ASIGURAREA RISCULUI CIBERNETIC - O MARE PROVOCARE CU CARE SE CONFRUNTĂ ECONOMIILE MODERNE

Prof.univ.dr. Leonardo Badea[1)] și Lect.univ.dr. Călin Mihai Rangu[2)*]

[1)] Președinte, Autoritatea de Supraveghere Financiară, București, România
[2)] Director, Autoritatea de Supraveghere Financiară, București, România

Rezumat

Asigurarea cibernetică dincolo de concept, trebuie să reprezinte un produs care să fie oferit societății moderne. Trăim într-o lume complexă bazată pe digitalizarea produselor si serviciilor. Digitalizarea implică şi un sistem complex de riscuri asociate. Drumul spre lumea de mâine trece prin lumea de azi și o analiză a situației existente în economiile contemporane cu privire la asigurarea riscului cibernetic este doar un prim pas pe care acest articol își propune sa-l realizeze.

Studiul urmărește fundamentarea nevoii de formulare și asumare de politici și de susținere a reglementării acoperirii riscurilor cibernetice prin asigurare, a nevoii de susținere a unor strategii sectoriale pentru creșterea nivelului de maturitate a companiilor din perspectiva protecției față de amenințările cibernetice. Este nevoie, de asemenea, de instituirea unui sistem de raportare a pierderilor generate de riscurile cibernetice, cel puțin pentru infrastructurile critice și importante, dezvoltarea și utilizarea de către asiguratori a unor modele de consultanță și evaluare, pe baza de standarde și certificări recunoscute la nivel mondial, inclusiv dezvoltarea competențelor necesare la nivelul asiguratorilor referitor la ingineria acestor riscuri.

Cuvinte cheie: risc cibernetic, asigurare, GDPR, management riscuri, subscriere, CISO, securitate IT, confidențialitate, disponibilitate, integritate date, infrastructuri critice, NIS, CERT

Clasificare JEL: D81, G22, H56, M15

Introducere

Tehnologia informației și a comunicațiilor digitale este prezentă zilnic în viața noastră, atât personală cât și a activităților profesionale, în servicii, în comerț, în susținerea infrastructurilor critice, peste tot. Dacă în asigurări unul din conceptele principale este cel de omogenizare, prin conectarea tuturor într-o rețea distribuită, prin intermediul Internetului,

* Autor de contact, **Călin RANGU** - Calin.RANGU@asfromania.ro

participăm la o rețea globală, omogenă. Deși această rețea virtuală si utilizatorii săi, sunt expuși unor mari și noi riscuri, amenințări concrete care fructifică din ce în ce mai mult vulnerabilitățile instituțiilor, companiilor și a persoanelor, conexiunea cu asigurările nu s-a realizat încă și este impetuos necesar să se realizeze pentru desfășurarea unei vieți digitale liniștite.

Conform Geneva Association[1] riscul cibernetic este cu siguranță cea mai mare provocare cu care se confruntă economiile moderne. Acesta poate fi definit ca orice risc care decurge din utilizarea tehnologiei informațiilor și a comunicațiilor inclusiv „încercarea deliberată a unor infractori informatici care se folosesc de internet pentru a utiliza rețelele de calculatoare asupra cărora au preluat controlul în scopul de a modifica, de a bloca sau de a distruge sisteme computerizate, rețele de calculatoare ori date sau programe stocate pe ele ori transmise de acestea”[2]. Atacurile cibernetice compromit confidențialitatea, disponibilitatea sau integritatea datelor sau a serviciilor. Acestea duc la întreruperea activităților/afacerilor, indisponibilizând infrastructurile critice (servicii publice, energie, transport, financiar etc), afectând oameni și proprietăți.

Noțiunea de risc cibernetic cuprinde o multitudine de riscuri care amenință bunurile firmelor, guvernelor sau persoanelor fizice, pierderile în general incluzând active financiare sau nefinanciare, identități, divulgarea de informații sensibile și întreruperea activităților/afacerii.

Riscurile cibernetice apar ca rezultat fie al atacurilor intenționate (criminale, teroriste, susținute de state ostile, activiști, șantaj sau din motive personale), fie evenimentelor accidentale (ștergeri date, întreruperi servicii)[3].

1. Amenințările cibernetice se află într-un trend de creștere, atât din punct de vedere al numărului, cât și al complexității.

Conform raportului CERT-RO[4] privind evoluția amenințărilor cibernetice pentru anul 2017 alertele de securitate cibernetică în România au crescut cu 25% față de anul 2016, afectând 33,71% (2,89 de milioane) adrese IP unice din România, din totalul IP-urilor alocate RO. Un procent de 10,32% (14,33 mil.) din alertele procesate se referă la sisteme informatice compromise, în sensul că, fie au fost infectate, fie au fost exploatate[5] și utilizate de atacatori în diferite tipuri de atacuri.

La nivel mondial atacurile majore sunt într-o creștere accelerată conform Fig.1, în primele 3 luni din 2019 s-au înregistrat 13 atacuri cibernetice importante conform CSIS & Hackmageddon[6].

---

[1] [3] [5] Understanding and Addressing Global Insurance Protection Gaps, Geneva Association, aprilie 2018

[2] https://wol.jw.org/ro/wol/d/r34/lp-m/102012171#h=1

[3] Raport privind evoluția amenințărilor cibernetice în 2017, CERT-RO, aprilie 2018,

[3] [4] Interviu Leonardo Badea, Președintele A.S.F.: https://www.ziarulprofit.ro/index.php/semnal-de-alarma-tras-de-presedintele-asf-asigurarea-riscului-cibernetic-o-mare-provocare-cu-care-se-confrunta-economiile-moderne/

[6] https://www.hackmageddon.com/category/security/cyber-attacks-statistics/

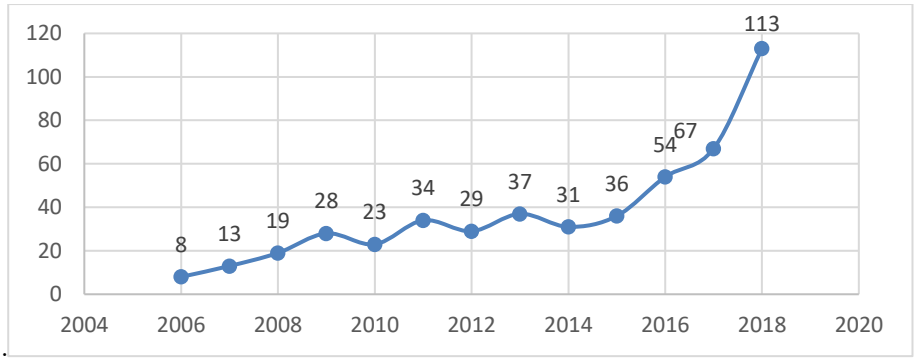

Figura nr. 1. Evoluţia anuală a numărului de atacuri cibernetice în perioada 2006 – 2018

Sursa : CSIS & Hackmageddon 2019 şi prelucrări proprii

Pe baza informațiilor disponibile publicului conform CSIS Technology Policy Program și hackmageddon.com, privind spionajul cibernetic și războiul cibernetic, excluzând criminalitatea informatică țările de origine și al victimelor ar fi cele reprezentate în Fig. 2. Campaniile de spionaj de lungă durată au fost tratate ca evenimente singulare în scopul totalurilor incidentelor. Datele sunt parțiali deoarece unele state ascund incidentele, în timp ce altele nu reușesc să le detecteze.

