KIBERBIZTOSÍTÁSI TRENDEK

Ötvös Gergő (vezető tanácsadó, PwC Magyarország, vállalati kockázatkezelési tanácsadás) gergo.otvos@hu.pwc.com

ÖSSZEFOGLALÓ

A vállalatok és környezetük folyamatos, egyre nagyobb mértékű digitalizációja egyértelmű trend, amely a biztosítási piac számára is új távlatokat nyit, és új biztosítási termékek kialakításának, bevezetésének lehetőségét kínálja. **Ebből adódóan a biztosítási piac egyik leggyorsabban fejlődő ága az új terület veszélyeire fedezetet nyújtó kiberbiztosítások piaca.** A vállalatok egyre inkább beépítik stratégiájukba a kiberbiztonság növelését és az információbiztonsági kockázatok csökkentését. Kutatásunk szerint a maradványkockázatok enyhítésére 59 százalék vesz igénybe valamilyen kiberbiztosítási szolgáltatást.

Az egyik legnagyobb probléma az információbiztonsági piacon, hogy az információbiztonsági kockázatok csökkentésére költött összegek megtérülése (és ezáltal alátámasztása) nehezen számszerűsíthető. Azonban a kiberbiztosításokon keresztül, az azok alapjául szolgáló kockázatfelméréssel és a kapcsolódó biztosítói árazási modellekkel ez jobban megfoghatóvá válik.

SUMMARY

The continuously increasing digitalization level of businesses and their environment is a clear trend that opens new perspectives for the insurance market and offers the business opportunity to design and introduce new insurance products. **Consequently cyber insurance is one of the fastest developing segment of the insurance market.** The growing number of businesses integrate cyber security into their strategies, for example 59% have cyber insurance to mitigate residual risks.

One of the biggest challenges of the information security market is calculating ROI on information security investments. However the risk assessment performed by the insurers and the related cyber insurance pricing models makes it more and more simplified.

Kulcsszavak: kiberbiztonság, biztosítás, információ
Key words: cyber security, insurance, information

JEL: G22, D89

DOI: 10.18530/BK.2016.1.58
http://dx.doi.org/1018530/BK.2016.1.58

A kiberbiztosítás és ami mögötte van[1]

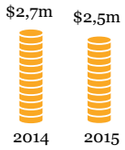
A vállalatok és környezetük folyamatos, egyre nagyobb mértékű digitalizációja egyértelmű trend, amely a biztosítási piac számára is új távlatokat nyit, és új biztosítási termékek kialakításának, bevezetésének lehetőségét kínálja. Az elmúlt években a biztosítótársaságok, felismerve ügyfeleik igényét, alkalmazkodtak a trendekhez, ami elvezetett odáig, hogy a híresség (celebek) hangja és arca mellett mára az adatok és a vállalati rendszerek kiesése is biztosítható. A trend a nemzetközi piac mellett a hazai piacon is érzékelhető, azonban a hazai piacon a kiberbiztosítások még nem terjedtek el széles körűen, mivel a hazai biztosítók egyelőre kockázatosnak tartják. Ennek fő oka a hazai tapasztalatok hiánya a kockázat természetéről, árazási technikájáról, amely faktorokra jelen cikk is fókuszál.

A PwC, mint a világ egyik vezető tanácsadó vállalata, nemcsak a biztosítási piac szereplőivel tartja a folyamatos kapcsolatot, de évente elkészíti az információ- és kiberbiztonság világszintű állapotáról és az aktuális trendekről szóló jelentését Global State of Information Security Survey címen (továbbiakban Security Survey), melynek legújabb – 2016-os – kiadása a közelmúltban jelent meg. Az elmúlt évek biztonsági betörésekről szóló sajtóhírei és a Security Survey felmérése alapján is jól látszik, hogy az információbiztonsági incidensek száma évről évre nő. 2015-ben a növekedés drasztikus, 38 százalékos az előző évhez képest. Nemcsak az incidensek száma, de a szellemi tulajdonhoz, többnyire szabadalmakhoz kapcsolódó adatlopás mértéke is nőtt 56 százalékkal 2015-ben.A növekedés az elmúlt évek alapján és a várható előrejelzések szerint sem fog üteméből veszíteni.

