A KIBERKOCKÁZAT BIZTOSÍTHATÓSÁGA VÁLLALATI SZINTEN

Balogh Márk (Budapest Corvinus Egyetem, Nemzetközi gazdálkodás szak), baloghmarkster@gmail.com

ÖSSZEFOGLALÓ

A 21. században az üzleti életben is egyre nagyobb szerepük van a számítógépeknek és az internetnek. A digitalizáció egyik legnagyobb veszélye a kiberkockázatnak való kitettség. Dolgozatomban arra keresem a választ, hogyan biztosítható a vállalatok kiberkockázata, melyek a hatékony biztosítás akadályai, illetve ezek hogyan csökkenthetők. A kutatás során öt, a kiberkockázat területén jártas személlyel készítettem mélyinterjút.

A hatékony biztosítás előtt álló legnagyobb akadály a tapasztalat- és adathiány. A probléma újszerűsége miatt a biztosítók nem rendelkeznek elég információval ahhoz, hogy pontos becsléseket végezzenek.

Arra a következtetésre jutottam, hogy a kiberbiztosítás szélesebb körben való elterjedéséhez elengedhetetlen, hogy a vállalatok, a biztosítók, valamint az IT szakemberek között bizalmi együttműködés alakuljon ki. A gazdasági szereplők közötti rendszeres kommunikáció és a tapasztalatok megosztása lehetővé teheti a kiberkockázatok eredményes biztosítását.

SUMMARY

In the 21st century computers and the internet has a growing role in business life. One of the greatest dangers of digitization is cyber risk exposure. In my study I am looking for an answer to how companies' cyber risk can be insured, what the obstacles to effective insurance are, and how they can be reduced. During my research I conducted five in-depth interviews with professionals of the topic.

The greatest obstacle to effective insurance is the lack of experience and data. Due to the novelty of the problem, insurance companies do not have enough information to make accurate estimates.

I came to the conclusion that for the widespread use of cyber-insurance it is essential to establish a cooperation based on trust between companies, insurers and IT professionals. Regular communication and the exchange of experience between economic operators can enable effective cyber-insurance.

Kulcsszavak: kiberkockázat, kiberbiztosítás, kibertámadás
Keywords: cyber risk, cyber-insurance, cyber attack

JEL: G22, O33

DOI: 10.18530/BK.2019.3.58
http://dx.doi.org/10.18530/BK.2019.3.58

1. Bevezetés

A 21. században életünk elképzelhetetlen lenne számítógépek és internet nélkül. A digitalizáció az üzleti világban is jelen van. Azok a vállalatok, melyek nem képesek lépést tartani a digitalizációval, könnyedén elveszíthetik piaci részesedésüket.

A nemzetközi vállalatok nemcsak információtárolásra használják a webet, hanem a különböző távoli termelőegységeik összekapcsolására és a cég pénzügyeinek és mindennapi műveleteinek lebonyolítására is. Ezáltal gyakran érzékeny üzleti titkok is keresztülmennek a világhálón. Az internetes információkezelés egyszerűbbé és hatékonyabbá teszi a vállalatok életét, azonban megvannak a maga hátrányai is. Az egyik legnagyobb veszélye a kiberkockázatnak való kitettség. Ha egy vállalat informatikai hálózatán rendszerhiba hiba lép fel, vagy hackertámadás éri a fogyasztói adatokat kezelő szervert, a céget várhatóan súlyos pénzügyi és hírnévveszteségek érik.

A Statista a világ egyik vezető statisztikai portálja. Adatai alapján 2016-ban a kibereseményekvoltak a harmadik vezető kockázat az Egyesült Államok vállalataira nézve (Statista, 2016), de a nagyfokú globalizáció és a nemzetközi vállalatok térhódítása miatt minden fejlett gazdaságban egyre komolyabb problémát jelentenek a kiberkárok. A Kaspersky Lab globális kiberbiztonsági vállalat felmérése alapján az elmúlt két évben az európai üzleti vállalkozások több mint felét érte legalább egy olyan kibertámadás, ami zavarokat okozott tevékenységükben (Biztosítási Szemle, 2019b). A kiberkockázat elterjedését támasztja alá az a kimutatás is, mely szerint 2018-ban a magyar vállalatok 78 százalékát érte valamilyen IT-biztonsági incidens (Biztosítási Szemle, 2019a). A digitalizáció okozta kockázatok térhódítására való tekintettel egyre több biztosítótársaság kínál kiberkockázat-biztosítást ügyfeleinek, azonban az iparág újszerűsége miatt még korántsem működik megfelelően.

Dolgozatom célja, hogy választ kapjak arra a kérdésre, hogyan biztosítható a vállalatok kiberkockázata, melyek a hatékony biztosítás akadályai, illetve ezek hogyan csökkenthetők. Ezzel a témakörrel már találkozhattak a Biztosítás és Kockázat olvasói Gulyás Attila (2017) cikkében is.

2. A kiberkockázat szakirodalma

Jóllehet a kiberkockázat csak nemrég robbant be a köztudatba, rengeteg különböző vélemény látott már napvilágot azzal kapcsolatban, hogy mit is jelent pontosan a fogalom, milyen kockázatok tartoznak ide, és melyek nem. A probléma tárgyalásához azonban fontos, hogy először tisztán és egyértelműen meghatározzuk, miről beszélünk.

2.1. Mi a kiberkockázat?

A kiberkockázat az angol „cyber risk" kifejezés tükörfordítása. Noha a probléma újszerűsége miatt nem létezik egységes definíció a kiberkockázatra, több álláspont is elterjedt. Biener et. al. (2015) szerint a kiberkockázat különböző típusú kockázatokat takar, melyek egy cég információs és technológiai eszközeit érintik. A kibertámadások közé tartozik a személyazonosság-lopás, az érzékeny információk közzététele és az üzemszünet okozása. A „kiber" kifejezés a „kibertér" szóra utal, ami informatikai rendszerekből, infrastruktúrából és szolgáltatásokból áll.

Ahhoz, hogy meg tudjuk különböztetni a kiberkockázatot az egyéb típusú kockázatoktól, pontosan definiálnunk kell a fogalmát. Dolgozatomban Eling és Schnell (2016) definíciójára támaszkodom, akik szerint a kiberkockázat „az információs és kommunikációs rendszerek használatából fakadó bármely kockázat, amely veszélyezteti az adatszolgáltatás titkosságát, rendelkezésre állását vagy sértetlenségét." (10. o.) Hozzáteszik, hogy az operációs technológia gyengülése üzleti zavarokat, infrastrukturális problémákat, valamint az emberek és a vagyon fizikai károsodását okozhatja. Véleményem szerint ez a definíció a leginkább megfelelő, mivel tartalmazza a potenciális kockázat forrását és következményét is.

