EGY HATÉKONY KIBERBIZTOSÍTÁSI PIAC MŰKÖDÉSÉNEK TÁMOGATÁSA
OECD-JELENTÉS A G7 ELNÖKSÉGE SZÁMÁRA – 2017. FEBRUÁR

Fordította: Gulyás Attila, attigulyas@gmail.com

ÖSSZEFOGLALÓ

Az információs technológiától való növekvő mértékű függés a gazdasági tevékenységek körében lényeges kockázatok kialakulásához vezet. E kockázatok között említendők a „digitális biztonsági kockázatok", melyek megnehezítik a gazdasági és társadalmi célok elérését azáltal, hogy az információ és az információs rendszerek integritását, elérhetőségét és bizalmi jellegét veszélyeztetik. A kiberkockázatok elleni biztosítási fedezet a vállalatok és az egyének számára olyan eszközt jelent, mellyel a pénzügyi kitettségük (kockázatuk) egy részét a biztosítási piacokra transzferálhatják. Jelen cikk annak az OECD-jelentésnek a magyar fordítása, mely a G7 2017. február 23-24-én tartott pénzügyminiszteri találkozóra készült a témában. Az eredeti angol verzió az alábbi linken található:

http://www.oecd.org/daf/fin/insurance/Supporting-an-effective-cyber-insurance-market.pdf

SUMMARY

The increasing use of and dependence on information technology in economic activities is leading to significant risks. Among them are "digital security risks" which, when they materialise, can disrupt the achievement of economic and social objectives by compromising the confidentiality, integrity and availability of information and information systems. Insurance coverage for cyber risk provides a means for companies and individuals to transfer a portion of their financial exposure to insurance markets. Present article is the Hungarian version of the report that has been prepared by the OECD for the G7 Deputy Finance Ministers meeting on 23-24 February 2017. The original English version is available below:

http://www.oecd.org/daf/fin/insurance/Supporting-an-effective-cyber-insurance-market.pdf

Kulcsszavak: digitális biztonsági kockázatok, kiberbiztosítási piac
Keywords: cyber insurance marker, digital security risk

JEL: G22, O33

DOI: 10.18530/BK.2017.3.76
http://dx.doi.org/1018530/BK.2017.3.76

BIZTOSÍTÁS ÉS KOCKÁZAT

Az információs technológiától való növekvő mértékű függés, illetve annak egyre intenzívebb használata a gazdasági tevékenységek körében – miközben jelentős termelékenységbeli és hatékonyságbeli előnyöket hoz létre – lényeges kockázatok kialakulásához is vezet. E kockázatok között említendők a „digitális biztonsági kockázatok", melyek anyagi valósággá válásukkor megnehezítik a gazdasági és társadalmi célok elérését azáltal, hogy az információ és az információs rendszerek integritását, elérhetőségét és bizalmi jellegét veszélyeztetik. Általánosan elterjedt az a vélekedés, hogy a legtöbb vállalat vagy már érintett volt valamely kiberincidensben[1], és erről tudomása is van (esetleg nincs), vagy a jövőben válik érintetté. Bár a kockázat mérése továbbra is formálódóban van, tele kihívásokkal, a kiberincidensek hatóköre és gyakorisága jelentős növekedést mutat mind az események számát, mind az érintett vállalatok részarányát tekintve. Mindez ahhoz vezetett, hogy a Világgazdasági Fórum 2017. évi Globális Kockázatok Jelentésében[2] a kiberkockázatot mint a legfontosabb (vagy második legfontosabb) problémakört határozták meg.

A kiberkockázatok elleni biztosítási fedezet a vállalatok és az egyének számára olyan eszközt jelent, mellyel a pénzügyi kitettségük (kockázatuk) egy részét a biztosítási piacokra transzferálhatják. A biztosítási piacok és a vállalatok a kockázat tudatosság növelésével, a kockázatok számszerűsítésére és mérséklésére való ösztönzéssel hozzá tudnak járulni a kiberkockázatok kezeléséhez. Példaként említhető:

- A biztosítási fedezet kiválasztásának folyamata azt követeli meg a szerződőktől, hogy megértsék (és számszerűsítsék) azt a kockázatot, amellyel szembenéznek, annak érdekében, hogy meg tudják határozni az általuk igényelt fedezet nagyságát.
- A biztosításkötési folyamat ki fog terjedni a kockázatmenedzsment és a biztonsági gyakorlat értékelésére, ami lehetőséget teremt jövőbeni preventív intézkedések megtételére.
- A kockázatárazás során olyan ösztönzőket kell kialakítani, amelyek a kockázatcsökkentés irányába hatnak. Így a kockázatmérséklés érdekében tett beruházások a fizetendő biztosítási díjak csökkenéséhez fognak vezetni.

Mindazonáltal annak érdekében, hogy a biztosítás komoly hatást váltson ki a kockázat mérséklésében, a piacnak a vállalatok jelentős hányada számára lényeges mértékű fedezetet kell ajánlania – ez ma még nem teljesül.

A G7 Elnökségének kérésére ez a jelentés áttekintést kíván adni a kiberbiztosítás piacáról, kitekintve az elérhető fedezetekre, a potenciális hiányosságokra, illetve a jelenlegi kihívásokra: különös tekintettel az adatok elérhetőségére, a kiberkockázat számszerűsítésére, a tudatosságra és a fedezettel kapcsolatos félreértések elkerülésére. A beszámoló az OECD által a kiberkockázat-biztosításról készült nagyobb tanulmányon alapul.[3] A jelentés célja, hogy meghatározza azokat a lehetséges szabályozói lépéseket, amelyek képesek választ adni a hatékony kiberbiztosítási piac fejlődését meghatározó kihívásokra, így téve lehetővé

a G7 pénzügyminiszterei és a jegybankok elnökei számára, hogy ebben a témakörben megfelelő „input"-tal rendelkezzenek egy nyilvános vitában.[4]

A kiberbiztosítási piac

A kiberincidensek – mint például a magánszféra sérelme, a „szolgáltatás-megtagadással járó" támadások, a kiberbűnözés vagy a kiberzsarolás – különböző típusú kockázatokat hozhatnak létre az érintett vállalatoknál (1. ábra). Néhány eset arról tanúskodik, hogy fizikai kár, illetve üzemzavar (üzemleállás) is keletkezhet kibertámadásból, példaként említhető egy német acélműben 2014-ben elszenvedett kár, illetve 2015-ben Ukrajnában az energiaellátás jelentős kiterjedésű megszakítását eredményező támadás.