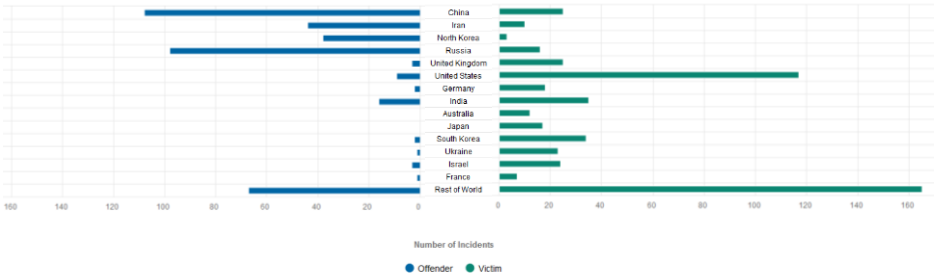

Figura nr. 2. Reprezentarea grafică pe ţări a numărului de atacuri cibernetice şi de victime, cumulate din 2006 până în 2019, CSIS Technology Policy Program

Sursa: CSIS & Hackmageddon

Estimarea costului incidentelor cibernetice este o provocare, companiile evitând a raporta pierderile. La nivel mondial se estimează pierderi cauzate de riscurile cibernetice la aproape 0,5 % din PIB-ul mondial și aproape de două ori mai mult decât media anuală a pierderilor cauzate de dezastrele naturale[7]. Dacă replicăm la nivelul României același procent de 0,5% din PIB ar rezulta pierderi de aproximativ 9 miliarde de EURO.

Valoarea pierderilor financiare generate de riscul cibernetic este dificil de estimat, existând un deficit de informație. Unele activități de criminalitate informatică nu au un cost direct sau nu pot fi cuantificate. Industria de profil încearcă să estimeze costurile totale,

costurile per incident, și costul pe înregistrare a unei încălcări a datelor conform tabelului 1[6]. Fig.3 și Fig. 4 prezintă estimări ale costurilor medii anuale ale criminalității informatice pe domenii și principalele țări afectate.

Tabel nr. 1. Costuri estimate ale criminalității informatice

GLOBAL COSTS (IN BILLION USD, PER ANNUM)	
Symantec (2013)	113
McAfee (2014)	445 (375-575)
Kshetri (2010)	100-1'000

COSTS PER INCIDENT (IN MILLION USD)	
Ponemon Institute (2015)	3.8
Geschonnek *et al.* (2013)	2.1
Kaspersky Lab (2013)	2.4

COST PER RECORD (IN USD)	
Symantec (2013)	298
Ponemon Institute (2015)	217
NetDiligence (2014)	956

COSTS BY COUNTRY (IN % OF GDP; MCAFEE; 2014)	
U.S.	0.64
China	0.63
Japan	0.02
Germany	1.60

Sursa: Geneva Association, 2016

În conformitate cu estimările companiei multinaționale „Accenture", de consultanță în management, soluții tehnologice și outsourcing, pe perioada 2015-2018, cele mai mari daune ale crimei cibernetice se înregistrează în domeniul pierderii informațiilor stocate electronic (circa 6 milioane de dolari SUA, în 2018), urmate de întreruperea afacerilor (circa 4 milioane de dolari SUA, în 2018), pierderile din cifra de afaceri şi avarierea echipamentelor (fig. nr. 3.):

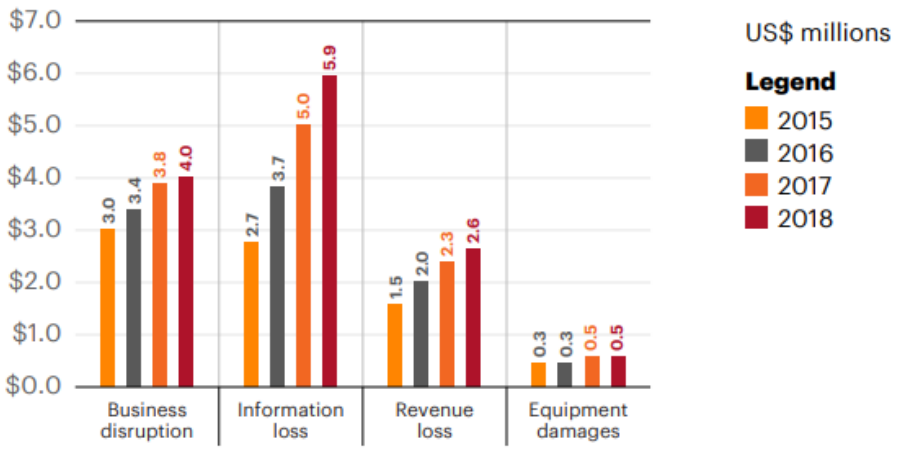

Figura nr. 3. Costurile medii anuale ale crimei cibernetice pe principalele domenii ale pierderilor

Sursa: Accenture, 2019

[6] Ten Key Questions on Cyber Risk and Cyber Risk Insurance, Geneva Association, nov 2016.

Sunt prezentate în continuare estimările aceleiași companii, pe ţări dezvoltate, în care SUA deţine recordul cu peste 27 milioane de dolari SUA, în 2018, urmată de Japonia, Germania Regatul Unit etc. (fig. nr. 4.).

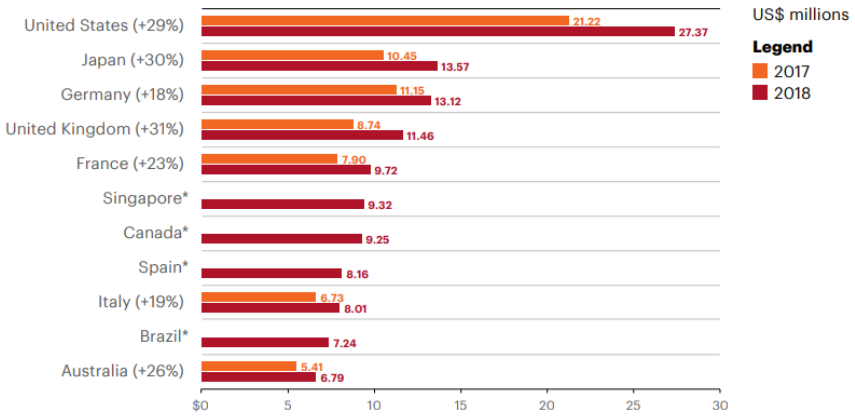

Figura nr. 4. Costurile medii anuale ale crimei cibernetice pe principalele ţări afectate
Sursa: Accenture, 2019

Pe baza unui barometru al riscurilor[8], realizat prin interviuri asupra a 968 de participanți, la nivelul anului 2019 s-au stabilit principalele cauze ale pierderilor generate de incidentele cibernetice (fig. 5):

1. Întreruperea afacerii
2. Pierderea reputației
3. Daunele generate de pierderea datelor
4. Costurile cu restaurarea datelor
5. Amenzi și penalități

Figura nr. 5. Principalele cauze ale pierderilor economice cauzate de incidentele cibernetice
Sursa: Allianz Risk Barometer, 2019

[8] Allianz Global Corporate & Specialty, Allianz Risk Barometer, 2019

Ca urmare a aplicării Regulamentului GDPR costuri majore, suplimentare, pot fi generate de afectarea datelor cu caracter personal.

2. Impactul financiar care poate fi acoperit de asigurările de risc cibernetic[7]:

- furtul de active (financiare),
- întreruperea activităților/afacerii cu afectarea veniturilor/cifrei de afaceri,
- costurile pentru protecție și despăgubiri, costuri adiționale cu investigarea pierderilor, costurile de comunicare (autorități, clienți, păgubiți) și de reparare.

Cu toate aceste pierderi, nivelul asigurărilor de risc cibernetic este foarte redus în comparație cu volumul de ansamblu al pieței asigurărilor. Swiss Re estimează ca în 2025 (Fig. 6) acest volum să ajungă la aproximativ 1% din piața globală a asigurărilor.