> **A kiberkockázat veszélyezteti az adatszolgáltatás titkosságát, rendelkezésre állását vagy sértetlenségét.**

Ahogy a digitalizáció egyre több teret nyer, az információs technológiai hibák fajtája is gyarapodik. Ma már annyi típusa van a kiberkockázatnak, hogy a jobb átláthatóság érdekében érdemes különböző csoportokba sorolni őket. A kategorizálás segítségével könnyebb lesz vizsgálni az internethez való csatlakozás kockázatának hatásait és lehetséges megoldásait. Dolgozatom ezen szakaszában Cebula és Young (2010) kutatására hagyatkozom, mivel ezt a csoportosítást találtam a legszéleskörűbbnek.

Cebula és Young (2010) négy kiberkockázat-kategóriát különböztet meg. Az első csoport az **emberi tevékenységek**. Ide soroljuk a vállalaton belülre vagy azon kívülre tartozó személyek által okozott problémákat, név szerint a gondatlanságot, szándékos károkozást és tétlenséget.

A kiberkockázatok második csoportja a rendszer- és technológiai hibák. Ez az operatív kockázatok olyan fajtáját jelenti, amelyek a technológiai eszközök, mint például hardverek és szoftverek problémás, abnormális vagy váratlan működéséből erednek.

A harmadik csoportba tartoznak a **sikertelen belső folyamatok**. Általában ezek a hibák helytelen folyamattervezésből, a folyamat működésének nem megfelelő ellenőrzéséből és a támogató folyamatok meghibásodásából adódnak. Egy esetleges probléma megelőzését segíti az emberi és pénzügyi források szükséges mennyiségének megléte, valamint a folyamatok pontosabb szervezése és kontrollja.

Eddig olyan belső rendellenességeket említettem, amelyek közvetlenül kapcsolódnak az információs technológiához. A negyedik és egyben utolsó csoport Cebula és Young (2010) szerint a **külső események**. Ez a kifejezés működési kockázatok olyan típusát jelenti, ami a vállalat irányításán kívül eső történésekből tevődik össze. Ilyen például a vis maior, a jogi esetek, a gazdasági környezet váratlan megváltozása vagy a szolgáltatásoktól való függőség.

Mivel ezekre a kockázattípusokra nincs ráhatásuk a vállalatoknak, nehéz küzdeni ellenük. Lehetséges ugyan mérsékelni például egy tűzeset veszélyét a biztonsági szabályok betartásával, vagy egy beszállítói kudarc előfordulását megbízható partnerek megválasztásával, de képtelenség nullára redukálni a kockázati tényezők számát. Ezeken hivatottak segíteni a biztosítótársaságok.

Jelenleg tehát a fent említett négy típusát különböztetjük meg a kiberkockázatnak. Noha ezek a csoportok homogének, a kockázat még nem tagolt eléggé ahhoz, hogy kellően nagy, de homogén kockázatközösségekről beszéljünk. Emiatt kezeljük a négy kategóriát egy kockázatként.

A kategorizálással kapcsolatban jelenleg nincs egyetértés a szakértők között. Egyesek a működési kockázat részének tekintik a kiberkockázatot, míg mások úgy gondolják, hogy a kiberkockázat típusai között vannak olyanok, melyek működési kockázatnak minősülnek. Ezek a típusok a fent felsoroltak közül az emberi tevékenységek csoportba tartoznak, és azon belül is főként a külső támadásokat sorolják ide (Risk.net, 2019).

2.2. A kiberkockázat biztosíthatósága

A kibertámadások által okozott károk mértéke csökkenthető a megfelelő biztosítás megkötésével. A legfejlettebb országokban már számos biztosítótársaság portfóliójában megtalálható a digitális veszélyekkel kapcsolatos károk fedezete. A kiberbiztosítások szegmense, mely 2006 és 2013 között ötszörös növekedést mutatott az USA-ban, a szakemberek szerint tovább fog nőni (Pandurics – Markó, 2015). Annak ellenére azonban, hogy kereslet és kínálat is létezik, az egyre nagyobb fontosságú kiberbiztosítási piac nem működik megfelelően.

Noha Európában 2012 és 2015 között növekvő tendenciát mutatott a biztosítást vásárlók száma, a cégeknek mindössze a 35 százaléka kötött kiberbiztosítást 2015-ben (Statista, 2015). A Marsh & McLennan Agency (2018) elemzése alapján 2018-ban az Egyesült Államokban a felmérésben részt vevő vállalatoknak csupán 36 százaléka rendelkezett kiberbiztosítással, és mindössze 9 százaléka tervezi a következő egy évben ilyen fedezet vásárlását vagy meglévő biztosításának fejlesztését.

Ennek az alacsony százaléknak a magyarázatához meg kell érteni a kiberkockázatok biztosíthatóságának feltételeit. Biener et. al. (2015) részletesen vizsgálta a Berliner (1985) által megállapított biztosítási kritériumokat (veszteség előfordulásának véletlenszerűsége, lehetséges legnagyobb kár, egy esetre jutó átlagos veszteség, veszteségnek való kitettség, információs aszimmetria, biztosítási díjak, fedezeti limit, közösségi politika és jogi korlátozások) a kiberkockázatra vonatkozóan.

Az elemzés alapján az információs aszimmetria jelenti az egyik legkomolyabb akadályt a hatékony kiberbiztosítás előtt. Biener et. al. (2015) az információs aszimmetriával kapcsolatban a morális kockázatot és a kontraszelekciót emelte ki. A morális kockázat problémaköre azzal foglalkozik, hogy azok a vállalatok, amelyek fedezetet vásárolnak, hajlamosak kevesebb pénzt fektetni a biztonsági infrastruktúrájukba (Bailey, 2014). Emiatt nő a kár bekövetkeztének va-

lószínűsége, és a biztosító várható költsége is. A morális kockázat ellen a biztosítótársaságok többek között a szerződésekbe iktatott kizárásokkal védekezhetnek, elvárás például tűzfal és vírusirtók használata (Kesan et. al. 2014).

Biener et. al. (2015) szerint a kontraszelekció oka az, hogy nagyobb valószínűséggel kérnek biztosítást azok a cégek, amelyek már áldozatául estek egy kibertámadásnak. Azok azonban, akik még sosem tapasztaltak ilyen problémát, nincsenek tisztában a biztosítás jelentőségével. Az előzetes információk hiánya megnehezíti a biztosítótársaságok számára ügyfeleik különböző kockázati csoportba sorolását, ami szintén kontraszelekciót eredményez (Gordon et. al., 2003).

Az információs aszimmetria jelenti az egyik legkomolyabb akadályt a hatékony kiberbiztosítás előtt.

További akadályt jelent a kiberbiztosítási csomagok magas árazása. Bandyopadhyay et. al. (2009) szerint a piaci tapasztalatok hiánya, a hatalmas mennyiségű elveszített adat és a könyvelési nehézségek a biztosítási termékek magas árazásához vezettek. A kiberkárokat átélt vállalatok általában biztonsági okokból nem hajlandóak megosztani a káresettel kapcsolatos adataikat. Az információhiány miatt a biztosítók kötelesek komoly kockázati tartalékokat beépíteni termékeik árába. Berliner (1985) is bebizonyította, hogy minél magasabb a biztosítótársaság kockázatkerülése, annál magasabb biztosítási díjat fog kiszabni.

