AUTORITATEA DE SUPRAVEGHERE FINANCIARĂ

InsurTech Hub ROMÂNIA

# CYBER INSURANCE


**Călin M. Rangu**

**Director ASF**

**Vicepreședinte**

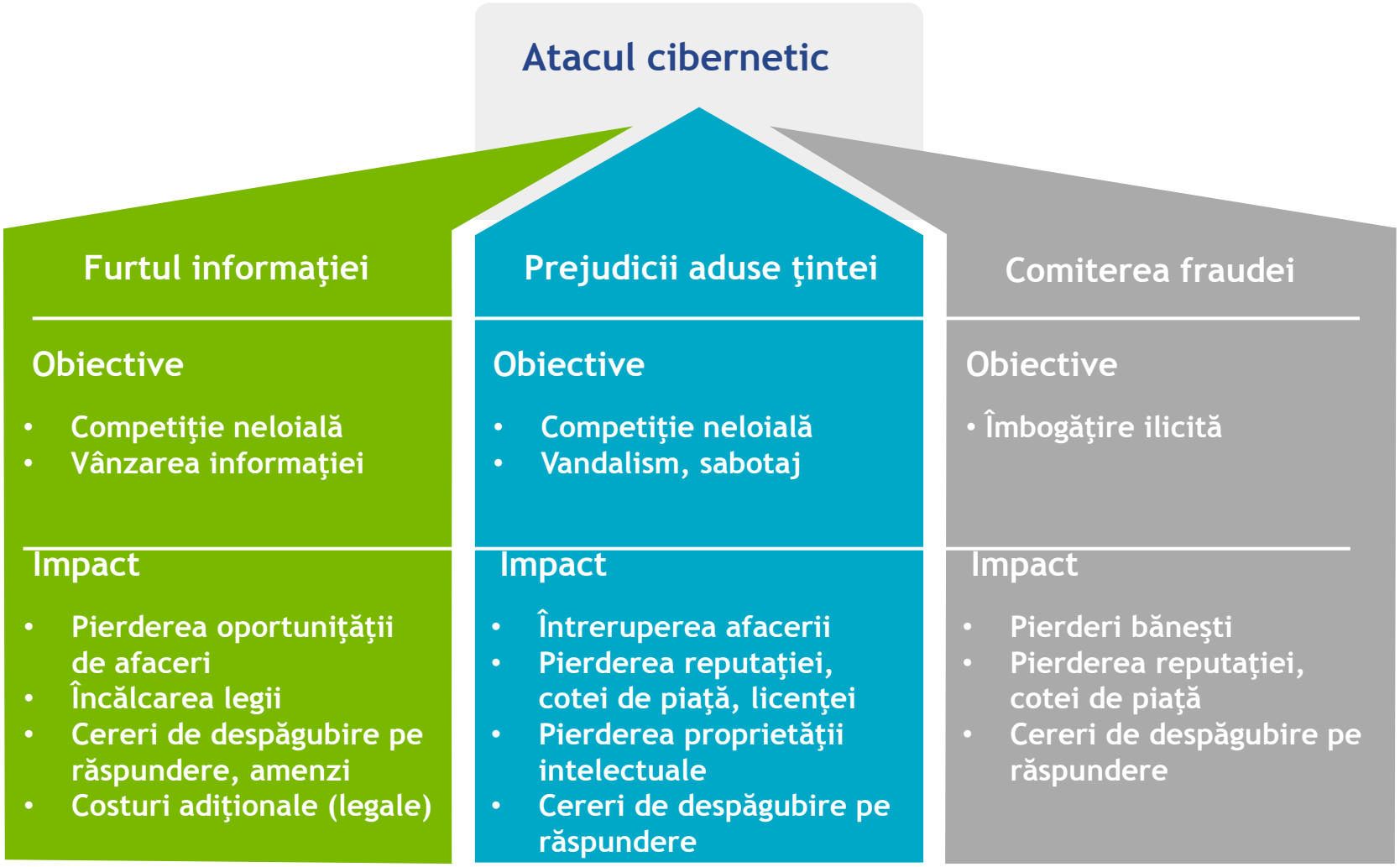
**InsurTech Task Force EIOPA**

# Ce este riscul cibernetic?

**Geneva Association definește Riscul cibernetic**

**orice risc care decurge din utilizarea tehnologiei informațiilor și a comunicațiilor care compromite confidențialitatea, disponibilitatea sau integritatea datelor sau a serviciilor, ducând la întreruperea activităților/afacerilor, întrerupând infrastructurile critice (servicii publice, energie, transport, financiar etc) și afectând oameni și proprietăți.**

