datorită automatizării şi a scăderii costurilor per tranzacţie.

De asemenea concurenţa împinge băncile să declare că serviciile oferite sunt disponibile 24 de ore din 24, 7 zile din 7, iar acest lucru a dus la creşterea considerabilă a aşteptărilor clienţilor reducând în acelaşi timp toleranţa la erori. Pentru a face faţă concurenţei şi pentru a evita riscul potenţial şi semnificativ legat de reputaţie care poate interveni în condiţii de întrerupere de furnizare a serviciilor datorate supraîncărcării sistemului, băncile trebuie să ofere combinaţia optimă de produse şi servicii securizate, caracterizate de acurateţe şi consistenţă. Aceşti factori diminuează importanţa continuităţii efective a furnizării de servicii, a recuperării din eroare şi a planurilor de răspuns la incidente. Mai mult, faptul că numeroase bănci apelează la terţi pentru furnizarea de servicii e-banking, face necesară verificarea regulată a capacităţii acestora de a asigura continuitatea furnizării de servicii şi existenţa la aceştia a unor planuri de recuperare din eroare şi de răspuns la incidente – la fel de eficiente ca şi cele stabilite în interiorul băncii. Atacuri de tipul *refuz de servicii* pot reduce sau elimina capacitatea băncii de a-şi servi clienţii în timpul atacului. Aceste atacuri au devenit din ce în ce mai frecvente şi au fost îndreptate împotriva celor mai mari actori de pe piaţa e-commerce. O provocare suplimentară este dată de imposibilitatea băncii de a controla disponibilitatea Internetului ca reţea.

In concluzie, o bancă trebuie să aibă în vedere, ca parte a planului de rezolvare a situaţiilor nefavorabile ce pot apare, alternative menite să furnizeze servicii în cazul producerii unui eveniment major care duce la întreruperea funcţionării unei părţi din Internet.

Control şi audit intern - abilitatea de a detecta şi a corecta erori este o componentă critică a sistemului de control intern din orice operaţiune bancară. Mai mult, organizaţiile bancare trebuie să aibă în funcţiune suficiente proceduri de control pentru prevenirea fraudei venite din exterior sau din interior şi să protejeze informaţiile şi activele băncii.

Mare parte din eficienţa şi reducerea costurilor generată de e-banking stă în abilitatea de implementare a procesării imediate, procesare ce se realizează automat, fără intervenţie umană. In timp ce beneficiile procesării automate a tranzacţiilor sunt numeroase, realitatea este că e-banking modifică modul în care se aplică pe canale de larg acces, procedurile de control intern, partajarea sarcinilor şi

responsabilităţilor şi păstrarea de informaţii de urmărire a tranzacţiilor în vederea auditului. Provocarea determinată de aceste schimbări este accentuată de absenţa competenţelor şi experienţei în industrie atât în aria operativă cât şi în aria de audit. Mergând înainte pe această cale, băncile vor fi solicitate din ce în ce mai mult să se asigure că mediul puternic automatizat oferă control eficient şi că aceste procese de control pot fi auditate independent. *Subcontractarea* - faptul că pentru dezvoltarea industriei de e-banking, băncile au fost nevoite să subcontracteze părţi importante din angrenajul de funcţionare, afectează în foarte mare măsură profilul de risc al băncilor indiferent de dimensiunea lor. Băncile mari subcontractează din ce în ce mai multe activităţi, pe măsura dezvoltării lor, încercând să şi canalizeze eforturile numai spre funcţia şi competenţa lor de bază, toate activităţile din afara sferei de competenţe bancare fiind subcontractate către terţi. Băncile mici, adeseori sunt nevoite să subcontracteze părţi ale activităţii desfăşurate din cauza lipsei de experienţă în domeniu şi a lipsei de competenţe tehnice şi a resurselor necesare pentru construirea unor canale de furnizare de servicii e-banking. In plus, scăderea preţului pe piaţă a soluţiilor gata făcute, a diminuat efortul financiar al băncilor mici de a furniza servicii e-banking. Aceste evoluţii sunt benefice pentru piaţă, pentru că au permis intrarea în competiţie şi a firmelor mai mici dar au şi adus noi provocări în managementul riscului operaţional, managementul relaţiilor cu terţii având impact asupra gestionării mai multor categorii de riscuri. Studiile realizate de EBG[6] au indicat faptul că băncile tind să se bazeze pe un număr relativ redus de furnizori, furnizorii fiind, cel mai frecvent, instituţii de dimensiuni medii şi mici. In anumite cazuri chiar furnizorii erau firme nou apărute pe piaţă, cu un istoric de activitate relativ scurt. Această dependenţă de un număr relativ mic de furnizori prezintă motive de îngrijorare pentru autorităţile de supraveghere ce ar putea avea implicaţii la nivel sistemic, de industrie bancară, dacă un asemenea furnizor de servicii s-ar confrunta cu probleme majore. Pentru a gestiona corect riscurile asociate cu subcontractarea, băncile trebuie să ia toate măsurile de precauţie şi să monitorizeze constant relaţia şi activitatea cu furnizorii de servicii. Corectitudinea termenilor din contractele de furnizare de servicii trebuie de asemenea bine evaluată pentru a reduce riscul de încălcare e unor legi în vigoare.

Procesarea operaţiunilor şi gestiunea riscului de menţinere a securităţii, a integrităţii şi a disponibilităţii serviciilor se complică datorită subcontractării. Mai mult, mulţi dintre furnizorii de servicii şi parteneri subcontractori, sunt societăţi nou înfiinţate şi pot avea carenţe în cunoştinţele cu privire la reglementările din domeniul bancar. Întreruperi minore de activitate la nivelul furnizorilor de servicii pot avea efecte majore în ceea ce priveşte imaginea băncii, poate duce la pierderi financiare importante şi la apariţia unui important risc de natură legală. Complexitatea în managementul riscurilor este adusă şi de relaţiile de interdependenţă dintre partenerii care subcontractează operaţiuni legate de e-banking. Subcontractarea poate duce la riscuri suplimentare de păstrare a confidenţialităţii datelor clienţilor. Băncile pot fi în necunoaştere de cauză cu privire la modul de culegere şi utilizare a datelor cu privire la clienţi de către terţii subcontractori. Pentru a evita asemenea situaţii ambigue, băncile trebuie să acorde o foarte mare atenţie, în momentul încheierii contractelor de cu terţi pentru sub-contractarea de servicii e-banking, stipulărilor cu privire la confidenţialitate şi la natura sensibilă a datelor gestionate.

Bibliografie

1. Basno Cezar, Dardac Nicolae - "Riscuri bancare. Cerinţe prudenţiale. Monitorizare" - EDP, 1999;
2. Basno Cezar, Dardac Nicolae - "Management bancar ", ISBN: 973-590-702-X, 2002;
3. Basno Cezar, Dardac Nicolae. "Operaţiuni bancare-instrumente si tehnici de plata.", EDP, 1996;
4. Basel Committee Publications : "Operational Risk Management" – sept 1998; "Risk Management Principles for Electronic Banking" – mai 2001; "Consultative Document - Operational Risk Supporting Document to the New Basel Capital Accord "- mai 2001; "Basel Committee Publications" No. 98, iulie 2003

[6] *EBG* = Electronic Banking Group, grup de lucru creat la iniţiativa Comitetului de la Basel pentru a stabili standarde şi recomandări prudenţiale pentru activitatea de e-banking