A fedezeti limit a biztosító által fedezett maximális kár értéke. A gyorsan változó digitális világnak köszönhetően sokszor kérdéses, hogy az adott kiberbiztosítás valójában mire is nyújt fedezetet. Emiatt a fedezeti limit kritérium is problémásnak tekinthető (Biener et. al., 2015).

Biener et. al. (2015) szerint a kiberesetek által okozott lehetséges legnagyobb kár általában sokkal alacsonyabb, mint az egyéb működési kockázatok által okozott veszteségek, így viszonylag könnyen tudják kezelni a biztosítók. Véleményem szerint azonban ma már ez az állítás nem helytálló. A közműveknél okozható következményes károk már fel sem mérhető nagyságrendűek. Ebből kifolyólag a lehetséges legnagyobb kár mértéke a biztosítás komoly akadálya.

Az egy esetre jutó átlagos veszteség számos tényezőtől függ, mint például a vállalat mérete vagy az alkalmazott védelmi rendszer. Biener et. al. (2015) arra jutott, hogy általánosságban a kibertámadások által okozott károk átlaga és mediánja alacsonyabb, mint az egyéb működési kockázatoké, tehát ez a kritérium egyelőre nem jelent problémát.

Biener et. al. (2015) empirikus elemzése azt mutatja, hogy a veszteség előfordulásának véletlenszerűsége és egymástól való függetlensége szintén nem ütközik komoly akadályokba, mivel a legtöbb kiberkockázattal kapcsolatos eset nincs összefüggésben más eseményekkel. Gyors fejlődésük azonban kiszámíthatatlanná teszi a kibertámadásokat, ezáltal biztosításuk igen nehéz és rizikós.

A veszteségnek való kitettség mértéke szintén biztosíthatósági kritérium. Minél gyakoribb a káreset, annál magasabb a kitettség, és annál problémásabb az adott kockázat biztosítása. A PricewaterhouseCoopers Magyarország Kft. kimutatása szerint 2016-ban naponta több mint 100.000 kibertámadás történt világszerte (Ötvös, 2016). Ez alapján megállapítható, hogy a veszteségnek való növekvő kitettség egyre komolyabb biztosíthatósági korlátot jelent a kiberkockázatok esetében.

Biener et. al. (2015) szerint a kiberbiztosítás közösségi politikájának összhangban kell lennie a társadalmi értékekkel. Ösztönzők hiányában a vállalatok nem fektetnek elég pénzt az önvédelembe. A káresetek biztosítása egyre komplikáltabb mind a vállalatok, mind a biztosítók számára. Ugyanakkor a kiberbiztosítási piac kormányzat általi elősegítése vagy a biztosítottság kötelezővé tétele jelenthet némi megoldást (Biener et. al., 2015).

A jogi korlátozások ügye rendkívül komplex. Shackelford (2012) úgy gondolja, hogy a kormányzatok által kibocsátott számos különböző törvény ellenére mind az amerikai, mind az európai államok az adatvédelmi törvények harmonizálására törekednek. Ilyen törekvés például az Amerikában bevezetett US Securities and Exchange Commission közzétételi irányelv, mely az adatbetörések értesítési kötelezettségét írja elő a vállalatok számára (Ötvös, 2016). Az Európai Unió 2018-ban fogadta el a Cybersecurity Act-et, melynek célja az Unió kiberbiztonságának növelése, valamint a tagállamoknak való segítségnyújtás különböző kiberproblémák esetén (European Commission, 2018). Hasonló jogszabályok léteznek már a világ számos országában. Amennyiben ezek a törekvések sikerrel járnak, a jogi korlátozásoknak ezen része kevésbé tekinthető a biztosítást korlátozó tényezőnek.

A kilenc kritériumból tehát négy igencsak, öt pedig kevésbé problémás. Összességében elmondható, hogy a kiberkockázat biztosítása lehetséges, de a biztosítótársaságok számára komoly akadályt jelent az információs aszimmetria és a digitalizáció gyors fejlődése.

2.3. Útmutató a kiberkárok megfelelő biztosításához

A szakirodalom számos megoldást kínál a potenciális digitális veszélyekkel kapcsolatos kockázat elkerülésére. Gordon et. al. (2003) részletesen kifejtette, melyek azok a lépések, melyeket a vállalatoknak szükséges megtenniük a megfelelő biztosítási csomag megvásárlásához.

Mindenekelőtt a szervezeteknek meg kell állapítaniuk az információs rendszerükhöz kapcsolódó fenyegetéseket és sebezhetőségeket. A kritikus információ meghatározását követően a vállalatoknak az elfogadható szint alá kell csökkenteniük a kiberkockázatot. Ennek egyik módja biztosítás vásárlása az esetleges károk fedezésére. A cégnek olyan biztosítási lehetőségeket kell keresnie, melyek elfogadható díjért cserébe megfelelő fedezetet biztosítanak. A legtöbb biztosítás kiterjed mind a vagyoni (például profitvesztés lehetősége), mind pedig a felelősségi kockázatra (például más cégnek vagy egyénnek okozott károk). (Gordon et. al., 2003)

A kockázat típusa nagymértékben függ a vállalat tevékenységétől. Egy mezőgazdasági cégnél például, ahol a munkát gépek végzik, egy szoftverhiba a teljes termelés leállását eredményezheti. Ebben az esetben a kár nem feltétlenül érint külső résztvevőket. Azonban, ha egy adott vállalat számlázását, banki műveleteit vagy ügyféladatait éri a támadás, a kár kiterjed a vállalattal kapcsolatban álló egyénekre, cégekre is. Látható tehát, milyen sok szempontot kell figyelembe venni a biztosítás kiválasztásánál.

Miután kiválasztásra került a biztosítási csomag, az adott biztosítótársaság szintén fel fogja mérni a vállalat kitettségét. Kesan et. al. (2014) szerint ez a felmérés egy részletes online kérdőívből és egy mélyreható biztonsági, hálózati és folyamati átvilágításból áll. Noha a legtöbb cég nem szívesen oszt meg üzleti titkokat külső felekkel, a kockázat elleni lefedettség miatt megéri együttműködni.

3. Módszertan

A következőkben dolgozatom kutatási részének módszertanát fogom bemutatni. A dolgozat gyakorlati része adatok gyűjtésére és azok feldolgozására, elemzésére épül. Gyulavári et. al. (2014) A marketingkutatás című könyvében arról ír, hogy a kutatás általános célja szerint beszélhetünk feltáró vagy következtető kutatásról. Mivel a kiberkockázat szakszerű vizsgálatához új, előre nem ismert, összetett ötletek gyűjtésére van szükség, kutatásomban a feltáró módszerre támaszkodtam.