1. ábra: A gyakori kiberincidensekből eredő kockázattípusok[5]

Annak ellenére, hogy a kiberkockázatok elleni biztosítási termékek mintegy 20 éve már elérhetők néhány országban, a kiberbiztosítási piacra mint fejlődésben lévő piacra tekintenek. A fedezet nyújtható különálló biztosítás formájában, meglévő biztosítások kiegészítőjeként (pl. amikor meghatározott kockázatokra vonatkozó fedezettel bővítenek egy vagyonbiztosítást) vagy hagyományos biztosítás formájában, mindenfajta különleges kiterjesztés nélkül. (Erre a típusra gyakran ún. csendes kiberfedezetként utalnak. Lásd 1. doboz)

A különálló kiberbiztosítási piacon 2016-ban kb. 3,5 milliárd USA dollár értékű díjat írtak elő, amelyből mintegy 3 milliárd dollár értékű díjbevétel tartozott az Egyesült Államokban székhellyel rendelkező vállalatokhoz, míg az európai vállalatok 300 millió USA dollár értékben kötöttek biztosításokat. (Összehasonlításképpen: a bruttó előírt díjbevétel a G7 országokban 2015-ben a kötelező gépjármű-felelősségbiztosítási szegmensben 373 milliárd dollár, míg a tűz- és ingatlanbiztosítás (lakó- és kereskedelmi) díjbevétele 230 milliárd dollár volt. OECD 2016.)

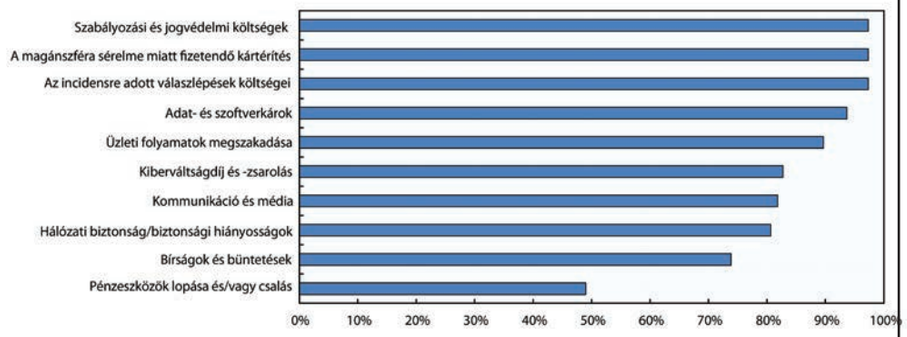
Egyes becslések szerint a piac 2020-ra megduplázódhat, alapvetően az Európában bekövetkező növekedésnek köszönhetően, részben az EU Általános Adatvédelmi rendeletének hatására, mely rendelet egységes értékesítési és közzétételi (nyilvánosságra hozatali) követelményeket fogalmaz meg, szankciókat és büntetéseket irányoz elő, valamint az adatlopást elszenvedett áldozatok számára elősegíti a kártérítési igények érvényesíthetőségét.

1. doboz: A kiberincidensekhez kapcsolódó veszteségek biztosítási fedezetének lehetséges formái

A különálló kiberbiztosítás

A különálló kiberbiztosítások piaca a kibertérből származó veszteségeknek a vagyon-, bűnügyi, emberrablás-, váltságdíj-, felelősség- és egyéb hagyományos biztosításaiból való kizárására adott válaszként fejlődött ki. Három jelentős kizárt kockázati kör definiálható: (i) kibertámadásokból vagy incidensekből származó veszteség általános érvényű kizárása; (ii) az általános felelősségbiztosítások szerződéses feltételeiben alkalmazott, az adatlopással kapcsolatos felelősség kizárása; (iii) mindazon veszteségek kizárása, amelyek az adat-helyreállítással kapcsolatosak. Ezen kizárások alkalmazása – azzal a követelménnyel együtt, hogy vagyoni kárnak kell keletkeznie ahhoz, hogy az üzleti folyamatok megszakadására nyújtott fedezet igénybe vehető legyen – vezetett a kiberincidensekből eredő veszteségekre nyújtott fedezetekben meglévő hiányosságokhoz. Mindezek eredményeként a legtöbb különálló kiberbiztosítás úgy került kifejlesztésre, hogy lezárja ezeket a réseket, és lefedjen néhány főbb kockázatot, mely jellemzően a magánszféra sérelméből származik, továbbá kisebb mértékben a szolgáltatás megtagadásával kapcsolatos támadásokból, a kiberzsarolásból, illetve a kiberbűnözésből eredő károkat is térítse (lásd 2. ábra).

2.ábra: A különálló kiberbiztosítások részesedése kockázattípusonként



Forrás: A fenti arányszámok az alábbiak átlagaként kerültek meghatározásra: (i) azon biztosítások aránya, amelyek az adott típusú kockázatokra fedezetet nyújtanak a 7 legnagyobb különálló kiberbiztosítást nyújtó biztosítónál (AIG, Allianz, AXA, Beazley, Chubb, XL Catlin, Zürich); (ii) azon biztosítások aránya, amelyek az adott típusú kockázatokra nyújtanak fedezetet; a számítás 26, a Risk Management Solutions Inc., valamint a Cambridge Centre for Risk Studies (2016) által vizsgált kötvényen alapuló kutatásból származik; (iii) biztosítási kötvények részesedése, amelyek az adott típusú kockázatokra nyújtanak fedezetet, és mely felmérés az OECD kutatási kérdőívére adott válaszokon nyugszik. (Ez magában foglalja a világ 9 biztosító társaságát és 9 biztosítási brókercégét.)

A hagyományos biztosításokban lévő („beágyazott" vagy csendes) kiberkockázati fedezet

Azokban az esetekben, amikor a hagyományos biztosítások a fentiekben megnevezett kizárásokat nem tartalmazzák, néhány kiber vonatkozású veszteségre a hagyományos vagyon-, felelősség-, bűnügyi/fidelitási, emberrablási, váltságdíj-biztosítások is fedezetet nyújthatnak (lásd 3. számú ábra). Ezt a fedezetet a biztosító, illetve a kötvénybirtokos egyértelművé teheti, például oly módon, hogy a kötvénybe belefoglal egy speciális kitételt, amely rendelkezik az ilyen kockázatra nyújtott fedezetről. Mindazonáltal más esetekben ez a fedezet csak egy jogvita vagy bírósági ügy eredményeként kerülhet „feltárásra". A hagyományos biztosítási kötvényekben korlátozottan áll rendelkezésre információ mind a kibervonatkozású kitételek, mind a kizárt kockázatok tekintetében (és ebből eredően e biztosításokban a kiberkockázatokra nyújtott fedezetek mértékére nézve is). Az OECD kérdőívére adott egyes válaszok, adatok azt sugallják, hogy a vagyonbiztosításokban lévő kizárások (pl. a kiber eredetű kockázatok általános kizárása és az adat-helyreállításból eredő veszteségek kizárása) a legtöbb piacon gyakorta alkalmazott megoldások, míg az általános felelősségi kizárások sokkal jellemzőbbek az Egyesült Államokban, mint az európai piacon (beleértve az Egyesült Királyságot is).