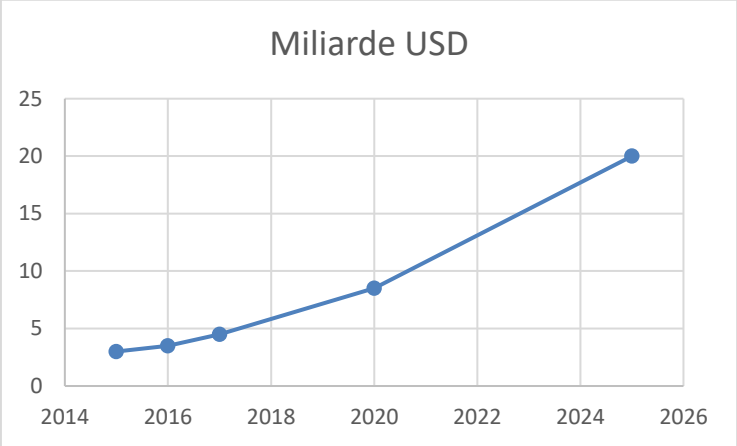

Figura nr. 6. Evoluția primelor subscrise pentru asigurările cibernetice
Sursa: Swiss Re, 2018

Previziuni similare realizează și portalul german on line pentru statistici „Statista”[9] pentru primelor de asigurare cibernetică subscrise la nivel mondial în perioada 2014-2020 conform Fig. 7.

[7] https://asfromania.ro/files/analize/Asigurari_risc_cibernetic.pdf
[9] https://www.statista.com/markets/414/topic/461/insurance/

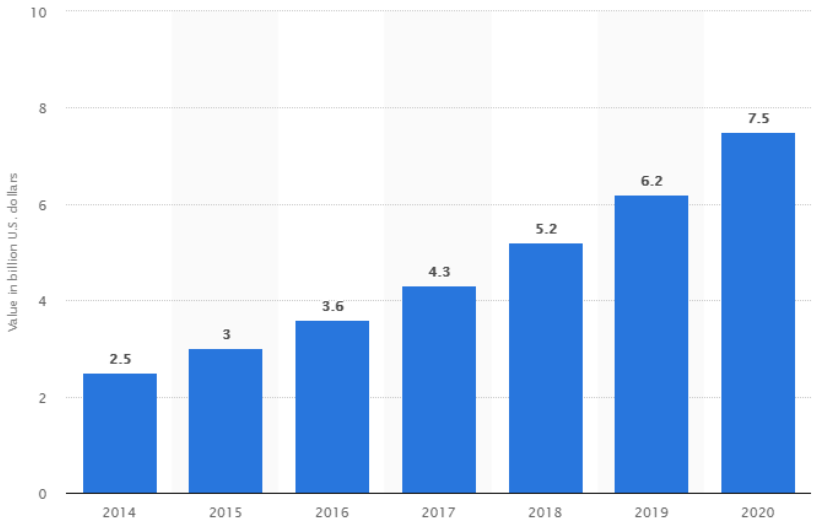

Figura nr. 7. Valorile estimate ale primelor subscrise pentru asigurările de risc cibernetic 2014-2020 (miliarde USD)
Sursa: © Statista 2019

Conform *Raportului privind analiza tematică referitoare la asigurarea de risc cibernetic*[10], elaborat de către A.S.F., riscurile cibernetice sunt în responsabilitatea atât a managementului instituțiilor și companiilor, cât și la nivel de angajați, asigurările cibernetice putând acoperi și riscurile profesionale generate de riscurile cibernetice.

Majoritatea politicilor de asigurare a proprietății acoperă pagubele fizice (chiar dacă întreruperea activității este în mod constant o parte din partea de proprietate comercială) și în general exclude riscul cibernetic. La nivel mondial mai puțin de 10% dintre companii sunt considerate a fi achiziționat astăzi produse de asigurări cibernetice. În România nu avem informații.

Asigurarea este un instrument care completează (și nu înlocuiește) cadrul de gestionare a riscurilor pe care fiecare organizație ar trebui să îl aibă și, prin urmare, este relevant deoarece[11]:

- În fiecare zi, organizațiile se luptă împotriva riscului, concentrându-se asupra frecvenței (evitând un incident) prin prevenirea și securitatea cibernetică (CISO, CERT etc.)
- În cazul în care atacul are succes și impactul este amplu, consecințele financiare pot fi uriașe, iar repercusiunile politice / sociale/ destabilizarea politică / invazia militară sunt ușurate dacă infrastructurile cheie devin nefuncționale (energia, telecomunicațiile, băncile, administrațiile publice, transportul, infrastructuri etc.)
- Asigurarea informatică există pentru a îmbunătăți rezistența organizațiilor prin sprijin financiar.

Accenture în 2018[12] a prezentat propria analiză asupra costurilor medii ale criminalității informatice, observând că investițiile în securitatea informatică au un impact

[10] [11] https://asfromania.ro/files/analize/Asigurari_risc_cibernetic.pdf
[12] Cost of cyber crime study, pag. 12, 17, Accenture, 2017

pozitiv major (fig. 8) și corelația dintre costul anual al criminalității cibernetice și dimensiunea organizațională a companiilor afectate (fig. 9).

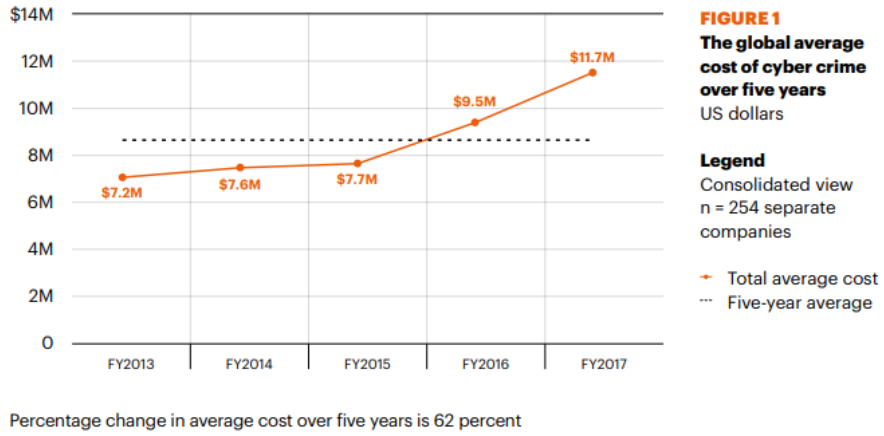

Figura nr. 8. Costul mediu global al criminalității cibernetice în perioada 2013 – 2017
Sursa: Accenture, 2018

De asemenea, compania Accenture ne prezintă, la nivelul anului 2017, o evoluție a costului anual al criminalității cibernetice în funcție de mărimea firmelor afectate din SUA cu un vârf de pierderi de peste 75 milioane dolari SUA pentru companii mari. Regresia acestor înregistrări ne indică, în medie, un vârf de peste 25 milioane dolari SUA pentru firme foarte mari.

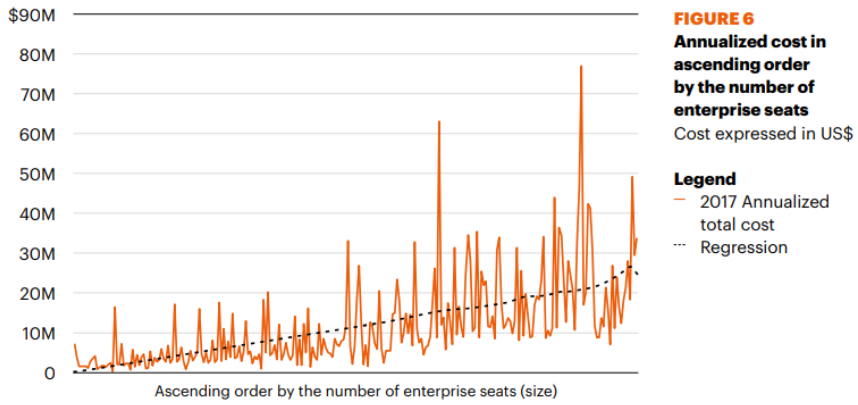

Figura nr. 9. Corelația dintre costul anual al criminalității cibernetice și dimensiunea organizațională a companiilor afectate
Sursa: Accenture, 2018