A kutatásnál felhasznált adatok eredete szerint beszélhetünk primer vagy szekunder kutatásról (Gyulavári et. al., 2014). A kiberesetek mélyreható elemzéséhez rendelkezésre álló információ a téma újszerűsége miatt rendkívül korlátolt, ezért kutatási kérdéseim megválaszolásához a közvetlen adatgyűjtést, azaz a primer kutatást választottam, tehát magam gyűjtöttem az adatokat.

Malhotra (2001) szerint a primer adatok kvalitatív vagy kvantitatív típusúak lehetnek. A kvantitatív kutatás az adatok számszerűsítésére és a minta alapján általánosítások megfogalmazására törekszik. Ehhez nagy elemszámú és reprezentatív mintára van szükség, melyet statisztikai módszerekkel elemeznek. Ezzel szemben a kvalitatív kutatás a mögöttes okok és motivációk minőségi megértésére irányul, kisszámú, nem reprezentatív mintával dolgozik, és a probléma megértését segíti (Malhotra, 2001). Dolgozatom témájából és a kutatási kérdés bonyolultságából fakadóan kvalitatív típusú adatokat gyűjtöttem.

A kvalitatív adatgyűjtés strukturálatlan, közvetlen formáját választottam, melynek legelterjedtebb fajtái a mélyinterjú és a fókuszcsoport. Gyulavári et. al. (2014) értelmezésében a mélyinterjút többek között akkor érdemes alkalmazni, ha részletes információra van szükség, érzékeny témájú a kutatás, és az interjúalanyok szempontjainak alapos megértése a cél. Ezek a szempontok mind teljesülnek az általam elemzett problémára, így a mélyinterjús megkérdezést tartottam a leghatékonyabb információgyűjtési formának dolgozatom elemző részéhez.

Malhotra (2001) jellemzése alapján a mélyinterjú egy 30-60 perces közvetlen beszélgetés a témában képzett kérdező és a megkérdezett között. Az interjúkészítő általános kérdésekkel indít (pl.: Hallott már ön a kiberkockázatról?), majd arra ösztönzi a beszélgetőpartnerét, hogy szabadon fejtse ki véleményét az adott témában. Innentől kezdve az interjú strukturálatlan formát követ. Az interjúkészítő további kérdéseinek megfogalmazását és sorrendjét a válaszadó feleletei határozzák meg (Malhotra, 2001).

Mélyinterjúimat 2019 áprilisában vettem fel. Az interjúk során igyekeztem olyan alanyok tapasztalatát felmérni, akik valamilyen szempontból szakértők a szakmában, és releváns tudással rendelkeznek a kiberkockázat területén. Interjúalanyaimat három főbb csoportra bontottam: szakértők, biztosítók és vállalatok munkatársai.

4. A mélyinterjúk elemzése

A következő fejezetben mélyinterjúim részletes elemzését mutatom be. A fejezet felépítése az alanyok már említett csoportosítását követi (szakértők, biztosítók, vállalatok). A szakértő csoporton belül három személlyel folytattam beszélgetést: Bálint Biankával, aki a PricewaterhouseCoopers Könyvvizsgáló Kft. Risk and Assurance részlegén Senior Assistantként dolgozik; Dr. Trinh Anh Tuannal, a Budapesti Corvinus Egyetem docensével, aki a Corvinus Fintech Center és az IVSZ Fintech munkacsoport vezetője; valamint Dr. Krasznay Csabával, a Nemzeti Közszolgálati Egyetem Kiberbiztonsági Akadémiájának igazgatójával. A biztosítási szektorból Berényi Dániellel, a Generali Biztosító Zrt. kiemelt biztosítástechnikai szakértőjével készítettem interjút. A vállalati oldalról pedig Polereczki Andreát, az Inter-Computer Informatikai Zrt. Chief Cyber Security Officerét kerestem fel, aki számos korábbi szakmai tapasztalatát osztotta meg velem.

> **Az energia-, gáz-, víz-, távközlési és egészségügyi szolgáltatók különösen nagy veszélyben vannak, de a pénzügyi intézetek is fenyegetettek.**

4.1. Kiberkockázat a szakértők szemszögéből

Szakértőkkel készített mélyinterjúim alapján elmondható, hogy mindannyian releváns és komoly problémának tartják a kiberkockázatot. Úgy vélik, hogy ez a jelenség minden olyan vállalatot érint, ahol számítógépes rendszerekkel dolgoznak. Dr. Krasznay Csaba és Dr. Trinh Anh Tuan kiemelték, hogy a kritikus infrastruktúrák, mint az energia-, gáz-, víz-, távközlési és egészségügyi szolgáltatók különösen nagy veszélyben vannak, de a pénzügyi intézetek is fenyegetettek. A jövőben hatványozódni fog a kockázat mértéke, és az olyan fejlesztések területén, mint az önvezető gépjárművek, akár emberi életek is foroghatnak kockán.

4.1.1. A probléma észlelése

Interjúalanyaim úgy gondolják, hogy a növekvő fenyegetettség miatt a cégeknek kiemelt figyelmet kell fordítaniuk a biztonságra. A legfejlettebb országokban (USA, Németország, Kína) főleg a nagyobb vállalatok már tudatosan foglalkoznak a kiberkockázattal, és ez már a stratégiában is megjelenik. Interjúalanyaim szerint azonban a kisebb országokban, köztük Magyarországon, még nem alakult ki ez a tudatosság. Ezekben az országokban általában amíg

el nem éri a vállalatokat a veszély szele, addig nem motiváltak a védekezésre vagy a biztosításkötésre. Dr. Krasznay Csaba szerint a vállalatok általában akkor fektetnek pénzt a biztonságba, ha külsőleg kötelezik rá őket, ha jól felfogott érdekük fűződik hozzá, vagy ha már érte őket káresemény. Ezek közül az első a leggyakoribb. Az állami szabályozással kapcsolatban azonban Dr. Trinh Anh Tuan kiemelte, hogy a hatóságok mindig lassabban reagálnak, mint a vállalatok. Éppen ezért véleményem szerint nem szabad mindent az állami szabályozásra bízni, hiszen ez a rohamosan növekvő kockázat azonnali reagálást igényel. A megfelelő gondolkodásmód elősegítésében és a problémát érintő kutatások támogatásában azonban mindenképpen nagy szerepe lehet az államnak. Az Európai Unióban például már célzott kutatások vannak a kkv-k kiberbiztonságának növelésére. Ezek a vállalatok azért kiemelten veszélyeztetettek, mert a tudás, a szakember, a technológia és a külső nyomás is hiányzik náluk a biztonság kialakításához.