3. ábra: Kiberkockázatokra nyújtott lehetséges fedezetek a hagyományos kötvényekben

A kiberbiztosítási fedezetek szintjét a hagyományos biztosításokban nehéz (ha éppen nem lehetetlen) megbecsülni, miután a beszedendő díjbevételnek az a része, amely a kiberkockázatok fedezetére szolgálna, nincs elkülönítetten kimutatva (ha egyáltalán erre a célra el van különítve).

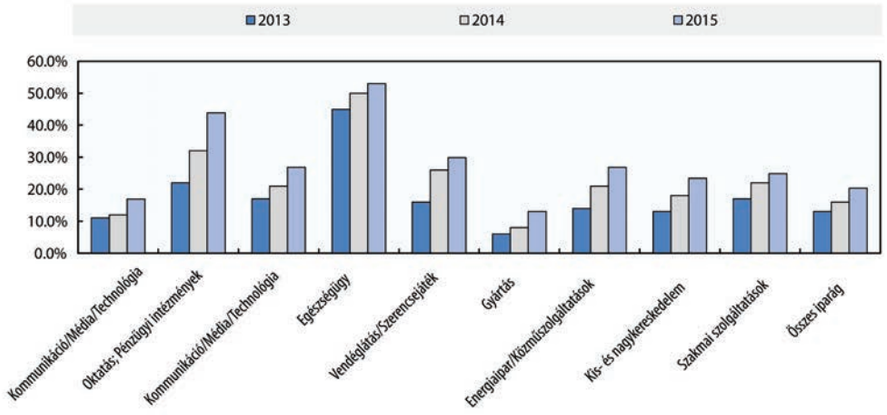
A piac éretlenségének jelei

Bár az elmúlt években a piac erőteljesen növekedett, számos jelét látni még a piac éretlenségének:

- *Kevéssé elterjedt a kiberbiztosítás:* A legtöbb érett biztosítási piacon a vállalati vagyon- és felelősségbiztosítás elterjedtsége magas (akár a 100%-ot is megközelítő). Kiberbiztosítást ezzel szemben kevesebb vállalat vásárol – az Egyesült Államok vállalatainak 20-35 százaléka rendelkezik (különálló vagy beágyazott) kiberbiztosítási fedezettel, míg ez az arány Európában és az Egyesült Királyságban becslések szerint 20-25 százalék a közepes és nagyvállalatok esetében. Tekintve, hogy a kiberkockázatok a hagyományos biztosítási fedezetekből nincsenek konzekvensen kizárva, nem szükséges

minden vállalkozás számára kiberbiztosítás vásárlása. Ugyanakkor a különböző szektorok közötti (lásd 4. ábra), illetve cégméret mentén tapasztalható eltérések azt sugallják, hogy az alacsony piaci penetrációt részben a tájékozatlanság magyarázza.[6]

4. ábra: Becsült különálló kiberbiztosítási fedezetek szektoronként (Marsh-ügyfelek)



Forrás: Marsh (2015c) jelentés az ügyfélkör 2013-as és 2014-es fedezeti arányairól (többségében egyesült államokbeli ügyfelek). Marsh (2016) csak a fedezetekben bekövetkezett változást teszi közzé, így a 2015-ös adatok ezen változást felhasználva kerültek megállapításra.

- *Nagy különbségek vannak az egyes biztosítók által kínált fedezetekben:* Mind a különálló kiberbiztosítások által fedezett kockázatok köre, mind a hagyományos biztosításokba beágyazott kiberkockázat-fedezetek kizárások utáni mértéke erőteljesen különbözik a biztosítást kínálók között. A különálló biztosítások erőteljes különbözőséget mutatnak abban a tekintetben, hogy a biztosítás milyen felelősségi helyzetekre nyújt fedezetet (kártérítés magánszféra sérelme esetén, kommunikáció-, média- és hálózatbiztonsági hiányosságok), hogy a bírságokra, büntetésekre és váltságdíjakra fedezetet nyújt-e fedezetet a biztosítás[7], valamint a tekintetben, hogy milyen mértékben fedezettek a részben emberi hibára visszavezethető károk.[8]

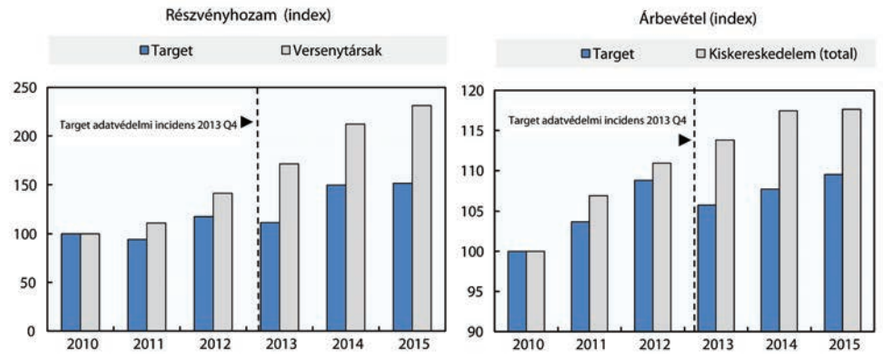
- *A biztosítás lényeges kockázatokra nem nyújthat fedezetet:* Bizonyos kiberincidensek olyan jelentős károkhoz vezethetnek, amelyekre a különálló vagy hagyományos biztosítások fedezetei általában nem terjednek ki. Egy példát említve, belső felhasználásra szánt adatok kiszivárgása komoly hatással lehet egy vállalat hírnevére és jövőbeni üzletére (lásd 2. doboz). Ennek ellenére nagyon kevés biztosítás[9] téríti meg ezeket a típusú károkat (ez rendszerint más típusú kockázatok esetében is így van). A szellemi tulajdon értékében bekövetkezett csökkenésre (például kiberkémkedés általi eltulajdonítás következtében) mind a hagyományos biztosításokba ágyazott[10] , mind a különálló kiberbiztosítások ritkán nyújtanak fedezetet. A legfőbb akadály mindkét esetben annak számszerűsítése, hogy a jó hírnéven esett csorba miatt mekkora az elvesztett jövőbeni üzlet, vagy hogy a szellemi tulajdon üzleti értékként való realizálásának lehetősége[11] milyen mértékben csökken annak sérelme esetén.

- *A fedezet értéke korlátos lehet:* Bizonyos mértékig alátámasztott, hogy az elérhető fedezetek mértéke, különösen a kockázatos iparágakban tevékenykedő nagyvállalatok esetében, elégtelen a vállalatok igényeihez viszonyítva.[12] Ezen túlmenően olyan korlátok, illetve önrészek vannak, mint például az üzletmenet megszakadását követő, a fedezet életbelépését megelőző 8-12 órás önrész periódus, ami tovább csökkenti az elérhető fedezet mértékét.