A vállalatok is próbálnak lépést tartani a digitalizáció hatására megváltozott kockázati környezettel, amit jól szemléltet az a tény, hogy a felmérésben részt vevő válaszadók átlagosan 24 százalékkal növelték információbiztonsági kiadásaikat 2015-ben (1. ábra). A megemelkedett költségek hatására az információbiztonsági incidensek által okozott átlagos pénzügyi kár a 2014-es 2,7 millió dollárról 5 százalékkal, 2,5 millió dollárra csökkent az idei évre (2. ábra). A növekvő kiadások mellett fontos kiemelni, hogy a vállalatok, egyre nagyobb jelentőséget tulajdonítva a kiberbiztonságnak, beépítik stratégiájukba a kiberbiztonság növelését és az információbiztonsági kockázatok csökkentését. Jól szemlélteti ezt, hogy a vállalatok 91 százaléka vezetett be kockázatalapú információbiztonsági keretrendszert, **valamint a vállalatok 59 százaléka vásárol kiberbiztonsági szolgáltatást azon kockázatokra, amelyeket nem tud megoldani önerőből** (3. ábra) (PwC, 2015/d.).

A válaszadók átlagosan 24%-kal növelték idén információbiztonsági kiadásaikat

1. ábra - Átlagos információbiztonsági költségkeret



-5%

Az információbiztonsági incidensek által okozott pénzügyi hatás 5%-os csökkenést mutat a tavalyi évhez képest

2. ábra - Biztonsági incidensek átlagos pénzügyi hatása

59% vesz igénybe kiberbiztosítási szolgáltatást

3. ábra - Kiberbiztosítások aránya

Ami nem védhető, az biztosítható

Tapasztalatból tudjuk, hogy a fejlett kiberbiztonsági technológiák nem állítanak, és a technológiák összetettségéből adódóan nem is állíthatnak meg minden kibertámadást, mivel a szintén fejlett technológiákat használó ellenfelek és kiberbűnözők mindig megtalálják a módot a védelmi mechanizmusok megkerülésére, a biztonsági rések kihasználására. A kiberbiztonsági piac – akármennyire is igyekszik – emiatt többnyire reaktívan viselkedik, és ennek következtében, az információbiztonsági piac növekedésével párhuzamosan az ügyfelek egyre gyakrabban vásárolnak kiberbiztosítást az információbiztonsági incidensek káros pénzügyi hatásainak enyhítésére. Sőt mi több, **a kiberbiztosítási szegmens a biztosítási piac egyik leggyorsabban fejlődő része, amely az előrejelzések szerint a 2015-ös 2,5 milliárd dollárról 2020-ra háromszorosára, 7,5 milliárd dollárra duzzad**.

A kiberbűnözéshez kapcsolható pénzügyi kockázatok csökkentése mellett a biztosítást kötő vállalatok mélyebb megértést nyerhetnek az informatikai felkészültségükről és információbiztonsági érettségükről. Ennek oka, hogy a biztosítások megkötésének előfeltétele a jelenlegi

> **A kiberbiztosítási szegmens a biztosítási piac egyik leggyorsabban fejlődő része.**

információbiztonsági képességek és a fennálló kockázatok átfogó helyzetelemzése. Ezek az elemzések segítenek feltárni és megérteni az információbiztonsági kockázatokból adódó szabályozói és törvényi kitettséget, az incidens-válaszidők és a hírnévvesztés lehetséges költségeit.

Számos esetben a kiberbiztosítási csomagokban nem megfelelő az érték- és kockázatmenedzsment aránya. A Canadian Imperial Bank of Commerce (CIBC) évek óta monitorozza és értékeli a kiberbiztosítási piacot: „A mi biztonsági és vállalati biztosításokkal foglalkozó csapatunk évről évre elemzi és felülvizsgálja a kockázatokat a rendelkezésre álló biztosítási csomagok és a kapcsolódó költségek vonatkozásában. Erre alapozva mi nem veszünk igénybe kiberbiztosítási szolgáltatást, mivel még nem teljesen kiforrottak a termékek” – állítja Joe LoBianco, a CIBC információbiztonsági vezetőhelyettese. „A legnagyobb félelmünk a kiberbiztonsági betörésekkel kapcsolatban az ügyfeleink adatainak biztonsága és ezáltal a bankunkba vetett bizalom, amelynek biztosítása nem egyszerű.”