3. Asigurarea riscurilor cibernetice are trei provocări principale[13]:

- Lipsa previzibilității pierderilor cibernetice. Expunerile sunt în mare parte imprevizibile nu numai din cauza lipsei de date statistice din trecut, dar mai mult din cauza dinamicii criminalității cibernetice și a riscurilor asociate care complică evaluarea acestora.
- Asimetria informațională. Selecția adversă este aproape inevitabilă, organizații care au luat asigurare de risc cibernetic au experimentat incidente cibernetice înainte de a cumpăra asigurarea. Lipsa datelor privind pierderile afectează clasificarea riscului deținătorilor de polițe de asigurare.
- Limitele de acoperire. Politicile tind să acopere doar pierderi maxime limitate (10-500 milioane USD, vezi, Biener, Eling, Matt și Wirfs, 2015; Finkle, 2015), și conțin mai multe excluderi (de exemplu, pierderi provocate de sine, accesarea site-urilor nesigure sau a terorismului). Potenţialele scenarii extreme (uneori numite "Cybergeddon") nu pot fi acoperite de polița de asigurare. În plus, ar putea fi indirect neacoperite efectele pierderilor cibernetice care nu pot fi măsurate (de exemplu, pierderile de reputație și impactul acestora privind prețurile acțiunilor). Un alt aspect problematic al acoperirii este complexitatea poliței. Având în vedere numărul de excluderi și natura dinamică a riscului cibernetic, există incertitudine cu privire la ceea ce polița de risc cibernetic acoperă de fapt, incertitudine asupra terminologiei convenite, situație care face ofertele de asigurări foarte greu de comparat.

Deloitte[14] a prezentat cercul vicios al asigurărilor cibernetice (fig. 10) care pune accentul pe faptul că lipsa datelor istorice este, probabil, provocarea fundamentală și contribuie la strângerea limitele de acoperire pe pieţele de asigurări cibernetice și apariția de excluderi, cum ar fi pierderile de la accesarea site-urilor nesigure sau a terorismului. Unele efecte indirecte ale incidentelor cibernetice nu pot fi măsurate și, ca rezultat, nu sunt acoperite (de exemplu daunele reputaționale)[15].

[13] Ten Key Questions on Cyber Risk and Cyber Risk Insurance**,** Geneva Association, nov 2016
[14] Demystifying cyber insurance coverage: Clearing obstacles in a problematic but promising growth market, Deloitte, 2017
[15] Understanding and Addressing Global Insurance Protection Gaps, Geneva Association, aprilie 2018

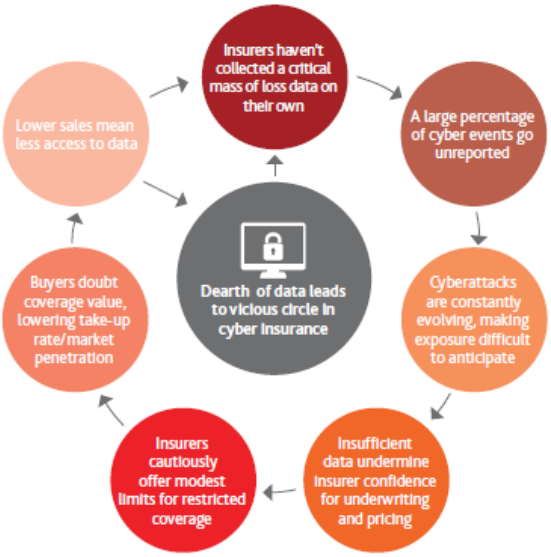

Figura nr. 10. Cercul vicios al asigurărilor cibernetice
Sursa: Deloitte, 2017

Cu toate aceste neajunsuri există deja produse de *asigurare cibernetică globală oferite la nivel internațional și adaptate profilului de risc al companiei client. Acestea permit companiilor să beneficieze de o protecție completă împotriva criminalității cibernetice și a altor incidente cibernetice, indirecte sau externe, rău intenționate sau accidentale.*

4. Cele mai importante 5 abordări la nivel global pentru astfel de produse, ar fi:

1. abordarea de sprijinire a clienților cu nevoi de asigurare cibernetică, oferind instrumente de prevenire a pierderilor informatice și servicii orientate spre recâștigarea stabilității în urma unor atacuri cibernetice.
2 abordarea unei zone estinse prin introducerea în mod specific a cazurilor de eșec uman sau neglijență a angajaților, deci nu doar asigurări cibernetice de afaceri, dar asigurare în mod individual. Unele domenii cheie din această acoperire includ pagubele produse de hackeri, furtul cibernetic, ingineria socială, extorcarea cibernetică și răspunderea pentru mass-media on-line.
3. abordarea analizării gradului în care un client gestionează riscul. Această evaluare cantitativă utilizează modele statistice care sunt apoi aplicate procesului de subscriere. Recunoscând o temă a organizațiilor care se concentrează în întregime pe evitarea încălcărilor, în general, se urmărește o abordare pe care întreprinderile o doresc, personalizată calculând cele mai mari riscuri cibernetice care se confruntă cu o anumită țintă și construind o politică în consecință.
4. abordarea integrată cu managementul tehnologic clarifică faptul că tehnologia și, mai precis, cyber-space ul au creat o forma de asigurare cu totul nouă. Recunoscând modul în care tehnologia acum pătrunde în societate, se remarcă nivelul ridicat al riscului pe care îl aduce acest lucru. Abordarea a fost formulată pentru a privi dincolo de protecția financiara,

oferind de asemenea o capacitate de consultanță in spațiul cibernetic. De fapt sprijinul acordat de experți în acest domeniu poate ajuta, clienții să-și îmbunătățească siguranța. Există platforme care oferă acces la zeci de asiguratori de risc cibernetici . Folosind această armadă de asistență, se propun, de asemenea, politici de asigurare cibernetică adaptate clienților individuali și propriului lor profil de risc specific.

5. abordarea din perspectiva complexității amenințărilor cibernetice. Protecția de confidențialitate este o zonă centrală de interes, furnizând acoperirea riscului de reputație, o zonă crucială din cauza creșterii frecvenței și gravității încălcărilor privind protecția datelor. Sunt luați în considerare factori precum costurile medico-legale și costurile de monitorizare a creditelor și cheltuielile de PR.

În ciuda numeroaselor provocări la adresa asigurării riscului cibernetic, aceste exemple dovedesc că există, modele de risc și seturi de date relevante ce se îmbunătățesc continuu. Noii jucători vor crește capacitatea pieței, iar concurența se va intensifica.

Swiss Re se așteaptă să crească brusc asigurarea globală de risc cibernetic la 18 miliarde USD până în 2025; totuși, aceasta ar fi în continuare mai mică de 1% din piața globală de asigurări generale. 99% din pagubele provocate de incidente cibernetice rămân neasigurate.

Nu în ultimul rând, problema fundamentală a asigurării cibernetice poate fi abordată de către parteneriate public-privat pentru a dezvolta din perspectiva riscurilor cibernetice un parteneriat comercial robust.