2. doboz: Az elvesztett jövőbeni üzlet következményei: a Target vállalat példája

2013 harmadik negyedévében a Target, az USA egyik meghatározó kiskereskedelmi vállalata egy jelentős adatlopásra derített fényt, amely megközelítőleg 40 millió fizetési kártya adatainak illetéktelen kezekbe jutásához vezetett. (70 millió egyéb információt, úgymint telefonszám és cím, tartalmazó rekord mellett.) A vállalat 2016. január 30-i jelentése szerint az illetéktelen adatszerzés közvetlen következményeként 291 millió USD költség merült fel, ideértve a négy nagy fizetésikártya-hálózatot működtető féllel, a vásárlókkal, illetve a pénzügyi intézményekkel mint kártyakibocsátókkal történő megállapodások költségeit. Ezen túlmenően számos, még függőben lévő peres eljárás, úgymint a kanadai ügyfelekkel és részvényesekkel folytatott per, valamint az Egyesült Államok főügyésze és a Szövetségi Kereskedelmi Bizottság által indított eljárások további fizetési kötelezettséget vonhatnak maguk után bírság és büntetés formájában (Target Corporation, 2016). Bár a közvetlen költségek jelentősek voltak, bizonyos rendelkezésre álló információk alapján arra lehet következtetni, hogy az elvesztett jövőbeni üzlet és a hírnéven esett csorba gazdasági hatása meghaladja a közvetlen költségekét. Míg a versenytársak részvényeinek hozamai és árbevételei növekedtek ezen időszak alatt, a Target esetében az illetéktelen adatszerzést követően azonnal csökkenés mutatkozott e mutatók körében, aminek következtében nőtt a Target lemaradása a versenytársaihoz képest (lásd 5. ábra).

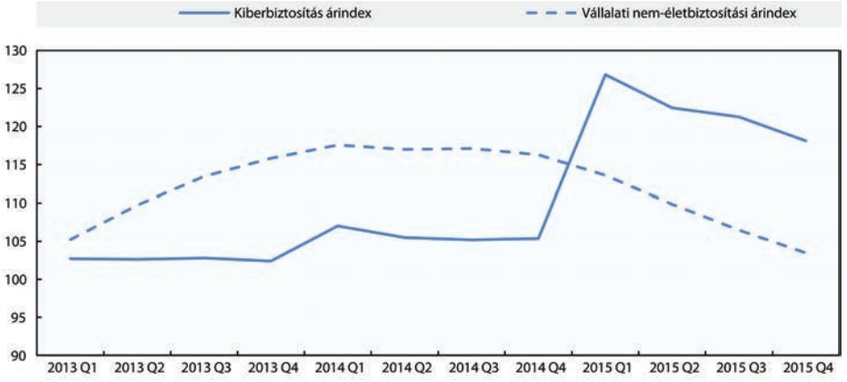
5. ábra: Az adatlopás gazdasági hatása (Target)



Forrás: Target Corporation (2014 and 2016); US Census Bureau, Retail Excluding Motor Vehicle and Parts Dealers, www.census.gov/retail/marts/www/adv4400a.txt (letöltve 2016. november 22-én) A részvényhozamot megjelenítő grafikonon feltüntetett versenytársi körnek, valamint maguknak az adatoknak is a forrása a Target Corporation (2016). Mind a részvényhozam, mind az árbevétel indexszé lett konvertálva.

- *A kiberbiztosítások díjai magasak, és szóródást mutatnak:* A kiberbiztosítási fedezet egységnyi díja (egy adott pénznemben kifejezett egy egységnyi [pl. 1 Ft] fedezet díja) becslések szerint háromszorosa az általános felelősségbiztosítások és hatszorosa a vagyonbiztosítások egységnyi biztosítási díjának. Ráadásul a kiberbiztosítások díjai az elmúlt hónapokban (általánosságban) növekedtek, míg az egyéb vállalati biztosítások díjai csökkentek (lásd 6. ábra). Bizonyos piaci beszámolók ugyanakkor az egyes biztosítók által ugyanazon kockázatokra kiterjedő fedezetek biztosítási díjaiban tapasztalható szignifikáns eltérésekről tanúskodnak. [13]

6. ábra: Kiber- és vállalati ingatlanbiztosítások árindexei (Egyesült Államok)



Forrás: A kiberbiztosítási árindex a kiberbiztosítások felelősségi fedezetéért kiszabott, Marsh (2014a, 2015c, 2016) által közzétett egységnyi díj éves átlagos növekedési üteme alapján került kiszámításra (2012=100). (A Marsh által közzétett növekedési ráták az előző év azonos időszakához viszonyítanak.) Az ábrán feltüntetett évekre az adatok többségében a Marsh egyesült államokbeli ügyfeleit jellemzik. A vállalati nem-életbiztosítási árindex forrása a Council of Insurance Agents and Brokers (2013, 2014, 2015b, 2016b) által az egyesült államokbeli vállalatok negyedéves átlagos biztosítási díjai alapján közzétett jelentés volt (2012 Q4=100).

Kihívások a kiberbiztosítások piacán

Számos hatás akadályozhatja a kiberbiztosítás elérhetőségét és megfizethetőségét, beleértve azokat a tényezőket is, amelyek magas díjhoz vezetnek (pl. bizonytalanság a kiberkockázatoknak való kitettség mértékét és a kitettséggel összefüggő kockázatok körét illetően), továbbá azokat a tényezőket is, amelyek csökkenthetik a vállalatok biztosítás iránti fizetési hajlandóságát (pl. tudatlanság és félreértés az elérhető fedezeteket illetően):

- *Bizonytalanság a kitettséget illetően:* A kiberkockázatok viszonylag új keletű kockázatok, ily módon korlátozottan áll rendelkezésre adat, amelyre a kockázat árazása során támaszkodni lehetne. A kibertámadások áldozatai általában tartózkodnak attól, hogy tájékoztatást adjanak az incidens körülményeiről és következményeiről. Ennek oka kétségkívül azoknak az áldozat hírnevére gyakorolt esetleges hatása, valamint további gát az adatokhoz való hozzáférés. Ezen túlmenően a kiberkockázatok gyors változása – a kibertámadások elkövetői várhatóan fejleszteni fogják meglévő módszereiket, és új módokat fognak találni a kibervédelmi vonalak megkerülésére – a rendelkezésre álló adatok használhatóságát tovább csökkenti. A jogi és szabályozási környezet gyors változása szintén befolyásolja a kiberincindensek okozta költségek körét és mértékét.