# Ce este atacul cibernetic?



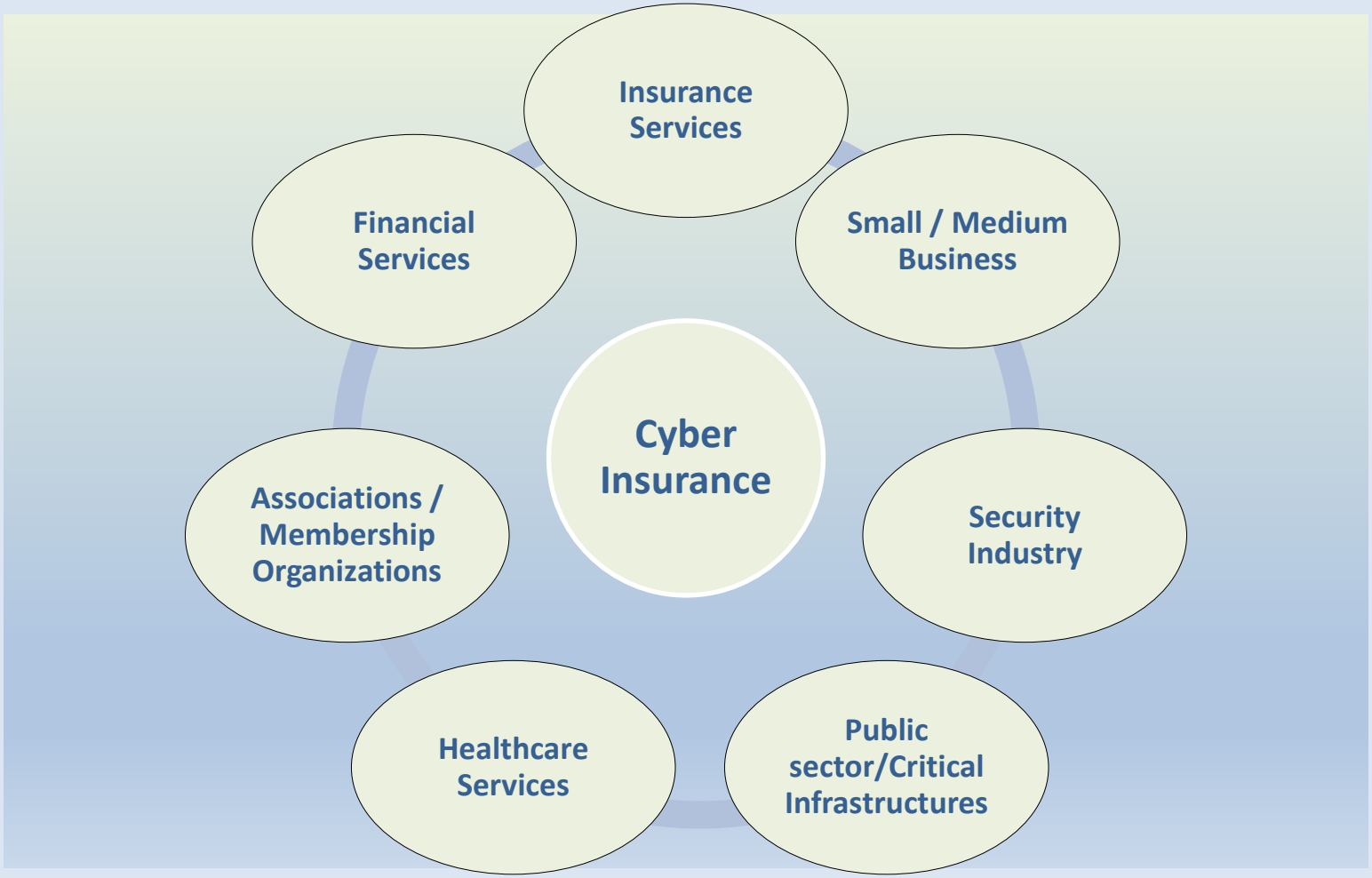

Sursa MARSH BK

# Ce este cyber insurance?

**Asigurarea este un instrument care completează** (și nu înlocuiește) cadrul de gestionare a riscurilor pe care fiecare organizație ar trebui să îl aibă


Cyber Insurance există pentru a îmbunătăți rezistența organizațiilor prin sprijin financiar.

# Pentru cine este cyber insurance?



# De ce cyber insurance?

- În anul 2017 alertele de securitate cibernetică **au crescut cu 25% față de anul 2016**, afectând 33,71% (2,89 de milioane) adrese IP unice din România
- **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 și utilizate de atacatori în diferite tipuri de atacuri (CERT-RO, aprilie 2018)
- 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 (Raport privind evoluția amenințărilor cibernetice în 2017)

# De ce cyber insurance? (2)

**Pentru susținerea**

- **protecției infrastructurilor critice,**
- **activităților sectorului public,**
- **a bunului mers al economiei**
- **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.

# Provocări pentru beneficiari

**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**

- Lipsa datelor privind pierderile afectează clasificarea riscului deținătorilor de polițe de asigurare.