5. Asigurarea riscurilor cibernetice este un subiect important pentru autorități[16] cel puțin din următoarele 6 motive:

1. Este un element de stabilitate economică, socială și politică, atât pentru infrastructurile critice, guvernamentale, cât și pentru cele comerciale și personale, inclusiv pentru sectorul financiar și ar trebui să fie utilizat în evaluarea solidității/sănătății financiare și a susținerii activității prin recuperarea rapidă a pierderilor și continuarea activității[17]
2. Poate fi un element al securității naționale (să susțină activitatea instituțiilor de profil – SRI, MAPN, etc)
3. Este benefic pentru societate, deoarece pretențiile legate de confidențialitatea datelor (adică pierderea datelor clientului de către un operator de telecomunicații, în sistemul medical, cel de protecție socială, în sistemul bancar și nebancar etc.) vor avea un impact asupra vieții tuturor cetățenilor. Capacitatea de despăgubire rapidă, cu sprijinul financiar al unui asigurător, este o garanție că aceste crize generate de producerea riscului nu va genera unele tulburări în rândul populației timp de luni de zile.
4. Riscurile cibernetice nu pot fi eliminate oricât s-ar investi, atacatorii fiind înaintea soluțiilor tehnice de remediere. Poate fi acoperit financiar prin sistemul de asigurări, doar un risc rezidual major pentru evitarea răspunderii atât financiare a instituțiilor/companiilor (care pot determina chiar incapacitate de plată), cât și personale, sociale, sau chiar penale.
5. Tendințele și interdependențele tehnologice vor aduce noi riscuri cibernetice majore prin interconectarea caselor, a vieții curente prin sisteme inteligente (IoT), inteligență artificială, robotică etc.

[16] Navigating through Cyber Risk, Thomas MARCADET, mai 2018, prezentare Marsh
[17] https://asfromania.ro/files/analize/Asigurari_risc_cibernetic.pdf

6. În prezent instituțiile de rating[18] și autoritățile cer măsuri concrete de eliminare a riscurilor cibernetice, solicitând aplicarea de reglementări, standarde, audituri, care se completează natural cu asigurarea pe zonele în care vulnerabilitățile nu pot fi acoperite tehnic. Unul dintre cele mai importante acte legislative adoptate în domeniul securității cibernetice la nivel european este „Directiva pentru securitatea rețelelor și a sistemelor informatice" (NIS Directive 2016/1148)[19] a Parlamentului European, care stabilește măsuri în vederea obținerii unui nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în cadrul Uniunii, astfel încât să se îmbunătățească funcționarea pieței interne. Această directivă solicită măsuri concrete la nivelul infrastructurilor critice dar nu numai, reglementările alocând responsabilitatea către factorii de răspundere și către instituții/companii.

***Calendarul de implementare al Directivei NIS este următorul*:**

August 2016	–	Intrarea în vigoare a Directivei
Februarie 2017	6 luni	Grupul de cooperare își începe activitățile
August 2017	12 luni	Comisia Europeană adoptă actele de punere în aplicare a cerințelor de securitate și notificare pentru furnizorii de servicii digitale
Februarie 2018	18 luni	Grupul de cooperare stabilește programul de lucru
9 Mai 2018	21 de luni	Transpunerea Directivei NIS în legislația națională
Noiembrie 2018	27 de luni	Statele membre vor identifica operatorii de servicii esențiale
Mai 2019	33 de luni (1 an de la transpunere)	Raportul Comisiei Europene
Mai 2021	57 de luni (3 ani de la transpunere)	Revizuire de către Comisia Europeană

Evoluția amenințărilor cibernetice va crește în frecvență și în sofisticare. Instituțiile/companiile au nevoie de o strategie cuprinzătoare de management al riscului cibernetic – strategie bazată pe modelarea riscurilor economice, pe securitate cibernetică optimizată, pe programe de asigurare cibernetică robustă și pe capabilități de reacție eficace și care să răspundă în timp util și eficient, menținând întreruperile la minimum și asigurând revenirea la operațiunile normale cât mai repede posibil, cu costuri cât mai reduse[20].

În general despre riscurile cibernetice se discută tehnic, cu noțiuni specializate domeniului IT, dar acest subiect deja transcende acest domeniu și este transpus în domeniul afacerilor, al economiei sociale, a modelării matematice și statistice, a managementului datelor, a teoriilor incertitudinii, a managementului riscurilor, (de exemplu, Maillart și Sornette 2010; Biener, Eling și Wirfs, 2015). Aceste noțiuni privesc domeniul complexității

[18] Cyber Risk And Corporate Credit – June 9, 2015, WWW.STANDARDANDPOORS.COM/RATINGSDIRECT
[19] https://eur-lex.europa.eu/legal-content/RO/TXT/?qid=1479977104870&uri=CELEX:32016L1148
[20] WannaCry: Lessons learned following ransomware attack, Jean Bayon de La Tour, Marsh

și a structurilor de risc dependente (de exemplu, Hofmann și Ramaj, 2011; Ögüt, Raghunathan și Menon, 2011) sau domeniul selecție adversă și al problemelor de hazard moral (de exemplu, Gordon, Loeb și Sohail, 2003), domeniul infrastructurilor critice (de ex Forum economic, 2010; Ruffle și colab., 2014; Lloyd's, 2015b; Long Finance, 2015). Studiile existente confirmă provocările în gestionarea riscurilor și a asigurării riscurilor cibernetice.[4]

Conform Asociației de la Geneva, prin documentul *Ten Key Questions on Cyber Risk and Cyber Risk Insurance*[4], s-a constat că:

- *O cădere globală al internetului este puțin probabilă, dar căderi limitate la nivel regional au avut deja loc; având în vedere conexiunea la nivel global între economie și societate, identificăm consecințe potențiale masive ale unor scenarii extreme privind companiile și persoanele fizice. Același lucru este valabil și pentru alte scenarii cibernetice, cum ar fi, de exemplu, blocarea sistemelor energetice. Pentru asiguratori, astfel de scenarii reprezintă un risc de acumulare putând inhiba asigurarea la nivel general,* dacă nu se aplică metode hibride de analiză.
- *Piața asigurărilor cibernetice este în prezent mică în comparație cu alte linii de afaceri, dar este de așteptat să crească semnificativ în următorii ani. Statele Unite ale Americii sunt înaintea Europei și a Asiei, de exemplu, în ceea ce privește cerințele de raportare. Principalele probleme ale extinderii acestor asigurări sunt lipsa datelor, riscul de schimbare, riscul de acumulare și potențialele probleme generate de hazardul moral.*
- *Datele privind riscul cibernetic sunt foarte puține, deoarece victimele sunt reticente să raporteze astfel de evenimente. Cele mai multe lucrări empirice privind riscul cibernetic se bazează pe informații privind pierderea datelor (nu pierderea de informații), dar recent s-au constituit primele baze de date cu pierderi (NetDiligence (2014) în SUA, Biener et al. (2015) la nivel global).*
- *Industria de asigurări ar trebui: să dezvolte standarde, taxonomii și bune practici comune ; să dezvolte analize de scenarii; să inițieze și / sau intensifice dialogul cu părțile interesate; să urmărească dezvoltările tehnologice (cloud computing, Internet of Things, blockchain etc.), să crească propriile abilități analitice (criminalistică digitală) și să facă propriul IT mai rezistent, să susțină concret asigurarea cibernetică fie prin dezvoltarea de baze de date anonime de (re) asigurare și dezvoltarea de noi politici*, fie prin stabilirea de noi modele și abordări pe bază de consultanță și evaluare
- *Modelarea frecvenței și severității riscului cibernetic poate fi făcută prin aplicarea teoria valorilor extreme și abordarea vârfurilor peste limită. Au fost propuse distribuții, legea puterii sau distribuția log-normală pentru severitate și distribuția binomială negativă pentru frecvență. Agregarea riscului cibernetic trebuie să ia în considerare dependența neliniară. Analiza de scenarii este un instrument popular în astfel de situații.*
- *Pentru a preveni riscurile cibernetice trebuie să se intensifice combaterea criminalității informatice prin colaborare internațională, să se inițieze dialoguri globale și convenții care vizează limitarea războiului cibernetic, să se stimuleze reziliența sistemelor IT, să se introducă cerințe de raportare, sprijinirea dezvoltării bazelor de date cu incidente cibernetice și elaborarea de standarde minime pentru atenuarea riscurilor.*
- *Pentru susținerea asigurării cibernetice se recomandă a se stabili parteneriate public-privat cu guvernul în calitate de asigurător de ultimă instanță (asigurare guvernamentală pentru scenarii extreme); a se stimula dezvoltarea de baze de date anonimizate, stimularea dezvoltării mecanismelor tradiționale și alternative de transfer de risc*

Cu toate acestea, Maillart și Sornette (2010) au investigat încălcări ale datelor cu caracter personal, cum ar fi cărțile de credit, numere de securitate socială, conturi bancare

sau dosare medicale. Ei găsesc o creștere exponențială a frecvenței acestor incidente (rata evenimentelor) pentru perioada 2001 - 2006 (fig. 11). Referitor la funcția de distribuție ilustrată în Figura 11, punctele violete sunt observațiile înainte de 2006, iar puncte albastre observațiile după acea dată. In timp ce încălcările datelor cu caracter personal sunt doar un tip de risc cibernetic autorii susțin că aceste constatări sunt reprezentative pentru alte tipuri de riscuri cibernetice provin din Internet[21].