4.1.2. A biztosítók szerepe

Interjúalanyaim szerint a kiberkockázat-kezelés hatékony formája lehet a kockázat áthárítása harmadik félre, tehát a biztosítások megjelenése. Azonban biztosítástechnikai szempontból rendkívül nehezen felmérhető ez az új terület. Az adatok és a tapasztalatok hiánya nehezíti az árazást, valamint bizonytalanná teszi, hogy a biztosítók milyen károkra tudnak fedezetet nyújtani és milyenekre nem. Minél többet beszélünk azonban a károkról, annál több értékes információ kerül felszínre, és a biztosításmatematikusok annál mélyebb adatbázisból végezhetik majd becsléseiket. Azokban az országokban, ahol kulturálisan magasabb szintű a bizalom, és nagyobb figyelmet is fektetnek a biztonságra, mint például Németországban, a globális nagyvállalatok szintjén már jelen van a biztosítás, mint kiberkockázat-kezelési megoldás.

Az adatok és a tapasztalatok hiánya nehezíti az árazást.

Dr. Krasznay Csaba úgy véli, hogy az adathiányon sokat fog segíteni, hogy az incidenseket kötelező lesz jelenteni, viszont ezekről az incidensekről Magyarországon nincsenek publikus statisztikák. Erre megoldást jelenthetne, ha a Nemzeti Kibervédelmi Intézet és a Nemzeti Adatvédelmi és Információszabadság Hatóság együtt tudna működni a biztosítókkal, és hozzáférést engednének az esetekhez. A Magyar Biztosítók Szövetségénél történő egységes adatgyűjtés ugyancsak csökkentené az információhiányt. Ahhoz, hogy a cégek hajlandóbbak legyenek megosztani a hatóságokkal, egymással és a biztosítókkal tapasztalataikat, ki kell alakítani azokat az együttműködéseket, amelyek garantálják, hogy a vállalatoktól származó információ anonim marad, és nem vezethető vissza hozzájuk. Mindenkinek meg kell értenie, hogy az az információ, amit megoszt, nagyon hasznos tud lenni mások és a saját biztonsága számára is. Úgy gondolom, hogy egy ilyen szemléletmód kialakítása valóban megoldást jelenthet, ezért az államnak, a médiának, valamint a különböző oktatási intézeteknek is érdemes erre hangsúlyt fektetniük.

Amint már említettem, az Európai Unióban célként tűzték ki a kkv-k kiberbiztonságának növelését. Interjúim során megtudtam, hogy az EU 2015-ben kiírt egy olyan pályázatot, melynek kimondottan az volt a célja, hogy a kisvállalkozás–IT szolgáltató–biztosító háromszögben megvalósulhasson a kölcsönös együttműködés.

Az államilag kötelezővé tett kiberbiztosítás az interjúk alapján segíthet a biztosítás elterjedésében, de nem feltétlenül ez a leghelyesebb irány. Magyarországon a digitális bizalmi szolgáltatások terén már kötelező egy IT károkra vonatkozó felelősségbiztosítást kötni. Komoly probléma azonban ezzel kapcsolatban, hogy a cégek nehezen találják meg a szolgáltatást a hazai biztosítótársaságok portfóliójában. A kötelező biztosítás széles körű előírása Dr. Krasznay Csaba szerint versenyjogi szabályokba is ütközne. Bálint Bianka is szkeptikus az állami közbeavatkozást illetően, hiszen az tovább bonyolítaná a bürokráciát, így számottevően több szabályozást eredményezne a cselekvés helyett. Dr. Trinh Anh Tuan azon a véleményen van, hogy az elrettentés nem jó módszer a cégek figyelmének felhívására. Úgy gondolom, a kötelező biztosítás azért sem reális, mert az állami cégeknek hatalmas költségeket jelentene, a magáncégek pedig nem szívesen adnának ki adatot állami intézménynek.

4.2. Kiberkockázat a biztosítók szemszögéből

A Generali Biztosító Zrt. valós és folyamatosan növekvő fenyegetésnek tekinti a kiberkockázatot, mely a magánszemélyek mellett a vállalati szektort is jelentősen veszélyezteti. Nemzetközi szinten egyre hevesebb az érdeklődés a számítógépes kockázatok biztosításában rejlő lehetőségekkel kapcsolatban. Ezért a Generalinál kiemelt feladatnak tartják a kiberbiztosítási irány fejlesztését, ami azonban számos akadályba ütközik. A legkomolyabb problémát az jelenti, hogy a megfelelő kártapasztalat hiánya miatt a kár nagyságát és gyakoriságát is nehéz megbecsülni. Ennek kiküszöbölésére holding szinten érkezett egy kérés a biztosítók felé, hogy tapasztalatszerzés céljából iktassák be portfóliójukba a kiberbiztosítást alacsony biztosítási díjak mellett, hogy minél több ügyfél ismerkedhessen meg az új fedezettel.

4.2.1. A Generali kiberbiztosítási terméke

A biztosító Magyarországon 2018 októberében kezdett el kiberfedezetet nyújtani, jellemzően a vagyon- és felelősségbiztosítási csomag részeként. A biztosítás főleg kkv-k részére köthető, mivel a nagyobb vállalatok nagyobb kockázataihoz már több tapasztalatra és magasabb fedezeti limitekre lenne szükség.

A kiegészítő biztosításnak három lába van: az első a szoftver- és adatvesztési biztosítás. Ez a számítógépen tárolt adatállományra és a szoftverekre terjed ki. Hackertámadás, rosszindulatú (kártevő) program, valamint munkavállalói hiba miatt keletkező károkra nyújt fedezetet. Adatvesztés esetén az érintett vállalat megbíz egy informatikai céget

az adatok visszanyerésére, és ennek az adatvisszanyerésnek, valamint a vírusirtásnak a költségét téríti a biztosító. A fedezeti limitek és biztosítási díjak alakulása a következő:

Biztosítási összeg	Biztosítási díj
250 000 Ft	5 000 Ft
500 000 Ft	10 000 Ft
750 000 Ft	15 000 Ft

Egy nagyobb, multinacionális vállalat már nem férne bele ezekbe a limitekbe, a kkv-k azonban viszonylag alacsony díjért cserébe biztosíthatják kiberkockázatukat.

A biztosítás második lába a kiber üzemszünet fedezet, mely az adatvesztés okozta üzemszünet miatt elszenvedett bevételkiesés, valamint a leállás alatti fix költségek térítésére vonatkozik a következő limitekkel:

Biztosítási összeg	Biztosítási díj
100 000 Ft	6 000 Ft
200 000 Ft	12 000 Ft
300 000 Ft	18 000 Ft

A kiegészítő biztosítás harmadik része a felelősségbiztosítási fedezet. Ha személyes adatok szivárognak ki a cégtől, akkor az ezzel kapcsolatosan okozott károkat, illetve sérelemdíjakat fizeti a biztosító. A fedezeti limit ebben az esetben maximum 30 millió Ft káronként, és 100 millió Ft évente, a díj pedig a tevékenységi felelősségbiztosításra fizetendő 30 százalékos pótdíj. A biztosításnak ez a része leginkább a GDPR szabályozás bevezetésével lett népszerű.

Kizáró tényező például, ha a vállalat saját fejlesztésű vagy nem jogtiszta szoftverekkel dolgozik.