A szervezetek számára további elgondolkodtató tényező a kiberbiztosítás mértékének kiválasztása, mivel az egyéb biztosítási termékekhez hasonlóan természetesen nincs „one-size fits all” megoldás, annak ellenére, hogy a biztonsági kockázatok természete hasonló lehet. „A vállalatoknak meg kell érteniük, hogy nem képesek biztosítást kötni a teljes veszteségükre, mivel a piac még nem készült fel teljesen” – fogalmazta meg Joseph Nocera, a PwC igazgatója. „Vessünk egy pillantást az elmúlt évek legnagyobb információbiztonsági betöréseire; a legnagyobb vállalatok 80-100 millió dollár körüli biztosítást szeretnének kötni, míg a kisebbek megelégednek a 10 millió dolláros biztosítással is. Nincs generális megoldás az olyan egyedi változók miatt, mint az eltérő iparágak, vállalatméret, tárolt adatok típusa, védelmi mechanizmusok érettsége vagy az egyedi kockázatvállalási hajlandóság. Emellett fontos észben tartani, hogy egy biztosítás sem képes megvédeni a vállalat reputációját.”

Biztosítás és kockázat

A kiberbiztosítási termékek fejlesztését és értékelését több tényező nehezíti. A kapcsolódó kockázatok ugyanis a hagyományosan biztosítható kockázatoktól eltérő tulajdonságokkal rendelkeznek. A legfőbbek az események gyakoriságából és a kibervilág összefonódásából adódnak.

1. Gyakori és súlyos

Éves információbiztonsági, IT és üzleti vezetői felmérésünk kimutatta, hogy naponta több mint 100.000 kibertámadás történik világszerte. Az egyes támadások által okozott pénzügyi veszteség bizonyos esetekben eléri a több tízmillió dolláros értéket. A biztosítók sorozatos, komoly ráfizetéses esetekkel nézhetnek szembe, megnehezítve a veszteségek elviselését, illetve a mérleg újjáépítését, hasonlóan egy katasztrófahelyzethez.

2. A veszteség terjedését nehéz feltartóztatni

Az üzleti folyamatok fennakadása és a rendszerek javítása további közvetett veszteségeket okoz, mint például bírságok, jogi költségek és a jó hírnév sérelme. Minden vállalat egyre jobban összefonódó és összefüggő ökoszisztémában működik, melyben nemcsak saját rendszereik és adataik sérülékenyek, hanem a hozzájuk kötődő beszállítók, ügyfelek és stratégiai partnerek adatai, illetve IT rendszerei is. Az „Internet of Things” (IoT) tovább növeli az összekapcsolódás mértékét és a hozzá kapcsolódó sérülékenységet. További kockázat a rendszereket kiszolgáló infrastruktúrákra irányuló támadások.

3. Nehéz a kockázatok észlelése, felmérése és pénzügyi értékelése

Az IT-biztonsági támadások pénzügyi behatásairól csak korlátozott adatok állnak rendelkezésre, ami ezt a kockázatot nehezen értékelhetővé és beárazhatóvá teszi. Míg a rendszerek visszaállítási költségeit meg lehet becsülni a tűz- vagy vízkár utáni helyreállítási adatok alapján, a kibertámadások okozta márkahírnév-veszteségből, a kártérítési kifizetésekből fakadó további veszteségek számszerűsítésére nincs elegendő mennyiségű adat. A bizonytalanságot tovább fokozza, hogy az IT biztonsági betörések természetüknél fogva

hónapokig vagy akár évekig észrevétlenek maradhatnak, így fennáll a veszélye további, akár összeadódó veszteségek realizálódásának.

Ha egy vállalatnak nem kínál önálló kibermódozatot, akkor is fel kell mérnie a szélesebb környezetét, lehetséges üzleti fennakadások, általános veszélyek, hibák és mulasztások után kutatva. Létezhetnek szabályozások, melyek korlátozzák a követelések jogosságát (például a fizikai sérülés szükségessége egy üzleti folyamat megakadásához), de ez a felmérés mindenképpen hasznos és szükséges lehet.