- *A kitettségek összefüggőségének kockázata:* A kibertérből eredeztethető károk összefüggőségének kockázata – azaz annak kockázata, hogy ugyanaz vagy ugyanolyan típusú incidens több biztosítottat érint egyszerre – magas. A károk összefüggősége számos esetben fennállhat, úgymint (i) egy sokak által használt szoftver sérülékenysége esetén, amely illetéktelen adatszerzések és szabotázsok széles körben történő elkövetését tenné lehetővé (ahogyan az a 2014-ben felfedezett „Heartbleed”sérülékenység[14] esetén is megtörténhetett volna); (ii) egyszerűen általánosítható és széles körben alkalmazható támadási eljárások esetén; vagy (iii) az alapvető információs technológiai infrastruktúrát célzó támadások esetén, mint például egy felhőalapú megoldásokat nyújtó szolgáltató vagy az internetműködést biztosító doménnévrendszer (DNS) (úgymint a 2016. október 21-i szolgáltatásmegtagadással járó támadás (DoS) egy doménnévrendszer szolgáltató ellen, amely számos weboldalt tett elérhetetlenné az Egyesült Államokban), alapvető infrastruktúra-szolgáltatók

(pl. elektromosáram-szolgáltató, fizetési rendszert, valamint műholdakat vagy légi forgalmat irányító szolgáltatók) vagy termelési láncok meghatározó szereplői ellen.

- *Korlátozott tájékozottság a kiberkároknak való kitettség mértékéről:* Bár a legtöbb vállalat tudatában van annak, hogy a hálózata feltörhető, az internet-hozzáférést biztosító szerverei DoS támadásnak eshetnek áldozatul, mégis nagyon kevés mérte fel ezen kiberincidensek pénzügyi hatását[15]– mely általában alapja a biztosítási fedezet vásárlásáról való döntésnek.

- *Az elérhető fedezetek körüli félreértések:* A kibertérből eredeztethető károk elleni biztosítási védelem formáját tekintve lehet különálló kiberbiztosítás, hagyományos biztosítás kiberbiztosítási kiegészítője vagy olyan tradicionális biztosítás, amely fedezetet nyújt vagyoni károkra, valamint bűnözésből, emberrablásból, váltságdíjból származó vagy más felelősségbiztosítás hatálya alá eső kár ellen. Még a különálló kiberbiztosítások esetében is jelentős eltérés mutatkozik a fedezett károk, az alkalmazott korlátozások, önrészek, valamint a kár bejelentésére rendelkezésre álló idő tekintetében. A megfelelő védelmet nyújtó kiberbiztosítás összetettsége, valamint a piacon elérhető biztosítások által fedezett kockázatok köre és néhány gyakorta előforduló kár (pl. hírnéven esett csorba, szellemi tulajdon sérelme) közti átfedés hiánya azt eredményezte, hogy sokak számára kérdésessé vált, hogy a megvásárolt kiberbiztosítás valóban megtéríti-e a károkat egy incidens esetén[16].

A kiberbiztosítási piac fejlődésének hátráltatói és lehetséges prioritások egy támogató szabályozói politika számára

A kiberbiztosítás csak abban az esetben tud hozzájárulni a kiberkockázatok csökkentéséhez és kezeléséhez, amennyiben a piac a vállalati és lakossági ügyfelek legfontosabb elvárásainak meg tud felelni. A kormányzatok fontos szerepet játszhatnak a piac fejlődésének támogatásában és a biztosítási piacnak e gyorsan változó kockázat kezeléséhez való hozzájárulásának maximalizálásában azáltal, hogy a piacfejlődés előtt álló gátló akadályokat elhárítja, különös tekintettel az alábbi pontokra:

- *A piacfejlődés akadályainak és a piaci rés jelenlétének megértése:* Ahogy a kiberincidensekből származó károk értéke növekszik, úgy egyre több előnyt rejt, és egyre nagyobb érdeklődés övezi az e kockázatokra fedezetet nyújtó biztosításokat. Ugyanakkor jelenleg számos tényező gátolja e fedezet széles körben való elterjedését és a keresleti oldal igényeihez való idomulását. A nemzetközi szervezeteket e témában folytatott kutatásaik, munkáik elmélyítésére kell ösztönözni, ideértve különösen az OECD-t, amely ajánlást tervez közzétenni szabályozók számára a piac fejlődését gátló akadályok elhárítását és a kiberbiztosítás elterjedését elősegítő lépésekről. Ez a jelentés, melyet a G7 országok rendelkezésére fognak bocsátani, szintén a piacfejlődést elősegítő lehetséges lépésekről folytatott vitához hivatott hozzájárulni.

- *A kitettségek számszerűsítéséhez rendelkezésre álló adatok elérhetőségének javítása:* Több, a kiberincidensek bekövetkezési gyakoriságára és súlyosságára (és kapcsolódó kárkifizetésekre) kiterjedő, átfogó adatforrás csökkentené a kiberkockázatokra kiterjedő biztosítási fedezeteket övező bizonytalanságot, ily módon elősegítené azok elterjedését és megfizethetőségét. Egy átfogóbb, kiberincidenseket taglaló adatbázis létrejötte valószínűleg az alábbiakat követelné meg: (i) a kiberincidensek és kártípusok sztenderd csoportosítása; (ii) az adatok gyűjtéséért és közzétételéért felelő hiteles szereplő (pl. kormányzati szerv); és (iii) ösztönzők (vagy előírások) az adatszolgáltatásra vonatkozóan azon vállalatok számára, amelyek kiberincidensek áldozatául estek, valamint azon biztosítók számára, amelyek ezen incidensekhez kapcsolódó kárkifizetéseket teljesítettek. Számtalan kezdeményezés indult el a biztosítási szektorban és egyes országokban, amelyek ezen feltételek részben vagy egészben történő teljesülését célozzák[17]. Az OECD a 2016-ban, Cancúnban megrendezett digitális gazdaságról szóló miniszteri konferenciát követően elindított, a kiberbiztonságról és adatvédelem-szabályozásról rendelkezésre álló tudásbázis fejlesztését célzó munkájának részeként szintén elkezdte a fenti témakörök feldolgozását.

- *A kiberkockázatok kezelésére vonatkozó szabályozás fejlesztése:* A legtöbb kormányzat nemzeti kiberbiztonsági vagy digitális biztonsági stratégiákat fogadott el az elmúlt években. Ugyanakkor, bár ezek a stratégiák célul tűzik a kiberkockázatokról való tájékozottság fejlesztését, nem minden esetben közelítik meg a kiberbiztonságot gazdasági és társadalmi kockázati nézőpontból. Ahogy a 2015-ös OECD tanácsi ajánlás a „Digitális biztonság kockázatainak kezelése a gazdasági és társadalmi fejlődés érdekében" című munkája is felhívja a rá a figyelmet, a nemzeti stratégiák tartalmazhatnak vállalatoknak szóló ösztönzőket a kiberkockázatoknak való kitettség mérésére és kezelésére. A vállalatirányítási gyakorlatok különösen alkalmasak arra, hogy a kiberkockázatok a vállalat átfogó kockázatkezelési rendszerébe beillesztésre kerüljenek (elkerülve e kockázatok pusztán technikai kérdésként való kezelését). A nemzeti stratégiáknak szintén ki kellene térniük a kiberbiztonságért felelős kormányzati szervek – ideértve a biztosítási piac felügyeletéért felelős szervek – közti együttműködés és közös koordináció előnyeire. Végezetül a kormányzatok szerepet játszhatnak abban, hogy tisztázásra kerüljön a különálló és hagyományos biztosításokba ágyazott kiberincidensekre vonatkozó fedezetek mértéke. Ezt oly módon tehetik meg, ha ösztönzik a biztosítási és biztosítotti közösséget arra, hogy a kiberkárok elleni fedezet szerepéről egyetértésre jussanak és/vagy azáltal, hogy követelményeket állítanak fel a biztosítók számára, amelyek a kínált fedezet (és a kizárt kockázatok körének) átláthatóságát növelik[18]. Ez különösen fontos volna kis- és középvállalatok, valamint magánszemélyek számára.