A biztosító jelenleg még nem végez előzetes kockázatfelmérést, viszont mindhárom kiberbiztosítási terület esetében megállapítja a fedezetet kizáró tényezőket. Ilyen tényező például, ha a vállalat saját fejlesztésű vagy nem jogtiszta szoftverekkel dolgozik.

A kiegészítő csomag népszerűsítése különböző portálok és cikkek támogatásával kezdődött. A HVG-n például több olyan írás is megjelent, melyek felhívták olvasóik figyelmét a kiberkockázatokra, és beszámoltak a közelmúlt leghíresebb kiberkáreseményeiről.

A bevezetést követő első negyedévben az új kötések és szerződésmódosítások 10%-ánál szerepelt legalább egy kiberkiegészítő. Ez az arány kifejezetten magasnak mondható. 210 új üzletet kötöttek szoftver és adatvesztés biztosítására, 86-ot kiber felelősségbiztosításra, és 19-et kiber üzemszünet biztosítására. A legélénkebb érdeklődés tehát kimagaslóan az adatvesztésre szóló fedezet iránt mutatkozott, ami arra enged következtetni, hogy ettől a kockázattól tartanak leginkább a vállalatok. A biztosító eddigi tapasztalatai alapján is a külső támadás okozta adatvesztések fordulnak elő a legtöbbször.

4.2.2. A biztosítást akadályozó tényezők

A szakirodalom által egyik legkomolyabb problémának tartott morális kockázat ellen a Generali a biztosítási szerződésbe iktatott kizárásokkal védekezik. A biztosított félnek gondoskodnia kell a megfelelő jelszókezelésről, a hozzáférések szabályozásáról, a tűzfalak szakszerű beállításáról, valamint a vírusirtók és az operációs rendszerek folyamatos frissítéséről. A kár bekövetkezte esetén az ügyfél által az adatvisszanyerésre megbízott szakértő cég megvizsgálja, teljesültek-e ezek a feltételek, és amennyiben nem, úgy a biztosító nem fizet. Ilyen esetekben azonban, úgy gondolom, jogosan vetődhet fel a kérdés, hogy az adott szakértő cég pártatlan-e, és véleménye dönthet-e egy ilyen szituációban. Ennek a problémának a kiküszöbölésére a Generali egy profi IT partnerrel szeretne leszerződni, akit akár kockázatelbírásra, akár az ügyfelek folyamatos ellenőrzésére is felkérhetnek. Ezáltal lehetséges lenne a nagyobb vállalatok biztosítása is önálló biztosítási termékekkel. Jelenleg azonban nem létezik olyan konkrét cég, amelyre ezt a feladatot rá lehetne bízni.

Arra a kérdésemre, hogy az ügyfelek mennyire hajlandóak megosztani érzékeny adatokat a biztosítóval, azt a választ kaptam, hogy ez az adott ország kultúrájától függ. Az osztrák cégek például teljesen megbíznak a biztosítókban, így gördülékenyebb az együttműködés. Magyarországon ez a bizalom kevésbé van jelen, ezért – különösen a kisebb vállalatok esetében – gyakran előfordul, hogy bizonyos információkat nem szívesen osztanak meg.

Problémát jelent még, hogy előzetes kockázatfelmérés hiányában a biztosító nem képes felmérni, hogy az adott ügyfél munkavállalói milyen oktatást kapnak a kiberkockázatról. Erre külföldön (például Csehországban) már létezik megoldás egy 110 kérdéses kérdőív formájában, amelynek hossza azonban sok ügyfél számára elrettentően hat. Véleményem szerint az effajta kérdőíves felmérés hatékonyabb lehetne, ha sikerülne csökkenteni a kérdések számát, és kiegészíteni a vizsgálatot egy biztonsági átvilágítással. Ez a gyakorlat több helyen is elterjedt, amint arról a szakirodalmi összefoglalóban is szó esett. A nagyobb vállalatok esetében mindenképpen szükség van mélyreható vizsgálatra, azonban a kkv-k esetében az is megoldást jelenthet, ha a biztosító tart kampány jellegű oktatást a munkavállalóknak. Úgy gondolom, a cégeknek ilyenkor akár az oktatási anyag miatt is megérheti fedezetet kötni. Fontos, hogy az oktatóanyagot szakértők állítsák össze, de a hétköznapi emberek számára is érthető legyen.

A vállalatok tájékozatlansága szintén akadályokat gördíthet a biztosításkötések elé. Noha a Generali szerint a nagyobb cégek felkészültebbek a kiberkockázatok kivédésére, és hajlandóak lehetnek biztosítást kötni, azonban a kisebb vállalatok számára Magyarországon még nem annyira kézzelfoghatók ezek az esetek, mint mondjuk a víz- vagy tűzkárok. Legtöbbükben akkor tudatosul a veszély mérete, mikor megtörténik velük a baj. Az esetek növekvő médiavisszhangja azonban segíthet ezen a problémán.

4.2.3. Lehetőségek a jövőre nézve

A Generali rendkívül innovatívan áll a kiberkockázathoz, és folyamatosan igyekszik kidolgozni olyan új megoldásokat, melyek elősegítik e biztosítási irány hatékonyságát. Ezt a célt szolgálták többek között a kétnapos, kiberbiztosításról szóló prágai workshopok, melyek során egymás tapasztalataira építve dolgoztak az új megoldásokon.

Ausztriában már használnak fedezetellenőrző szoftvert, mely rendszeresen küld jelzést, hogy érvényes-e a biztosítás.

Hogy képesek legyenek a jövőben emelni a fedezeti limiteket, Magyarországon jelenleg egy olyan szoftver/applikáció létrehozását tervezik, mely folyamatosan ellenőrzi az ügyfél tűzfalbeállításait, a vírusirtó működését, valamint frissülését. Ausztriában már használnak hasonló fedezetellenőrző szoftvert, mely rendszeresen küld jelzést a biztosítónak és az ügyfélnek is, így mindkét fél figyelemmel kísérheti, hogy érvényes-e a biztosítás. Amint már említettem, egy önálló termék kidolgozása is a tervek között szerepel, mely kihasználná a nagyobb pénzügyi és egészségügyi intézetek kiberbiztosításában rejlő potenciált.

A Generali hivatalos assistance partnerével, a Europ assistance-szel, egy IT segítségnyújtás jellegű szolgáltatás kidolgozásán is dolgozik, mely főleg a kiberkockázatot kevésbé ismerő kkv-k számára lenne hasznos. A szolgáltatás keretein belül a biztosító által küldött szakértő segítene a vállalat gépeire feltelepíteni a megfelelő védelmi rendszereket. Az IT assistance azonban nem csak a kisebb cégek esetén működhet. Ugyan a nagyvállalatok általában szakképzett informatikus csapattal rendelkeznek, egy komolyabb vírustámadás menedzselésére valószínűleg nem állnak készen. Ilyen krízisek kezelésében segíthetne a biztosító partnereként működő etikus hackercsoport. Úgy gondolom, az ilyen hackercsoportok alkalmazása minden vállalatnak segítségére lehet, hiszen ők az egyetlen szakértők, akik fel tudják venni a versenyt a rossz szándékú hackerekkel, akik általában a vállalatok és a biztosítók előtt járnak néhány lépéssel.