Árképzési megközelítés a kiberbiztosítási piacon

A biztosítók számára kritikus a kifizetések fedezetét biztosítandó megfelelő árképzés. A kiberbiztosítás mint termék újszerűsége és kiforratlansága, valamint a rendelkezésre álló kevés historikus adat miatt, a hagyományos, jól definiálható kockázat-kárérték összefüggéssel szemben kifinomultabb árképzési technikákat, modelleket igényel. A nehézségek ellenére a biztosítók folyamatosan csiszolják, finomítják kockázatalapú árképzési technikájukat, modelljüket, ahogy a biztosítási piac egyre jobban megérti a kiberbiztonsági iparágat.

1. Mennyit veszíthetsz, és mennyi veszteséget engedhetsz meg magadnak?

Az árképzés továbbra is amennyire tudomány, annyira művészet is marad a nagy mennyiségű aktuárius adat nélkül. Ettől függetlenül lehetőség van arra, hogy tisztább képet kapjunk a teljes maximális veszteségről, és ezt összehangoljuk a kockázati étvággyal és a kockázattűréssel. Ez különösen hasznos lehet a biztosítótársaságok döntésében, hogy mely területekre fókuszáljon, mikor és milyen területek lefedésére létezik további lehetőség.

A kulcsadatok tartalmazzák a biztosítási portfólióra vonatkozó „worst case scenario" analízist. Abban az esetben, ha a biztosítótársaság ügyfelei között sok amerikai energiaipari vállalat található, akkor milyen veszteségek származhatnak egy amerikai villamosenergia-hálózat elleni támadásból? Egy friss, „lehetséges, de extrém" eshetőséget felvázoló riport szerint, ha egy igen kifinomult hacker csoport képes volna behatolni az amerikai villamosenergia-hálózatba, olyan károkat tudna okozni, melyekből kifolyólag a biztosítótársaságok 21 és 71 milliárd dollár közötti kárigényekre számíthatnának a támadás méretétől és céljától függően (Lloyd's, 2015/a). Ezeknek az igényeknek mekkora arányáért lenne felelős a biztosító? Milyen lépéseket tudna tenni, hogy csökkentse a veszteségeket, a saját portfóliókockázat koncentrációjának csökkentésétől elkezdve az ügyfélbiztosíték és krízistervezésének javításáig?

2. Tudásfejlesztés

Annak érdekében, hogy a fenyegetettség- és ügyfélsebezhetőség-értékelési rendszereket minél hatékonyabban lehessen kialakítani, válik új emberek bevonása technológiai vállalatoktól és hírszerző ügynökségektől. Az ennek eredményeként létrejött kockázatértékelési, átvilágítási és árképzési folyamat a különböző üzleti és technológiai érintettek együttműködéséhez vezet, akik közösen tudnak koncentrálni az adatokra és informatikai rendszerekre, a vállalatokon belül példaképpen említhető a kockázatkezelési és informatikai vezetők közötti együttműködés.

A biztosítóknak előnyt jelent az elfogadott kockázatokról szóló jobb megértés, és pontosabb árazásra lesz lehetőség.

3. Kockázatalapú kondíciók

Napjainkban sok biztosító mindenre kiterjedő szerződési feltételeket használ. Ennél hatékonyabb megközelítés lehet a feltételekhez kötött fedezet a szerződött fél sebezhetőségeinek teljes körű és gyakoribb értékelésével, valamint az ajánlott lépések követéséről szóló megállapodásokkal. Ez magában foglalhatja az ügyfelek folyamatainak, felelősségi köreinek és a vezetés működésének felülvizsgálatát is. Emellett tartalmazhat iparágakra vagy egyes vállalkozásokra vonatkozó értékeléseket, melyek állami ügynökségektől vagy más megbízható forrásoktól származó fenyegetettségi ismeretekre és értékelésekre támaszkodhatnak. Ezen túl tartalmazhat támadást imitáló gyakorlatokat a gyengeségek tesztelése és a válaszlépések megtervezése érdekében. Ezek után meghatározható a szükséges megelőző és érzékelő technológiák és eljárások implementálása a teljes biztosítási lefedettség feltételeként.