Függelék: Kártípusok, definíciók (a 2016-os CFO fórum által elfogadva)

Incidens típusa	A fedezet hatóköre
Segítségnyújtás, pszichológiai támogatás	Az áldozat segítése és pszichológiai támogatása, amennyiben a kiberincidens miatt a szerződő beleegyezése nélkül, a szerződő számára hátrányos információ került nyilvánosságra.
Testi sérülés és haláleset	Kárpótlás testi sérülés vagy annak következtében bekövetkező halál esetén, amennyiben az a vizsgált társaság vagy kapcsolódó harmadik fél jogsértő vagy gondatlan magatartásának következménye.
Magánszféra sérelme, megsértése [kárpótlás]	Kárpótlás személyes adat vagy érzékeny információ kiszivárogtatása esetén, ideértve a hitelképesség-figyelő szolgáltatásokat, de nem ideértve az incidensre adott válasz költségeit.
Üzemszünet, üzleti folyamatok megszakadása	A nem fizikai kárra visszavezethető termelésleállás következtében elveszett nyereség megtérítése.
Kommunikáció és média	Kárpótlás a vizsgált biztosító kommunikációs csatornáinak rossz célú felhasználása miatt, amennyiben az valamely harmadik fél jó hírnevét, becsületét sérti. Ide értendő a weboldal eltorzítása, továbbá szabadalmi, szerzői jog megsértése, üzleti titok illetéktelen felhasználása.
Harmadik félnél bekövetkező, nem fizikai eredetű üzletmenet-megszakadás	A nem fizikai kárra visszavezethető, a vizsgált társasággal kapcsolatban álló harmadik félnél (beszállító, üzlettárs, szolgáltató, vevő) bekövetkező üzleti folyamat megszakadása következtében elveszett nyereség megtérítése.
Kiberváltságdíj és -zsarolás	Váltságdíjat és/vagy zsarolást magában foglaló incidens kezeléséhez szükséges szakértő bevonásának költsége, beleértve a fizetendő váltságdíjat is (pl. az adatokhoz való hozzáférés csak a váltságdíj megfizetését követően válik lehetségessé).
Adat- és szoftverkár	Olyan adat és/vagy szoftver helyreállításának és/vagy helyettesítésének és/vagy újbóli előállításának költsége, amely elveszett, módosult, ellopásra, törlésre vagy titkosításra került.
D&O (ügyvezetői és munkavállalói felelősség)	Harmadik fél által benyújtott kártérítési igény a vizsgált vállalat ügyvezetőjével és munkavállalóival szemben, ideértve a kiberincidensből származó kötelezettségszegést vagy bizalomsértést.
Környezeti kár	Kártérítés mérgező és/vagy szennyező termékek kiberincidenst követő kibocsátása miatt.
Pénzeszközök lopása és/vagy csalás	Tisztán pénzügyi veszteség, amely olyan belső vagy külső rosszindulatú kibertevékenységből származik, amely csalás elkövetésére, pénz vagy más pénzügyi eszköz (pl. részvény) eltulajdonítására irányult. Fedezi mind a vizsgált társaságnak, mind a vizsgált társasággal kapcsolatban álló harmadik félnek a vizsgált társaság bizonyítottan jogsértő magatartásából származó tisztán pénzügyi veszteségeket..
Bírságok és büntetések	A vizsgált társaságra kiszabott bírságok és büntetések megtérítése. A biztosító csak azokban a jogállamokban téríti meg e költségeket, amelyekben ez megengedett.
Az incidensre adott válaszlépés(ek) költségei	A válságmenedzsment / belső vagy külső szakértőt igénylő válaszlépések költségei, ide nem értve a szabályozással összefüggő és jogvédelmi költségeket. A fedezet magában foglalja: (i) IT vizsgálat és igazságügyi elemzés költségeit, ha azok nem közvetlenül szabályozással összefüggő vagy jogvédelmi költségekhez kapcsolódnak; (ii) PR és kommunikációs költségeket; (iii) a helyzet orvoslásának költségeit (pl. a biztosított ellen irányuló kártékony tartalom eltávolításának költségeit); (iv) tájékoztatási költségeket.
Szellemi tulajdon sérelme (lopása)	A szellemi tulajdon tisztán pénzügyi veszteséget eredményező értékvesztése.
Jogvédelem – ügyvédi díjazás	A szerződő által vagy ellen indított jogi eljárás költségei, beleértve az ügyvédi díjazást pereskedés esetén. Példa: személyazonosság ellopása, az áldozat személyazonosságának rossz célú felhasználását bizonyító eljárás ügyvédi költségei.
Hálózatbiztonság / biztonsági hiba	Harmadik félnek (beszállító, üzlettárs, szolgáltató, vevő) a szerződő/vizsgált társaság IT hálózatán keresztül okozott kár megtérítése, ide nem értve az incidensre adott válaszlépések költségeit. A szerződőnek/vizsgált társaságnak nem szükséges kárt elszenvednie, elégséges, ha köztes szereplőként járul hozzá a harmadik fél eléréséhez.