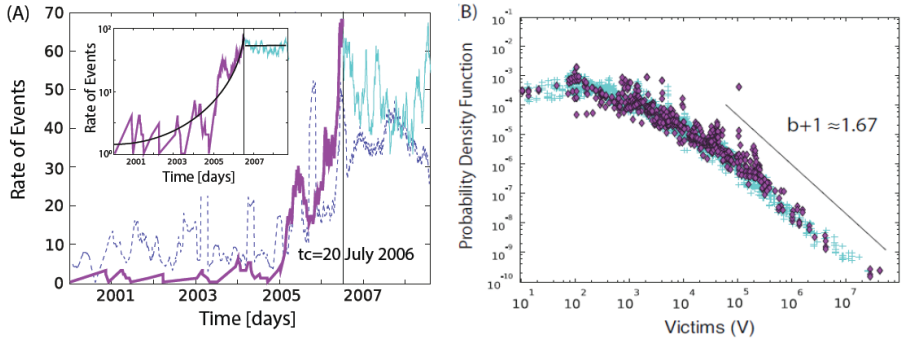

Figura nr. 11. Distribuția severității și a frecvenței
Sursa: Maillart și Sornette, 2010

Cercetarea în domeniul asigurărilor de risc cibernetic cuprinde două aspecte conform Geneva Association[4]:

- Perspectiva micro: cercetări pe partea cererii (de ex. percepția riscurilor, fatalismul); analiza asigurabilităţii și a modalităților de îmbunătățire a asigurabilității (în special cercetarea empirică, de exemplu, generarea de date, analiza datelor); analiza managementului optim al riscului (atenuarea vs asigurare) și nevoia capital necesar pentru a acoperi riscurile cibernetice.
- Perspectiva macro: analize de scenarii pentru măsurarea și de gestionarea riscului de acumulare, dacă companiile de asigurări pot înregistra un risc sistemic cu asigurarea riscurilor cibernetice, actorii implicați să devină parte a dialogului global. În lipsa datelor, analizele trebuie realizate mai mult din perspectivă tehnică decât statistică.

În mod deosebit în scopuri de asigurare, un simplu număr de încălcări nu este suficient pentru calcularea primelor, a capitalului sau a rezervelor de capital. În schimb, un indicator de preț corespunzător potențialei cereri de despăgubire trebuie să fie alocat fiecărei încălcări a securității. În cele din urmă, măsuri clasice de risc bazate pe medie și varianță nu sunt aplicabile și meritele diversificării ar putea dispărea datorită momentelor infinite care caracterizează riscurile cibernetice (vezi Chavez-Demoulin et al., 2006).

6. Riscul cibernetic trebuie gestionat din mai multe perspective.

Procesul clasic de gestionare a riscului constă în cinci etape:

1. definirea obiectivelor,

[21] National Vulnerability Database (by NIST)- Collects software vulnerabilities for the U.S., used by Maillart and Sornette; 2010

2. identificarea riscurilor,
3. evaluare /analiză,
4. gestionarea efectivă a riscurilor (evitarea, atenuare, transfer, retenție)
5. monitorizarea de risc.

Agenția NIST a SUA propune cadrul de lucru descris în figura 12.

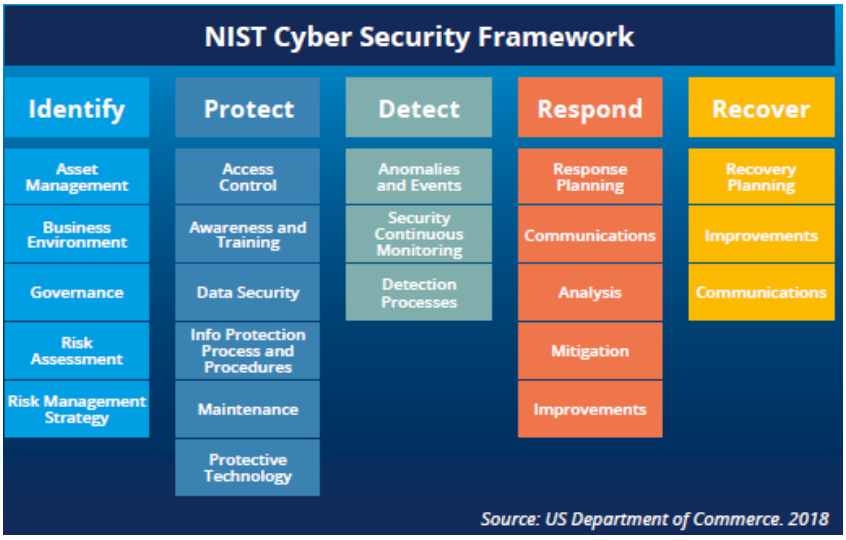

Figura nr. 12. Cadrul securității cibernetice
Sursa: US Department of Commerce, 2018

În fiecare etapă a procesului de management clasic al riscurilor, riscurile cibernetice prezintă caracteristici speciale, de exemplu managementul riscului cibernetic nu este responsabilitatea departamentului IT, dar este necesar un dialog de-a lungul companiei referitoare la acest risc (de exemplu, sensibilizare, instruire etc). Subiectul ar trebui, de asemenea, să fie încorporat în responsabilitățile conducerii de top, de nivel C[22]. Deja angajamentul instituțional - demonstrat prin desemnarea unei persoane responsabile de securitatea informațiilor – este esențial pentru o gestionare reușită a categoriei de riscuri.

De exemplu, firmele care au deja un ofițer de securitate informatică (CISO) sau o poziție similară, au o medie mai mică de evenimente când se produce riscul, înregistrându-se o pierdere de 157 USD / înregistrare vs. 236 USD per înregistrare pentru firmele fără conducere de securitate strategică (vezi Shackelford, 2012).

Accenture (2019) stabilește o ierarhie a principalelor patru activități de apărare[23] contra riscurilor cibernetice (fig. 13).