A biztosítóknak pedig előnyt jelent az elfogadott kockázatokról szóló jobb megértés és kontroll, ebből kifolyólag csökken a kitettség, és pontosabb árazásra lesz lehetőség. Az ügyfelek képessé válnak hatékonyabb és költséghatékonyabb védelemre. Ezek az értékelések emellett segítik az ügyfelekkel való közelebbi kapcsolat kialakulását, és a megbízásalapú tanácsadói szolgáltatások bázisául szolgálnak.

4. Még több adat megosztása

A pontosabb árképzés kulcsa a hatékonyabb adatmegosztás. Az ügyfelek reputációs okokból kifolyólag óvatosak az információbiztonsági betörések elismerésében, míg a biztosítók vonakodnak az adatmegosztástól a versenyelőny csökkenésétől való aggodalmuk miatt. Mindazonáltal az USA-ban már bevezetett és az EU-ban is bevezetésre kerülő adatbetörések értesítési kötelezettségéről szóló jogszabály segíthet az elérhető adatmennyiség növelésében. Bizonyos kormányok és törvényhozók emellett elindítottak adatmegosztási kezdeményezéseket (pl.: a szingapúri MAS vagy a UK Cyber Security Information Sharing Partnership). Az operatív kockázatokról történő adatgyűjtés az ORIC-on keresztül precedenst teremt még több iparági adatmegosztásra.

5. Valós idejű biztosítási szerződésfrissítés

Az évenkénti szerződésmegújítási és a 18 hónapos termékfejlesztési ciklusoknak teret kell adniuk a valós idejű analízisnek és a biztosítási szerződések folyamatos felülvizsgálatának. Ez a dinamikus megközelítés a biztonsági szoftverek frissítéseihez vagy a hitelfedezeti biztosítók által használt megoldáshoz hasonlítható, ahol a limitek és a kitettségek dinamikus menedzsmentje történik.

6. Hibrid kockázatáthárítás

Amíg a kiber viszontbiztosítási piac kevésbé fejlett, mint a direkt megfelelője, a növekvő veszély és a maximális kár jobb megértése egyre több viszontbiztosítási vállalat számára teheti vonzóvá a piacra történő belépést.

A kockázatáthárítási struktúrák általában tartalmaznak tradicionális veszteséget meghaladó viszontbiztosítást az alacsonyabb kárszintekben, a kiugró veszteségek elleni tőkepiaci struktúrák fejlesztésével. A lehetséges opciók tartalmazhatnak kártalanítást vagy ágazati viszontbiztosítási konstrukciókat és/vagy valamilyen formában feltételes tőkét. Ilyen tőkepiaci szerkezetek kívánatosak lehetnek a diverzifikációt és hozamot kereső befektetők számára. Az alapkezelők és a befektetési bankok behozhatják a megfelelő értékelési technikák kialakításához szükséges gyakorlatot viszontbiztosítási és/vagy technológiai vállalatoktól.

7. Kockázatcsökkentés

Ismerve a kiberbiztonságot körülvevő egyre összetettebb és bizonytalanabb, a fő veszteségeket okozó elemeket, egyre nő az igény az összehangolt kockázatmenedzsment megoldásokra, amelyek képesek az érintettek, köztük a vállalatok, biztosítási/viszontbiztosítási cégek, tőkepiacok és szabályozók összehozására. Valamilyen kockázatokra specializálódott tanácsadó cégre szükség lesz a felek összehozásához és a hatékony megoldás fejlesztésének vezetésére (PwC, 2014), beleértve a kiberbiztonsághoz fűződő szabványokat, melyeket megannyi kormány lelkesen vezet be.

8. Hitelességépítés hatékony saját belső védelmi intézkedések által

A hatékony saját belső védelmi intézkedések fejlesztése létfontosságú a kiberbiztonsági piacon a vállalattal mint egésszel szembeni bizalom fenntartása, valamint a hitelesség érdekében. Ha a biztosító nem tudja megvédeni magát, miért bíznának az ügyfelek abban, hogy képes lesz megvédeni őket?

A bankok dollár százmilliókat fektettek a kiberbiztonságba, hírszerző ügynökségek embereit, még ex-hackereket is magukhoz csábítva, hogy azok tanácsokat adjanak a szükséges biztosítékokról (Chon, Scannel, 2015). A biztosítóknak hasonlóképp szükséges megfelelő mértékben befektetni a saját kiberbiztonságukba, tekintve az általuk tárolt érzékeny szerződő felekről szóló információkat, amelyek veszélybe kerülése olyan bizalomvesztéshez vezethet, amelyet rendkívül nehéz lenne helyreállítani. A kiberbiztosítók által tárolt érzékeny adatok között ott vannak az ügyfelek kiberkockázatairól és védekezéseiről szóló információk, melyekhez hackerek esetleg hozzá akarnak férni.