Incidens típusa	A fedezet hatóköre
Tárgyi eszközben bekövetkezett kár	A vizsgált társaságra irányuló kiberincidens következtében fellépő, a vizsgált társaság tárgyi eszközének megrongálásával összefüggő károk (ideértve az üzleti folyamatok megszakadását és a harmadik félnél bekövetkező üzemszünetet).
Termékek	Kártérítés azokban az esetekben, amikor a vizsgált társaság által leszállított termékek vagy tevékenységek kiberincidens miatt hibásak vagy kárt okoznak, ide nem értve a technológiai termékfelelősség-biztosítást, valamint a szolgáltatói felelősségbiztosítást.
Szolgáltatói és szakmai felelősségbiztosítás	A kiberincidens következtében fellépő, nem megfelelő szolgáltatás nyújtásából vagy termék szállításából származó kár megtérítése, ide nem értve a technológiai termékfelelősség-biztosítást.
Szabályozással összefüggő költségek és perköltségek (kivéve bírság, büntetés)	A) Szabályozással összefüggő költségek: a vizsgált társaság vagy a vizsgált társasággal kapcsolatban álló harmadik fél azon költségeinek megtérítése, amely a szabályozó hatóság vagy kormányzati szerv részére történő, kiberincidenssel összefüggő adatszolgáltatásból fakad (magában foglalja a kiberincidens miatti adatszolgáltatással közvetlenül összefüggő jogi, technológiai vagy IT igazságügyi szolgáltatások költségeit, kivéve a bírságokat és büntetéseket). B) Jogvédelmi költségek: fedezet a vizsgált társaság vagy a vizsgált társasággal kapcsolatban álló harmadik fél bíróság előtt történő, kiberincidens következtében szükségessé váló jogi képviseletének költségeire.
Jó hírnév sérelme (kivéve a jogvédelmet)	Az ügyfélkörnek a társaság jó hírnéven esett csorba miatti bizalomvesztéséből fakadó csökkenése következtében elveszett nyereség megtérítése.
Technológiai termékfelelősség	A kiberincidens következtében fellépő, nem megfelelő technológiai szolgáltatás nyújtásából vagy technológiai termék szállításából származó kár megtérítése.

HIVATKOZÁSOK

[1] A jelen tanulmány szempontjából a „kiber” fogalom például a „kiberincidens” vagy a „kiberbiztosítás” kifejezésekben a digitális biztonsághoz kapcsolódó kérdésköröket takar.

[2] Az éves Globális Kockázati Jelentés céljainak tükrében a Világgazdasági Fórum a digitális biztonsághoz kapcsolódóan két technológiai kockázatot definiált: (i) „nagy volumenű kibertámadás”, amely olyan „nagyméretű kibertámadást vagy olyan rosszindulatú szoftvert jelöl, amely jelentős gazdasági károkat, geopolitikai feszültségeket okoz, vagy amely az internetbe vetett bizalom széles körű elvesztését okozza”, valamint (ii) tömeges adathamisítás, illetve lopás, mely „személyes vagy hivatalos adat korábban nem létező mértékű jogellenes felhasználását” jelöli.

[3] Ez a tanulmány részben egy OECD-kérdőívre az OECD-országok kormányai (pénzügyminisztériumai és szabályozó hatóságai), valamint nemzetközi színtéren működő biztosítók, viszontbiztosítók és brókerek által adott válaszokon alapszik. A projekttel kapcsolatos további információ a http://oecd.org/finance/insurance/ciber-risk-insurance.htm. címen érhető el.

[4] Ezek a kérdések az OECD előtt a digitális gazdaságpolitika perspektívájából, valamint az OECD-nek a kiberbiztonság, a magánszférát érintő kockázatok menedzselésének javításával foglalkozó munkájának részeként is megvitatásra kerülnek, összhangban a digitális gazdaságról tartott 2016. évi Cancúni Miniszteriális Tanácskozáson megfogalmazásra került célkitűzésekkel.

[5] Lásd a Függelékben a kárkategóriákat és definíciókat.

[6] Számos tanulmány azt sugallja, hogy a vállalatok korlátozott tájékozottsága a kiberkockázatokat – és különösen a kiberincidensek lehetséges költségét – illetően a fő gátja a kiberbiztosítás szélesebb körben való elterjedésének. Az OECD-kérdőív válaszadóinak közel 80%-a jelezte, hogy a potenciális szerződőknek a kiberbiztonsági kockázatok terén való korlátozott tájékozottsága meghatározó vagy mérsékelten meghatározó alkotóeleme a kiberbiztonsági kockázatoknak. A PwC 2016-os éves vállalatvezetői felmérése azt mutatja, hogy a vállalatvezetés kiberbiztonság iránti elkötelezettsége nagy eltéréseket mutat cégmérettől függően. Az óriásvállalatoknál például a vezetők 68%-a állította, hogy a vállalat vezetősége rendkívül elkötelezett a kibertámadások jelentette kockázatok megértésében, felügyelésében, ellentétben a kisebb vállalatoknál tapasztalható 32%-os aránnyal.

[7] Néhány jogértelmezés megengedi, hogy a biztosítási fedezet szabályozási szankciókra, bírságokra is kiterjedjen, illetve vannak olyan jogrendszerek, amelyekben megkérdőjelezik a büntetések, illetve bírságok kompenzációjára fizetendő biztosítások jogérvényességét. Továbbá néhány biztosító a saját üzleti gyakorlata (feltételrendszere) alapján nem nyújt fedezetet a bírságokra és a büntetésekre.

[8] Például az ún. „social engineering” (a másik jóhiszeműségének kijátszásával megszerzett információ, pszichológiai eszköz – ford. saját megjegyzése) alkalmazásával megszerzett tőkék eltulajdonítása „kizárt kockázat” olyan esetekben, amikor a pénzügyi veszteségre nyújtott fedezet gondatlanságból elkövetett cselekményekre korlátozódik (az adott pénzösszeg átutalása még olyan helyzetekben is, amikor a kezdeményezett félrevezető [eljárás] egy munkavállaló szándékosan elkövetett cselekményének is tekinthető.

[9] A Risk Management Solutions Inc. és a Cambridge Centre for Risk Studies (2016) által megvizsgált 26 kötvény kevesebb mint fele kínált fedezetet a jó hírnévben bekövetkezetett károkra, míg a 7 legnagyobb – különálló kiberbiztosítási kötvényt kibocsátó – biztosító egyetlen esetben sem nyújtott biztosítást a fenti típusú kockázatokra.

[10] A Risk Managament Solutions Inc. és a Cambridge Centre for Risk Studies (2016) által megvizsgált 26 kötvény kevesebb mint negyede kínált fedezetet a szellemi tulajdonjog sérelme miatt bekövetkezett károkra, míg a 7 legnagyobb – különálló kiberbiztosítási kötvényt kibocsátó – biztosító egyetlen esetben sem nyújtott biztosítást a fenti típusú kockázatokra.

[11] Csak egy példával illusztrálva, egy hivatalosan még nem forgalmazott filmről készült kalózmásolat (illetve forgalmazás) jelentős látogatószám-csökkenéshez vezethet a mozitársaságnál, bár különlegesen nehéz – ha nem lehetetlen – elkülöníteni egymástól az elveszett üzleti lehetőség értékét a jogosulatlan felhasználás okozta károktól.

[13] Lásd például: Betterely (2015); Biztosítási Ügynökök és Brókerek Tanácsa (2016a); PwC (2015b).

[13] Például egy Németországban lévő vállalat által 5 millió EUR összegig fedezetet nyújtó biztosítási igényére 20 és 120 ezer EUR összeg közötti ajánlatokat kapott. Egy gyógyszeripari cég az Egyesült Államokban egy meghatározott kockázati körre kapott ajánlatainak biztosítási díjai 300%-os variabilitást mutattak (Sclafane, 2015).