Összefoglalva tehát a Generali célja, hogy a jövőben elinduljon egy olyan önálló, versenyképes termék, amely a szoftveres kockázatelbírálás mellett az assistance szolgáltatásra és az oktatásra épülne.

Legvégül azt vizsgáltam, hogy a Generali szerint mennyiben segítené a biztosítás elterjedését egy esetleges erre irányuló szabályozás. Az állami szabályozás megalkotását nem tartja valószínűnek a közeljövőben a biztosító. Azonban egy Európai Unió-szintű rendelet – mint például a GDPR – bevezetése, mely a médiában is nagy hangsúlyt kapna, segíthetne felhívni a vállalatok figyelmét a kiberkockázatra, és igényt ébreszteni bennük annak biztosítására.

4.3. Kiberkockázat a vállalatok szemszögéből

Ebben az alfejezetben a vállalatok nézőpontjából vizsgálom a kiberkockázatot. Polereczki Andrea több olyan vállalatnál is dolgozott, amely érzékeny digitális információkat kezel. Az interjú keretein belül számos szakmai tapasztalatáról számolt be részletesen. Felfogásában a kiberkockázat folyamatos kihívást jelent a digitális élet változó körülményeivel szemben.

A számítógépes adatállomány védelme miatt Polereczki Andrea fontosnak tartja, hogy a cégek már a digitális infrastruktúra kialakításakor elvégezzék a szektorspecifikus kezdeti kockázatelemzéseket operációs rendszer szinten. Meg kell vizsgálni, melyek a releváns kiberkockázatok, majd meg kell állapítani egy elfogadható kockázati szintet a szakirodalmi részben már elemzett Gordon et. al. (2003) útmutatójában írtakhoz hasonlóan.

Polereczki Andrea elmondása szerint egy korábbi cégénél előfordult, hogy az elfogadható szint fölötti kockázatok esetében a lehetséges károk fedezésére biztosítást szerettek volna kötni, azonban ez nem sikerült. Megvizsgálták annak a lehetőségét, hogy az internetszolgáltatói kiesés esetében milyen feltételekkel lenne lehetőség biztosítást kötni, viszont a biztosítóval történő egyeztetések alkalmával nem született minden fél számára megfelelő megoldás. A legfőbb probléma az volt, hogy a biztosító által ajánlott konstrukciók nem terjedtek ki a vállalat igényeinek lefedésére.

Amennyiben találtak is volna megfelelő ajánlatot, akkor is nehéz lett volna megkötni a biztosítást, mivel a vállalat nem oszt meg semmilyen érzékeny információt a külső intézetekkel, még cégen belül is szigorúan korlátozva vannak a jogok és hozzáférések. Interjúalanyom elmondása szerint egy esetleges incidens után sem lennének hajlandóak információt megosztani, hiszen ez az adatok további kiszivárgásával járna. Ezek alapján is elmondható tehát, hogy rendkívül nehéz megvalósítani a vállalatok és a biztosítók közötti együttműködést.

5. Eredmények, következtetések

A szakértőkkel, valamint biztosítók és vállalatok munkatársaival készített mélyinterjúim alapján egyértelműen megállapítható, hogy a kiberkockázat minden vállalat számára növekvő fenyegetést és folyamatos kihívásokat jelent. Ebből is adódik, hogy a kiberbiztosítás iránt világszerte nő az érdeklődés. Nemzetközi szinten léteznek hatékony megoldások a digitális károk biztosítására, azonban a terület újdonsága és a kockázat felmérhetősége miatt a legtöbb biztosító még nem jutott el a terméktervezéshez. Így azok a vállalatok, amelyek szeretnének fedezetet vásárolni, általában nem találják a nekik megfelelő szolgáltatást a biztosítók portfóliójában, vagy végül nem születik megállapodás a felek között. A legnagyobb problémát a tapasztalat- és adathiány okozza. Mivel kiberkárok terén nem rendelkeznek a biztosítók elegendő információval, gyakran nem megfelelően árazzák termékeiket. A kontraszelekció, azaz, hogy a vállalatok csak az első kár bekövetkezte után vásárolnak fedezetet, szintén akadályozó tényező. A vállalati és biztosítói munkatársakkal készített interjúk során is meggyőződtem arról, hogy Magyarországon a cégek a kultúrából fakadóan is rendkívül bizalmatlanok, és nem szívesen osztanak meg belső információt harmadik féllel. Ez a jelenség ugyancsak gátolja a biztosítás létrejöttét.

Itthon a Generali Biztosító az elsők között tette elérhetővé a kiberkárok biztosítását. A biztosító alacsony fedezeti limitek és biztosítási díjak mellett nyújt kiberfedezetet a vagyon- és

felelősségbiztosítási csomag részeként. Ez a termék főleg a kkv-kat célozza, és leginkább tapasztalatszerzési céljai vannak. Az ügyfelekkel kötött szerződések tartalmaznak bizonyos feltételeket, melyek a morális kockázattól védik a biztosítót. A Generali még nem végez kockázatelemzést a vállalatoknál, viszont a fedezeti limitek emelése céljából a jövőben tervezik bevezetni egy olyan szoftver használatát, amely folyamatosan ellenőrzi az ügyfél digitális rendszereinek állapotát. Noha hatékony eszköznek tartom a kockázatelemzésnek ezt a formáját, a szoftver használata valószínűleg akadályokba fog ütközni a bizalmatlanabb ügyfelek körében.

A terület újdonsága miatt a legtöbb biztosító még nem jutott el a terméktervezéshez.

Egy másik irányvonal – amelyen jelenleg a Generali dolgozik – egy olyan termék, amely a szoftveres kockázatelbírálás mellett az assistance szolgáltatásra, valamint az ügyfelek oktatására épülne. Ez leginkább azoknak a kkv-knak lehetne hasznos, amelyek nem rendelkeznek a kiberbiztonság megteremtéséhez szükséges tudással és forrásokkal. Az EU2020 részeként 2015-ben már az Unió is célként tűzte ki, hogy a kisvállalkozások, az IT szolgáltatók és a biztosítók között megvalósuljon a kölcsönös együttműködés.

A kiberbiztosítás szélesebb körű elterjedését segítheti, ha a vállalatoknak kötelező bejelenteniük incidenseiket, valamint, ha a biztosítók hozzáférnek az ilyen esetekről készült statisztikákhoz. Így a biztosításmatematikusok nagyobb adathalmazzal dolgozhatnak, és pontosabb díjkalkulációt érhetnek el. Az állam által kötelezővé tett biztosítás is a potenciális megoldások közé sorolható, ugyanakkor az interjúválaszokból arra következtetek, hogy nem ez lenne a legeredményesebb megoldás. A szabályozás ugyanis könnyen sértheti a versenyjogot, és túlbonyolított bürokráciát eredményezhet. A kényszerből való biztosításkötésnél hatékonyabb, ha az adott vállalat megérti, mit jelent számára a kiberkockázat, és tudatosan dönt a biztosítás mellett.