Az első lépés a vállalatvezetők számára az irányítás átvétele a vállalaton belül az információ- és kiberbiztonság értékelésében és kezelésében, nem szabad egyszerűen IT-megfelelési kérdésként kezelni azokat.

Trendek

A kiberbiztosításban óriási, jórészt kiaknázatlan potenciál van, mind a biztosítók, mind pedig a viszontbiztosítók számára. A PwC számításai szerint az éves díjbevétel az ez évi 2,5 milliárd dollárról (Lloyds.com, 2015/a) 7,5 milliárd dollárral (PwC becslés) nőhet az évtized végére.

A kiberbiztosítás hamarosan elvárt szolgáltatás lehet az ügyfelek részéről.

Minden szektorban kezdik felismerni a kiberbiztosítás jelentőségét az egyre komplexebb és magas kockázatú digitális környezetben. Mind több biztosító és viszontbiztosító szeretne előnyt kovácsolni ezen a magas haszonnal kecsegtető, de még mindig formálódó, kevéssé szabályozott piacon. Ellenben többen is tartanak a kiberbiztonságtól. Meddig halogathatják a belépést? A kiberbiztosítás hamarosan elvárt szolgáltatás lehet az ügyfelek részéről, és a nem kellően proaktív biztosítók jelentős üzleti lehetőségekről maradhatnak le, ha a kibertermékek hiányoznak a portfóliójukból.

Mindeközben sok biztosító néz szembe jelentős kiberkitettséggel a különböző üzleti területeken. Az elsődleges prioritás ezen „rejtett" kitettségek felmérése és menedzselése.

Miért övezi ekkora szkepticizmus a kiberbiztosítást? A kihívás egyik része, hogy a kiberkockázat teljesen más típusú, mint amit a biztosítók és viszontbiztosítók korábban elvállaltak. Nagyon kevés nyilvánosan hozzáférhető adat áll rendelkezésre a kibertámadások mértékéről és pénzügyi hatásáról. Az adathiány okozta nehézségeket tovább súlyosbítja a fenyegetések fejlődési és terjedési sebessége. Míg a rendszerek helyreállításának hozzávetőleges költségei becsülhetőek, még nincs elég történeti adat a közvetett költségek (márkanév hírnévromlás, kártérítések) meghatározásához. Az Egyesült Királyságban készült jelentés 150 milliárd dollárra (Egyesült Királyság, Cabinet Office, 2015) becsüli a biztosítási piac globális kiberkockázati kitettségét, mely több mint harmadát teszi ki a Stratégiai és Nemzetközi Tanulmányok Központ (CSIS) becslésének a kibertámadások okozta 400 milliárd dolláros (Mcafee, 2014) veszteségről.

Ameddig a potenciális veszteségek nagyságrendje megegyezik a természeti katasztrófák okozta károkkal, az incidensek sokkal gyakoribbak. Következésképp a piaci szereplők egyre növekvő aggodalommal figyelik a kiberkockázat koncentráltságát, valamint a kevésbé tapasztalt biztosítók képességét az esetleges sorozatos magas veszteségű káresetek elviselésére.

A 2014-es évben hozzávetőleg 2,5 milliárd dollár kiberbiztosítási díj került befizetésre (Lloyds, 2015/b). Ezen biztosítások mintegy 90 százalékát amerikai vállalatok kötötték (Fortune, 2015 idézi PwC 2015/b), kihangsúlyozva a világpiac növekedési potenciálját. Az Egyesült Királyságban például csak a vállalatok 2 százaléka rendelkezik önálló

kiberbiztosítással (Reuters, 2015 idézi PwC, 2015/b). A gyártással foglalkozó vállalatoknak csak 5, míg az egészségügyi, technológiai és kereskedelmi szektor cégeinek közel 50 százaléka rendelkezik valamilyen formában kiberbiztosítással (Willis Insight 2014 idézi PwC, 2015/b).