[22] The step down of Target's CEO following a massive data breach in 2014 exemplifies that the top management might be held accountable for cyber incidents (http://www.forbes.com/sites/greatspeculations/2014/05/08/targets-ceo-steps-down-following-the-massive-data-breach-andcanadian- debacle/#799cf7283f56).
[23] Cost of cyber crime study, pag. 30, Accenture, 2017

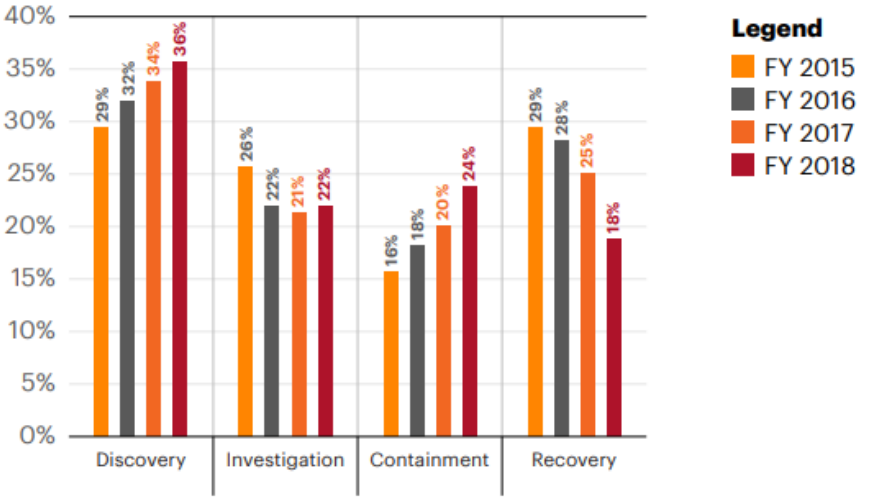

Figura nr. 13. Ponderea a patru activități de apărare contra riscurilor cibernetice
Sursa: Accenture, 2019

Primul pas în procesul de gestionare a riscurilor îl reprezintă definirea situației inițiale și a obiectivelor managementului riscului cibernetic. Până acum, există o multitudine de standarde, în special din domeniul tehnologiei informației, care pot servi ca șabloane pentru managementul riscului cibernetic, de exemplu, familia ISO / IEC 2700x, standardele BSI-IT-Grundschutz (BSI, 2008) sau Cyber Security Best Practices (Allianz, 2011). Există și posibilitatea de a certifica respectarea acestor standarde. De exemplu U.K.'s Department for Business, Innovation & Skills and Cabinet Office (2014) definește, în așa-numitul Cyber Essentials, un standard de securitate IT și o certificarea a implementării sale[24].

Partenerii de afaceri și clienții cer tot mai mult companiilor să verifice că îndeplinesc anumite standarde minime de securitate IT. Pentru asigurarea cibernetică asiguratorii ar trebui să se bazeze pe evaluări similare. Companiile care solicită acoperirea cibernetică ar avea nevoie să aibă astfel de certificate iar asigurătorul ar trebui să efectueze o evaluare similară a riscurilor[25]. Asigurătorii vor trebui să intre în zona de consultanță pre-evaluare, în vederea estimării riscurilor cibernetice și emiterea polițelor.

În acest sens, pentru identificarea riscului:

- Trebuie stabilite procesele de afaceri care sunt relevante pentru riscul cibernetic cu activele și valoarea lor corespunzătoare. După aceea, amenințările potențiale, tipul lor și sursele trebuie să fie determinate. O listă detaliată a amenințărilor curente se regăsesc în standardul ISO / IEC 27005.

[24] This certificate is required for companies in order to be admitted for public procurements. A similar framework is in place in Japan and a proprietary framework specifically tailored for the needs of SMEs is provided by VdS (2015)..

[25] ACGS (2014) analyses cyber risk management with the Business Model Canvas and the House of IT Quality.

- Trebuie să se colecteze date despre punctele slabe, întotdeauna în conexiune cu activele, amenințările și metodele de protecție deja existente. Un prim potențial indicator pentru identificarea riscului poate fi asigurat de auto-evaluarea de risc cibernetic; de exemplu metode propuse de companii specializate in distribuția unor astfel de asigurări[26]. Aceste instrumente pot ajuta la determinarea expunerii la risc și gradul de conștientizare a riscului de companie și să furnizeze indicații pentru riscurile încă neidentificate. Un alt aspect ar fi cum un atac cibernetic poate fi detectat cât mai repede posibil de la momentul când s-a întâmplat. Un instrument pentru analiza consecințelor asupra operațiunilor este analiza impactului asupra afacerii (BIA).

Pentru gestionarea efectivă a riscurilor există patru opțiuni:

a) evitarea riscurilor,
b) reducerea riscului / atenuarea,
c) transferul de risc
d) auto-asigurarea.

Evitarea riscurilor ar însemna că stocarea electronică a informațiilor și restricționarea utilizării sistemelor informatice. În lumea de astăzi, acest lucru este greu de imaginat. Reducerea riscului și atenuarea sunt mai eficiente. Acestea sunt instrumente pentru a reduce probabilitatea apariției (de ex. software anti-virus, firewall-uri etc.) sau care diminuează dimensiunea pierderilor (de exemplu, planuri de recuperare în caz de dezastru)[27] .

În general, transferul de risc este posibil prin cumpărare a unui contract de asigurare. Cu toate acestea, piața de asigurare cibernetică se dezvoltă, gama de produse va crește și o acoperire suficientă va deveni viabilă. Este deosebit de importantă și combinația dintre reducerea / atenuarea și transferul riscurilor. Un asigurător va emite polița dacă pentru reducerea / atenuarea riscurilor au fost instituite măsuri adecvate și asigurătorul a putut verifica situația eficienței acestor instrumente în evaluările inițiale. Prin urmare, evaluările în avans și interviurile, sau consultanța acordată direct de către asigurator, sunt necesare înainte de a semna un contract de asigurare. Aceste evaluări vor contribui, de asemenea, la creșterea gradului de conștientizare a riscului cibernetic.

În caz de auto-asigurare, compania decide să plătească pierderile pe cont propriu. În acest caz, capitalul firmei trebuie să servească drept tampon de siguranță și trebuie alocat în avans. Pe lângă acumularea capitalului propriu, trebuie stabilite planuri de urgență și de gestionare a crizelor.

Putem obține următoarele linii directoare pentru managementul riscului cibernetic de către companii (vezi, de asemenea, Biener, Eling, Matt și Wirfs, 2015): angajament instituțional, gestionarea efectivă a crizelor, dialogul despre riscuri cu toți angajații, dialogul despre riscuri cu clienții și furnizorii, certificarea, monitorizare continuă, transferul de risc prin asigurare ca singurul mijloc eficient de transferare a riscului cibernetic.

[26] http://www.marsh-stresstest.eu/.

[27] See CIS (2016) or ASD (2014) for guidance on how IT security measures, such as access control, authorisation of devices and software, malware defense, and network configuration, should be used.

7. Riscurile identificate trebuie să se regăsească în acoperirile sau excluderile asigurărilor cibernetice.

În general riscurile acoperite prin asigurare de societăți înregistrate în România, conform Raportului A.S.F. privind asigurările de risc cibernetic[28] , sunt:

- răspundere pentru scurgerea de informații, inclusiv pierderea datelor personale colectate;
- costuri generate de scurgerile de informații inclusiv costuri legate de notificări și analiză criminalistică;
- răspundere pentru securitatea rețelelor pentru sisteme compromise, inclusiv cauzate de atacuri DOS;
- răspundere media pentru publicații digitale;
- întreruperea afacerii cauzată de un incident informatic;
- costuri de restaurare a datelor și a aplicațiilor rezultate în urma unui incident de natură să afecteze funcționarea afacerii;
- comunicare de criză pentru reducerea riscului reputațional;
- răspundere pentru plăți electronice, inclusiv amenzi și penalități;
- pierderile generate de furtul de proprietate intelectuală.

Principalele excluderi din asigurare sunt în general:

- Pierderi auto-provocate;
- Acte de terorism;
- Altele: Încălcarea obligațiilor profesionale; Deficiențe ale furnizorilor de servicii; Patent sau secret comercial; Hacking săvârșit de directori sau parteneri; Distrugerea bunurilor corporale; Vătămare corporală; Sechestru și confiscare; Război, terorism și riscuri nucleare; Declarații defăimătoare; Insolventa; Probleme pre-existente; Acte abuzive și penale; Conduită iresponsabilă; Cereri de despăgubire cu privire la răspunderea media formulate de angajați; Amenzi, penalități și sancțiuni; Cereri de despăgubire în afara instanțelor competente.

În cazul producerii unui eveniment asigurat, viteza de reacție a societății de asigurare poate fi de 4 ore de la sesizarea evenimentului.

Tabelul nr. 2 arată diferite exemple de acoperiri prin asigurare de risc cibernetic la nivel internațional ca răspuns la diferitele etape ale atacului cibernetic sau a pierderii de date, din perspectiva FERMA (Federația Asociațiilor Europene pentru Managementul Riscurilor)[29].