Kutatásom alapján arra a végső következtetésre jutottam, hogy a cégeknek sokkal tudatosabban kell hozzáállniuk a kiberkockázathoz, és meg kell érteniük a biztonság lényegét. A növekvő fenyegetettség következményeként a kiberbiztosítás a jövőben hatalmas fejlődést produkálhat. Ehhez azonban elengedhetetlen, hogy a vállalatok, a biztosítók és az IT szakemberek rendszeresen kommunikáljanak egymással, megosszák tapasztalataikat, és kialakuljon köztük egy olyan bizalmi együttműködés, amely lehetővé teszi a kockázatok eredményes csökkentését és áthárítását.

6. Jövőbeni kutatási lehetőségek

Jövőbeni kutatási lehetőségként javaslom a vállalatok fókuszcsoportos elemzését, hiszen így alkalom nyílik a nézetek ütköztetésére, többféle álláspont megismerésére és a különböző tapasztalatok összevetésére. Azonban ez a módszer is csak akkor működhet, ha a résztvevők számára garantált a bizalmas közeg. Érdemes továbbá a külső szabályozás hatékonyságának kutatásához elemezni a már létező rendeletek, nemzetközi megállapodások eredményességét. A komolyabb, nagy összegű károk fedezésére célszerű megvizsgálni a veszélyközösségek kibővítésének lehetőségét, valamint a kockázat esetleges szétosztását a biztosítótársaságok között.

A folyamatos tanulás, az innovatív hozzáállás és a legjobb gyakorlat megismerése minden vállalat számára hasznos támponttal szolgálna a kiberkockázatok jelentette kihívásokkal szemben, ezért ezeket a területeket tartom a legfontosabbnak a további kutatások szempontjából.

IRODALOMJEGYZÉK

Bailey, L. M. D. (2014): Mitigating Moral Hazard in Cyber-Risk Insurance. 3 J.L. & Cyber Warfare 1 (2014)

Bandyopadhyay, T. – Mookerjee, V.S. – Rao, R. C. (2009): Why IT Managers Don't Go for Cyber-Insurance Products. Communications of the ACM, Vol. 52. No. 11. pp. 68–73.
http://dx.doi.org/10.1145/1592761.1592780

Berliner, B. (1985): Large Risks and Limits of Insurability. The Geneva Papers on Risk and Insurance, Vol. 10. No. 37. pp. 313–329.
http://dx.doi.org/10.1057/gpp.1985.22

Biener, C. – Eling, M. – Wirfs, J. H. (2015): Insurability of Cyber Risk: An Empirical Analysis. The Geneva Papers on Risk and Insurance Issues and Practice, Vol. 40. No. 1. pp. 131–158.
http://dx.doi.org/10.1057/gpp.2014.19

Biztosítási Szemle (2019a): Kibertámadások: három tényezőn múlik egy szervezet biztonsága.
Letöltés helye: http://www.biztositasiszemle.hu/cikk/hazaihirek/gazdasag/kibertamadasok_harom_tenyezon_mulik_egy_szervezet_biztonsaga.8795.html
Letöltés dátuma: 2019.02.07.

Biztosítási Szemle (2019b): Az európai cégek több mint felét érte már veszélyes kibertámadás.
Letöltés helye: http://www.biztositasiszemle.hu/cikk/hazaihirek/gazdasag/az_europai_cegek_tobb_mint_felet_erte_mar_veszelyes_kibertamadas.8879.html
Letöltés dátuma: 2019.03.21.

Cebula, J.J. – Young, L.R. (2010): A Taxonomy of Operational Cyber Security Risks, Technical Note CMU/ SEI-2010-TN-028. Software Engineering Institute. Carnegie Mellon University

European Commission (2018): Cybersecurity Act.
Letöltés helye: https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en
Letöltés dátuma: 2019.02.24.

Eling M. – Schnell W. (2016): Ten Key Questions on Cyber Risk and Cyber Risk Insurance. The Geneva Papers, Zürich

Gordon, L. A. – Loeb, M. P. – Sohail, T. (2003): A framework for using insurance for cyber-risk management. Communications of the ACM, Vol. 46. No. 3. pp. 81–85.
https://doi.org/10.1145/636772.636774

Gulyás Attila (2017): Egy hatékony kiberbiztosítási piac működésének támogatása. Biztosítás és Kockázat, 4. évf. 3. sz. pp. 76–93.
https://doi.org/10.18530/bk.2017.3.76

Gyulavári Tamás – Mitev Ariel Zoltán – Neulinger Ágnes – Neumann-Bódi Edit – Simon Judit – Szűcs Krisztián (2014): A marketingkutatás alapjai. Akadémiai Kiadó, Budapest
http://dx.doi.org/10.1556/9789630598880

Kesan, J.P. – Majuca, R. P. – Yurick, W. J. (2014): Cyberinsurance as a market-based solution to the problem of cybersecurity: a case study. University of Illinois at Urbana-Champaign, Illinois

Malhotra, N. K. (2001). Marketingkutatás. Műszaki könyvkiadó, Budapest
http://dx.doi.org/10.1556/9789630598675

Marsh & McLennan Agency (2018): Managing Cybersecurity: The Cyber Risk Perception Survey.
Letöltés helye: https://www.marshmma.com/blog/2018-cyber-and-data-security-risk-survey-report
Letöltés dátuma: 2019.04.28.

Ötvös Gergő (2016): Kiberbiztosítási Trendek. Biztosítás és Kockázat, 3. évf. 1. sz. pp. 58–69.
http://dx.doi.org/10.18530/BK.2016.1.58

Pandurics Anett – Markó Olga (2015): A felelősségbiztosítások szerepe, jelene és jövője Magyarországon. Biztosítás és Kockázat, 2. évf. 3. sz. pp. 78–93.
http://dx.doi.org/10.18530/BK.2015.3.78

Risk.net (2019): Operational risk.
Letöltés helye: https://www.risk.net/definition/operational-risk
Letöltés dátuma: 2019.04.21.

Shackelford, S. J. (2012): Should your firm invest in cyber risk insurance? Business Horizons No. 55. pp. 349–356.
http://dx.doi.org/10.1016/j.bushor.2012.02.004

Statista (2015): Does your organization purchase cyber liability insurance?
Letöltés helye: https://www.statista.com/statistics/424905/ownership-of-cyber-liability-insurance-europe/
Letöltés dátuma: 2018.05.10.

Statista (2016): Leading risks to business in the United States in 2016.
Letöltés helye: https://www.statista.com/statistics/422203/leading-business-risks-usa/
Letöltés dátuma: 2018.05.06.