A bankszektor vezetőinek 79 százaléka tekint a kibertámadásokra növekedést fenyegető tényezőként.

A vállalatvezetők 61, a biztosítótársaságok vezérigazgatóinak 71, a bankszektor vezetőinek 79 százaléka (a legmagasabb érték a többi szektorral összehasonlítva) tekint a kibertámadásokra növekedést fenyegető tényezőként, amely megelőzi ezzel a fogyasztói magatartás változását vagy a beszállítói lánc megszakadását (PwC, 2015/c). Ahogy a kiberfenyegetés veszélyeinek felmérése előrehalad, a kiberbiztosítások elterjedtsége a kevésbé lefedett iparágakban is nő, valamint a vállalatoknak bejelentési kötelezettségük van kiberlefedettségükről (pl.: US Securities and Exchange Commission közzétételi irányelv) (USA, SEC, 2011). Számításaink szerint a kiberbiztosítási piac 2018-ra elérheti az 5 milliárd dolláros határt, míg 2020-ra átlépheti a 7,5 milliárd dolláros értéket.

Talán meglepő eredmény, hogy a legnagyobb veszteségek nem is a szellemi tulajdonokhoz kapcsolódnak, hanem a személyes adatok elvesztéséből származnak. (4. ábra)

4. ábra - Incidensekhez kapcsolódó, kiberbiztosítások által fedezett veszteségek

Differenciálás és megtérülés

Kezdetben a hangsúlyt a kárigényeket kiváltó események és a biztosítási szerződések potenciális kitettségének azonosítására kell helyezni.

Ezt követően fejleszthető ki szcenárióelemzés, a dinamikus fenyegetéselhárítási intelligenciák és egyéb aktív kockázatcsökkentő intézkedések az ügyfélkockázatok értékelésére és a kitettségek hatékonyabb kontrollálására.

Ennek ellenére nehéz feladat az árazás az érettebb üzletágak esetében megszokott magabiztossággal és pontossággal. Egy információgazdagabb és fenntarthatóbb kiberbiztosítási modell segítségével lehetőség adódik az árképzés tartaléktartalmának csökkentésére, a tőke hatékonyabb allokálására, a hatékony viszontbiztosítások és felderítésére.

A biztosító saját kiberbiztonsága (értve ez alatt saját IT rendszereinek és IT infrastruktúrájának biztonságát és ennek közvetett hatását a biztosító profitjára) kritikus a digitalizáció hasznainak pénzzé alakításában, valamint abban is, hogy a gyorsan növekvő kiberbiztosítási piac vezetőjévé válhasson.

A kiberbiztosítások alapjául szolgáló kockázatfelméréssel egyszerűbbé válik az információbiztonságra költött összegek számszerűsítése.

A kiberbiztosítások előnyei nem érnek véget a pénzügyi veszteségek minimalizálásánál. Az egyik legnagyobb probléma az információbiztonsági piacon, hogy az információbiztonsági kockázatok csökkentésére költött összegek megtérülése nehezen számszerűsíthető, hiszen a menedzsment számára nehéz megfoghatóvá tenni, hogy az elköltött összegek hatására milyen biztonsági incidens nem történt meg. A kiberbiztosítások alapjául szolgáló kockázatfelméréssel és az ehhez kapcsolódó biztosítói árazási modellekkel azonban egyszerűbbé válik az információbiztonságra költött összegek számszerűsítése, aminek közvetlen hatása van a vállalatvezetők ez irányú költségkereteinek meghatározására és áttételesen az információbiztonsági piacra. A kulcs a kérdés vállalati szintű, és nem csak rendszer/technológiai veszélyként való értelmezése, valamint a vezetőség bátorítása, hogy vezető szerepet játsszanak a kiberbiztonság napi üzleti működésbe való integrálásában.

Ennek jótékony hatásai a biztosítási piacon is érződhetnek a jövőben, mivel ennek és a rendelkezésre álló nagyobb és pontosabb információhalmaznak köszönhetően egyszerűsödhetnek és finomodhatnak az árkalkulációs modellek.