[28] https://asfromania.ro/files/analize/Asigurari_risc_cibernetic.pdf
[29] Preparing for Cyber insurance, FERMA, Octombrie 2018

Tabel nr. 2 Acoperiri ale asigurărilor de risc cibernetic aferente atacurilor și a pierderii datelor

Possible actions following a cyber attack or data loss	Examples of cyber coverage components
Investigate what happened	These issues likely require the specialised assistance of forensic investigators. Cyber policies may include coverage for forensic investigation costs following a cyber-attack or data loss.
Deploy technical measures to contain the loss and repair the IT system	
Assess legal/regulatory obligations	Legal services/assistance can be covered by cyber policies for breaches where it is reasonably suspected that confidential information has been compromised, generally in two forms: (i) post incident discovery and assistance in managing a breach (ii) defence costs following a claim alleging a breach of information
Execute a plan to comply with your obligations	
Assess the complaints/legal challenges you receive	
Implement the emergency plan to continue servicing clients	Cyber policies may include coverage for costs incurred as a result of a cybersecurity breach to maintain or restore operations and for income that is lost during the outage period.
Assess the cost of the cyber-attack, including possible loss of turnover	
If you are facing extortion: - Hire a response/threat consultant - Pay ransom, if legally allowed	Cyber policies may include services and costs to investigate and manage an extortion threat, including forensic experts and threat consultants.
If you are facing a regulatory investigation or a legal suit from third parties: - Hire legal advisers; prepare defence strategy - Pay damages	Cyber policies may include coverage for defence costs and damages that are agreed and/or assessed.

Sursa: FERMA 2018

Concluzii

Conform analizei tematice a A.S.F.[30] referitoare la asigurarea de risc cibernetic:

- Riscurile cibernetice sunt în responsabilitatea atât a managementului instituțiilor și companiilor, cât și la nivel de angajați, asigurările cibernetice putând acoperi și riscurile profesionale generate de riscurile cibernetice.
- Instituțiile/companiile au nevoie de o strategie cuprinzătoare de management al riscului cibernetic asigurând revenirea la operațiunile normale cât mai repede posibil, cu costuri cât mai reduse.
- Asigurarea de risc cibernetic poate avea un rol esențial în a prelua/transfera riscurile la care companiile sunt expuse. Aceasta pot fi un instrument care completează (și nu înlocuiește) cadrul de gestionare a riscurilor pe care fiecare organizație ar trebui să îl aibă și ar trebui să fie un element de stabilitate economică și socială, atât pentru infrastructurile critice, guvernamentale, cât și pentru cele comerciale și personale, inclusiv pentru sectorul financiar.
- Asigurarea de risc cibernetic ar trebui să fie utilizată în evaluarea solidității/sănătății financiare și a susținerii activității prin recuperarea rapidă a pierderilor și continuarea activității.

Având în vedere cele de mai sus, pentru atingerea obiectivului de acoperire și a riscurilor generate de societatea digitală, se relevă următoarele concluzii:

[30] https://asfromania.ro/files/analize/Asigurari_risc_cibernetic.pdf

- Pentru susținerea protecției infrastructurilor critice, ale activităților sectorului public, a bunului mers al economiei și a protecției activelor naționale și individuale, cu expunere majoră la riscuri în contextul lumii digitale actuale, este esențială formularea și asumarea de politici și susținerea reglementării acoperirii riscurilor cibernetice prin asigurare, cu mutarea responsabilității financiare către cei care pot plăti pagube de dimensiuni posibil foarte mari prin reducerea impactului politic, social și economic. Aceste politici vor avea efecte benefice atât la nivelul cererii[31], cât și al ofertei.
- Pentru a asigura pe termen lung seriile de date necesare activității actuariale ale asigurătorilor, este necesară instituirea unui sistem de raportare a pierderilor generate de riscurile cibernetice, cel puțin pentru infrastructurile critice și importante,
- Pentru asigurarea dezvoltării produselor de asigurare specifice, pe termen scurt-mediu, este nevoie să se dezvolte și utilizeze de către asigurători a unor modele de consultanță și evaluare pentru clienții care doresc să se asigure împotriva amenințărilor cibernetice, pe baza de standarde și certificări recunoscute la nivel mondial, și dezvoltarea competențelor necesare la nivelul asigurătorilor referitor la ingineria acestor riscuri.
- Riscurile cibernetice impun realizarea unui front comun al beneficiarilor, al companiilor tehnologice și al asiguratorilor pentru a crește nivelul maturității informatice și a securității cibernetice, a aplicării principiilor de management al riscurilor, implementarea de mecanisme comune de luptă împotriva criminalității cibernetice și dezvoltarea de produse de asigurări specifice nevoilor clienților.

Bibliografie

[1] Geneva Association - Understanding and Addressing Global Insurance Protection Gaps, aprilie 2018;

[2] CERT-RO - Raport privind evoluția amenințărilor cibernetice în 2017, aprilie 2018;

[3] Demystifying cyber insurance coverage: Clearing obstacles in a problematic but promising growth market, Deloitte, 2017

[4] WannaCry: Lessons learned following ransomware attack, Jean Bayon de La Tour, Marsh;

[5] Thomas MARCADET - Navigating through Cyber Risk, , mai 2018, prezentare Marsh;

[6] www.standardandpoors.com - Cyber Risk And Corporate Credit – June 9, 2015,;

[7] ACGS (2014)- Analyses cyber risk management with the Business Model Canvas and the House of IT Quality;

[8] Ten Key Questions on Cyber Risk and Cyber Risk Insurance, Geneva Association, nov 2016,

[31] Interviu Leonardo Badea, Președintele A.S.F.: https://www.ziarulprofit.ro/index.php/semnal-de-alarma-tras-de-presedintele-asf-asigurarea-riscului-cibernetic-o-mare-provocare-cu-care-se-confrunta-economiile-moderne/

[9] Navigating through Cyber Risk, Thomas MARCADET, mai 2018, prezentare Marsh

[10] Cyber Risk And Corporate Credit – June 9, 2015, WWW.STANDARDANDPOORS.COM/RATINGSDIRECT

[11] The step down of Target's CEO following a massive data breach in 2014 exemplifies that the top management might be held accountable for cyber incidents (http://www.forbes.com/sites/greatspeculations/2014/05/08/targets-ceo-steps-down-following-the-massive-data-breach-andcanadian-debacle/#799cf7283f56).

[12] ACGS (2014) analyses cyber risk management with the Business Model Canvas and the House of IT Quality.

[13] http://www.marsh-stresstest.eu/.

[14] CIS (2016) or ASD (2014) for guidance on how IT security measures, such as access control, authorisation of devices and software, malware defense, and network configuration, should be used.

[15] National Vulnerability Database (by NIST), USA- Collects software vulnerabilities for the U.S., used by Maillart and Sornette; 2010

[16] Cost of cyber crime study, pag. 12, 17, 30, Accenture, 2017

[17] Preparing for Cyber insurance(ppt), FERMA, Octombrie 2018

[18] Interviu Leonardo Badea, Președintele Autorității de Supraveghere Finnaciară: https://www.ziarulprofit.ro/index.php/semnal-de-alarma-tras-de-presedintele-asf-asigurarea-riscului-cibernetic-o-mare-provocare-cu-care-se-confrunta-economiile-moderne/

[19] https://wol.jw.org/ro/wol/d/r34/lp-m/102012171#h=1

[20] https://asfromania.ro/files/analize/Asigurari_risc_cibernetic.pdf

[21] https://eur-lex.europa.eu/legal-content/RO/TXT/?qid=1479977104870&uri=CELEX:32016L1148

[22] https://www.hackmageddon.com/category/security/cyber-attacks-statistics/

[23] https://www.statista.com/markets/414/topic/461/insurance/