[14] Az ún. „Heartbleed” sérülékenység 2014 áprilisában széles körű publicitást kapott, mert ha az általánosan használt OpenSSL kriptografikai szoftver könyvtár komoly sérülékenysége eszkalálódott volna, akkor lehetővé tette volna olyan információk ellopását, melyeket normális körülmények között az SSL/TLS algoritmus véd. Az internet védelmére használt SSL/TLS biztosítja az interneten történő kommunikáció biztonságát és a magánadatok védelmét olyan alkalmazások esetében, mint a web, az e-mail, az IM (azonnali üzenetküldő rendszerek=instant message) és más virtuális magánhálózatok (heartbleed.com, 2014).

[15] Példaként [említve] a BAE Systems (2014) által nemzetközi (globális) vállalatokról készített kutatás azt találta, hogy a kibertámadások pénzügyi hatásainak csak 48%-át értékelték. Ezt a megállapítást erősítette meg az Advisen (2014) felmérése, amely azt közölte, hogy a biztosítói bróker válaszadók 73%-a azt [a feltételezést] erősítette meg, hogy a [kiberbiztosítások] megvásárlásának egyik legkomolyabb gátja a kiberbiztonság pénzügyi következményeiről való tájékozottság hiánya.

[16] Például a KPMG által az Egyesült Királyságban [dolgozó] IT szakemberek [bevonásával] készült felmérés azt találta, hogy a [megkérdezett szakemberek] közel 50%-a nem hiszi, hogy egy kibertámadás esetén a kiberbiztosítás kifizetődő lenne (Reeve,2015 z/Yen, 2015).

[17] Például a kiberincidensek kategorizálásáról készült tanulmány, amelyet a CR Fórum (megkérdezve a biztosítók kockázati menedzsereit) jegyez, és a CyRiM (Cyber Risk Management) Szingapúrban lefolytatott projektje alapján készült. Egy kiberincidensekről szóló központi adatrepozitórium létrehozásának lehetőségét folyamatosan vizsgálják a biztosítók, az Egyesült Királyság és az Egyesült Államok kormányzati szervei. Önkéntes (néhány esetben kötelező) kiberincidens-bejelentési kezdeményezést vezettek be számos országban.

[18] Például az Egyesült Királyság Tőkemegfelelést Vizsgáló Hatósága (Prudential Regulation Authority) nemrég közölt egy konzultációs tanulmányt, mely azt javasolja, hogy a biztosítók kifejezetten (külön díj ellenében) jelezzék a kiberincidensek elleni fedezetet a hagyományos kötvényekben. Franciaországban az IRT System X által vezetett gyakorlati [felmérések] egy mátrix kifejlesztését eredményezték, amely megmutatja az egyedülálló kötvények és a különböző hagyományos kötvények által lefedett kiberkockázati fedezetek területeit a francia piacon.

IRODALOMJEGYZÉK

Advisen (2014), Cyber Liability Insurance Market Trends: Survey, Advisen Ltd. (October).

BAE Systems (2014), Business and the Cyber Threat: The Rise of Digital Criminality, BAE Systems plc, Surrey, United Kingdom.

Betterley, R. (2015), "Cyber/Privacy Insurance Market Survey 2015", The Betterley Report, (June).

Council of Insurance Agents & Brokers (2016a), Cyber Insurance Market Watch Survey: Executive Summary, Council of Insurance Agents & Brokers (April).

Council of Insurance Agents & Brokers (2016b), Q2 Commercial P/C rates continued decline, according to CIAB Market Survey", News Release, 4 August, Council of Insurance Agents & Brokers.

Council of Insurance Agents & Brokers (2015), Pricing continued gradual decline in Q2, while interest in Cyber Liability grew", News Release, 29 July, Council of Insurance Agents & Brokers.

Council of Insurance Agents & Brokers (2014), Commercial P/C Pricing continued slide in Second Quarter of 2014, according to CIAB Survey", News Release, 31 July, Council of Insurance Agents & Brokers.

Council of Insurance Agents & Brokers (2013), Commercial P/C Pricing increases slowed in Second Quarter, according to CIAB Survey", News Release, 23 July, Council of Insurance Agents & Brokers.

CRO Forum (2016), CRO Forum Concept Paper on a proposed categorisation methodology for cyber risk, CRO Forum, Amsterdam, www.thecroforum.org/wp-content/uploads/2016/06/ZRH-1609033-P1_CRO_Forum_Cyber-Risk_web.pdf.

Marsh (2016), Benchmarking Trends: Operational Risks Drive Cyber Insurance Purchases, Marsh LLC, March.

Marsh (2015), Benchmarking Trends: As Cyber Concerns Broaden, Insurance Purchases Rise, Marsh LLC, March.

Marsh (2014), Benchmarking Trends: Interest in Cyber Insurance Continues to Climb, Marsh LLC, April.

OECD (2016), "Insurance business written in the reporting country: Premiums written by classes of non-life insurance", OECD. Stat, OECD Publishing, Paris, http://dotstat.oecd.org//Index.aspx?QueryId=25401.

Phillips, M. (2014), "Target's traffic still hasn't recovered from the giant data breach", Quartz, 21 May, http://qz.com/212003/targets-traffic-still-hasnt-recovered-from-the-giant-data-breach/, accessed 18 October 2016.

Prudential Regulation Authority (2016), Cyber insurance underwriting risk: Consultation Paper CP39/16 (November), Bank of England, London, www.bankofengland.co.uk/pra/Documents/publications/cp/2016/cp3916.pdf.

PwC (2015), Insurance 2020 & beyond: Reaping the dividends of cyber resilience, PwC.

PwC (2016), "The swinging pendulum: Board governance in the age of shareholder empowerment", PwC's 2016 Annual Corporate Directors Survey, PwC.

Reeve, T. (2015), "Cyber insurance not trusted by business, KPMG claims", SC Magazine UK, 1 May, www.scmagazineuk.com/cyber-insurance-not-trusted-by-business-kpmg-claims/article/412535/.

Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies (2016), Managing Cyber Insurance Accumulation Risk,

Risk Management Solutions, Inc. and Centre for Risk Studies, Cambridge University, http://cambridgeriskframework.com/getdocument/39.

Sclafane, S. (2015), "Cyber Risk Insurers Lag in Buying Cyber Cover", Carrier Management, 16 July, www.carriermanagement.com/news/2015/07/16/142577.htm.

Target Corporation (2016), 2015 Annual Report, Target Corporation, Minneapolis.

Target Corporation (2014), 2013 Annual Report, Target Corporation, Minneapolis.

World Economic Forum (2017), Global Risks Report 2017: 12th Edition, World Economic Forum, Geneva, www.weforum.org/reports/the-global-risks-report-2017.

Z/Yen Group (2015), Promoting UK Cyber Prosperity: Public-Private Cyber-Catastrophe Reinsurance, Long Finance.