Néhány biztosító és viszontbiztosító még mindig óvatos a kiberbiztonság kérdésében. A spektrum másik végén veszélyes kitettségekkel néz szembe. Mi ettől függetlenül hisszük, hogy az okos elemzésekből, az agilis válaszokból és a kockázatáthárítás fejlődésének kombinációjából a biztosítótársaságok tőkét tudnak kovácsolni az üzlet veszélybe sodrása nélkül.

Egy viszonylag átalánydíjas árképzésű és korlátozó rendelkező piacon a kiberkitettségek

jobb megértése és kontrollja mind tisztább versenydifferenciálást, mind fenntarthatóbb megtérülést biztosíthat. A legfontosabb előnyök között ott van a vonzóbb árképzés, kondíciók és kizárások találóbb ajánlása, valamint a hatékonyabb kockázatáthárítási megoldások.

HIVATKOZÁSOK

Chon, G., Scannel, K., 2015. Cyber insecurity: When 95% isn't good enough. Financial Times. [online] 2015.07.28. Elérhető: <http://www.ft.com/cms/s/0/251a40ea-2fcf-11e5-91ac-a5e17d9b4cff.html> [Letöltve: 2015.10.30].

Egyesült Királyság, Cabinet Office, 2015. UK cyber security: the role of insurance in managing and mitigating the risk. [pdf] HM Government. Elérhető: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf> [Letöltve: 2015.10.30]

Fortune, 2015.01.23. Idézi: PwC, 2015/b. Insurance 2020 & beyond: Reaping the dividends of cyber resilience. [pdf] PwC. Elérhető: <http://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf> [Letöltve: 2015.10.30].

Lloyds, 2015/a. Business Blackout - The insurance implications of a cyber attack on the US power grid. [pdf] Centre for Risk Studies, University of Cambridge. Elérhető: <http://www.empgridservices.com/wp-content/uploads/2015/07/Business-Blackout-July-2015.pdf> [Letöltve: 2015.10.30].

Lloyds, 2015/b. Vision 2025 and AAMGA. [online] 2015.05.28. Elérhető: <https://www.lloyds.com/lloyds/press-centre/speeches/2015/05/vision-2025-and-aamga> [Letöltve: 2015.10.30].

Mcafee, 2014. Net Losses: Estimating the Global Cost of Cybercrime - Economic impact of cybercrime II. [pdf] Center for Strategic and International Studies. Elérhető: <http://www.mcafee.com/mx/resources/reports/rp-economic-impact-cybercrime2.pdf> [Letöltve: 2015.10.30].

PwC, 2014. Broking 2020: Leading from the front in a new era of risk. PwC. Elérhető: <http://www.pwc.com/gx/en/insurance/reinsurance-rendezvous/assets/pwc-insurance-brokerage.pdf> [Letöltve: 2015.10.30].

PwC,2015/a. Insurance 2020 & beyond: Necessity is the mother of reinvention. [pdf] PwC. Elérhető: <http://www.pwc.com/gx/en/insurance/publications/assets/pwc-insurance-2020-and-beyond.pdf> [Letöltve: 2015.10.30].

PwC, 2015/b. Insurance 2020 & beyond: Reaping the dividends of cyber resilience. [pdf] PwC. Elérhető: <http://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf> [Letöltve: 2015.10.30]

PwC, 2015/c. 18th Annual Global CEO Survey - A marketplace without boundaries? Responding to disruption. [pdf] PwC, Elérhető: <http://www.pwc.com/gx/en/ceo-survey/2015/assets/pwc-18th-annual-global-ceo-survey-jan-2015.pdf> [Letöltve: 2015.10.30].

PwC, 2015/d. The Global State of Information Security Survey 2016
[pdf] PwC, Elérhető: <http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html> [Letöltve: 2015.10.30].

Reuters, 2015.03.23. Idézi: PwC, 2015/b. Insurance 2020 & beyond: Reaping the dividends of cyber resilience. [pdf] PwC. Elérhető: <http://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf> [Letöltve: 2015.10.30].

USA, Securities and Exchange Commission, Division of Corporation Finance. CF Disclosure Guidance: Topic No. 2. [online] Elérhető: <https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm> [Letöltve: 2015.10.30].

Willis Insights, 2014.03. Idézi: PwC, 2015/b. Insurance 2020 & beyond: Reaping the dividends of cyber resilience. [pdf] PwC. Elérhető: <http://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf> [Letöltve: 2015.10.30].