**Limitele de acoperire**

- Politicile tind să acopere doar pierderi maxime limitate și conțin mai multe excluderi (exemplu: pierderi provocate de sine, accesarea site-urilor nesigure sau a terorismului).
- Ar putea fi indirect neacoperite efectele pierderilor cibernetice care nu pot fi măsurate (exemplu: pierderile de reputație și impactul acestora privind prețurile acțiunilor).
- Un alt aspect problematic al acoperirii este complexitatea poliței.
- Incertitudine cu privire la ceea ce polița de risc cibernetic acoperă de fapt, asupra terminologiei convenite, care face ofertele foarte greu de comparat.

# Provocări pentru asigurători

Conform Geneva Association, cercetarea în domeniul cyber insurance cuprinde două aspecte:

**Perspectiva micro**: cercetări pe partea cererii (de ex. percepția riscurilor, fatalismul); analiza managementului optim al riscului (atenuarea vs asigurare) și cât de mult capital este necesar pentru a acoperi riscurile cibernetice.

**Perspectiva macro**: analize de scenarii pentru măsurare și de gestionare a riscului de acumulare. În lipsa datelor, analizele trebuie realizate mai mult din perspectivă tehnică decât statistică.

# Provocări pentru asigurători (2)

Procesul clasic de gestionare a riscului constă în **cinci etape**:

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

# Provocări pentru asigurători (3)

Principalele provocări cu care se confruntă societățile de asigurare din România și care le împiedică să lanseze astfel de produse de asigurare:

- **adaptarea pentru piața locală** a mecanismului de funcționare a acoperirii.
- **lipsa datelor statistice** privind evenimentele, lipsa unor informații minime de evaluare a expunerii și de stabilire a prețului riscului
- **imposibilitatea calculării de acumulări** ale expunerilor
- **lipsa personalului de specialitate**
- **lipsa cererii**
- **lipsa predictibilității evoluției** portofoliului de riscuri
- **lipsa cadrului legislativ specific**
- **lipsă know-how, lipsă date și informații statistice**

# Provocări pentru autorități, nevoia asigurării cibernetice

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 soliditătii/sănătății financiare și a susținerii activității prin recuperarea rapidă a pierderilor și continuarea activității
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 exemplu de către un operator de telecomunicații, de sistemul medical, cel de protecție socială, de către bănci 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 întâmplarea riscului nu va genera unele tulburări în populație** timp de luni de zile.

# Provocări pentru autorități, nevoia asigurării cibernetice (2)

4. Riscurile cibernetice nu pot fi eliminate oricât s-ar investi, atacatorii fiind înaintea soluțiilor tehnice de remediere, va rămâne **un risc rezidual major care poate fi acoperit financiar doar prin sistemul de asigurări**, 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.

6. În prezent **instituțiile de rating 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.

# Provocări pentru companii

- În fiecare etapă a procesului de management clasic al riscurilor, riscurile cibernetice prezintă caracteristici speciale
  - managementul riscului cibernetic **nu este responsabilitatea departamentului IT**,
  - este necesar **un dialog de-a lungul companiei** referitoare la acest risc (de exemplu, sensibilizare, instruire etc).
  - să fie **încorporat la responsabilitățile conducerii de top**, de nivel C .

➢ Firmele care au deja un ofițer de securitate informatică (CISO) sau o poziție similară, au **o medie mai mică a pierderilor când se produce riscul**, înregistrându-se o pierdere de 157 USD / înregistrare vs. 236 USD per înregistrare pentru firmele fără conducere de securitate strategică.

# Provocări pentru companii (2)

- Definirea **situației inițiale** și a **obiectivelor managementului** riscului cibernetic.
- **Aplicarea de standarde** pentru managementul riscului cibernetic, de exemplu, familia ISO / IEC 2700x, standardele BSI-IT-Grundschutz sau Cyber Security Best Practices.
- **Certificarea respectării standardelor**. 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.
- Parteneri de afaceri și clienții cer tot mai mult companiilor să verifice că îndeplinesc anumite standarde minime de securitate IT.
- **Asigurătorii** vor trebui să intre în zona de **consultanță pre-evaluare**, în vederea estimării riscurilor cibernetice și emiterea polițelor.
- 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.

# Linii directoare pentru managementul riscului cibernetic de către companii

- 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

# Concluzii

La nivel european, industria asigurărilor de risc cibernetic se așteaptă la **o creștere progresivă a cererii de astfel de asigurări**, datorată noilor reglementări, creșterea conștientizării riscului și frecvenței crescute a evenimentelor cibernetice.

**Piața de asigurări din România necesită susținere în dezvoltarea produselor de asigurare cibernetică, atât prin politici la nivel național, cât și la nivel sectorial.**

# Mulțumesc!

https://insurtech-hub.asfromania.ro

Întrebări?