

A gazdasági bűnözés konstans veszélyt jelent

2018. évi felmérés a globális és magyar gazdasági bűnözésről és visszaélésekről



Tartalom

	1. Magyarországi körkép-körkép	5
	A visszaélések gyakoribbá váltak – vagy csak javult az azokkal kapcsolatos tudatosság?	5
	„Vakfoltok”: mi az, amit nem látunk?	5
	Milyen visszaélésekkel szembesültek a magyar vállalatok?	6
	Válogassa meg üzletfeleit!	7
	A visszaélések továbbra is jelentős költségeket okoznak	8
	A költségeken túl	9
	Megfelelés ellentétés elvárásoknak	10
	2. Visszaélések napjainkban	11
	2.1 Kiberbűnözés: a célok és eszközök nincsenek összhangban egymással	11
	2.2 Üzleti szabályszegés és a mögöttes üzletviteli kockázat	13
	2.3 Vesztegetés és korrupció – egy valószínű „vakfolt”?	14
	2.4 Pénzmosás	15
	3. Felkészültségből jeles?	16
	3.1 A visszaélés kockázata még mindig nagyobb, mint a felderített esetek száma	16
	3.2 A rendszerszintű mechanizmusok fontos szerepet játszanak a visszaélések felderítésében	18
	3.3 Megfelelési programok, a visszaélések elleni küzdelemre fordított összegek	19
	4. Állítsuk a technológiát a visszaélések elleni küzdelem szolgálatába!	20
	Technológia-adaptációs trendek: az arany középut megtalálása	22
	Az ügyfelek nem csak egy tényezőt jelentenek a sok közül	22
	Mi történik az ügyfelek pénzével?	23
	Üzleti indokoltság	23

Előszó

Elemzésünkben a globális és magyar gazdasági bűnözésről és visszaélésekről készült 2018. évi felmérésünk eredményeit mutatjuk be, mely világszerte a legátfogóbb kutatás ebben a témában. Ahhoz, hogy naprakész áttekintést adjunk a gazdasági bűnözés jelenlegi helyzetéről, megítéléséről, hatásairól és a vállalatok gazdasági bűnözéssel kapcsolatos tudatosságáról, a felmérésbe 123 országból 7 228 szervezetet, köztük 71 vezető magyarországi céget vontunk be.

A gazdasági bűnözésről és a visszaélésekről szóló ideai felmérésünk az általános helyzetértékelésen túl kiterít a valamennyi szervezetet érintő legfontosabb stratégiai kihívásokra is – úgy, mint a jogszabályoknak való megfelelés, a technológia szerepe a visszaélések elleni küzdelemben és a kiberbűnözés.

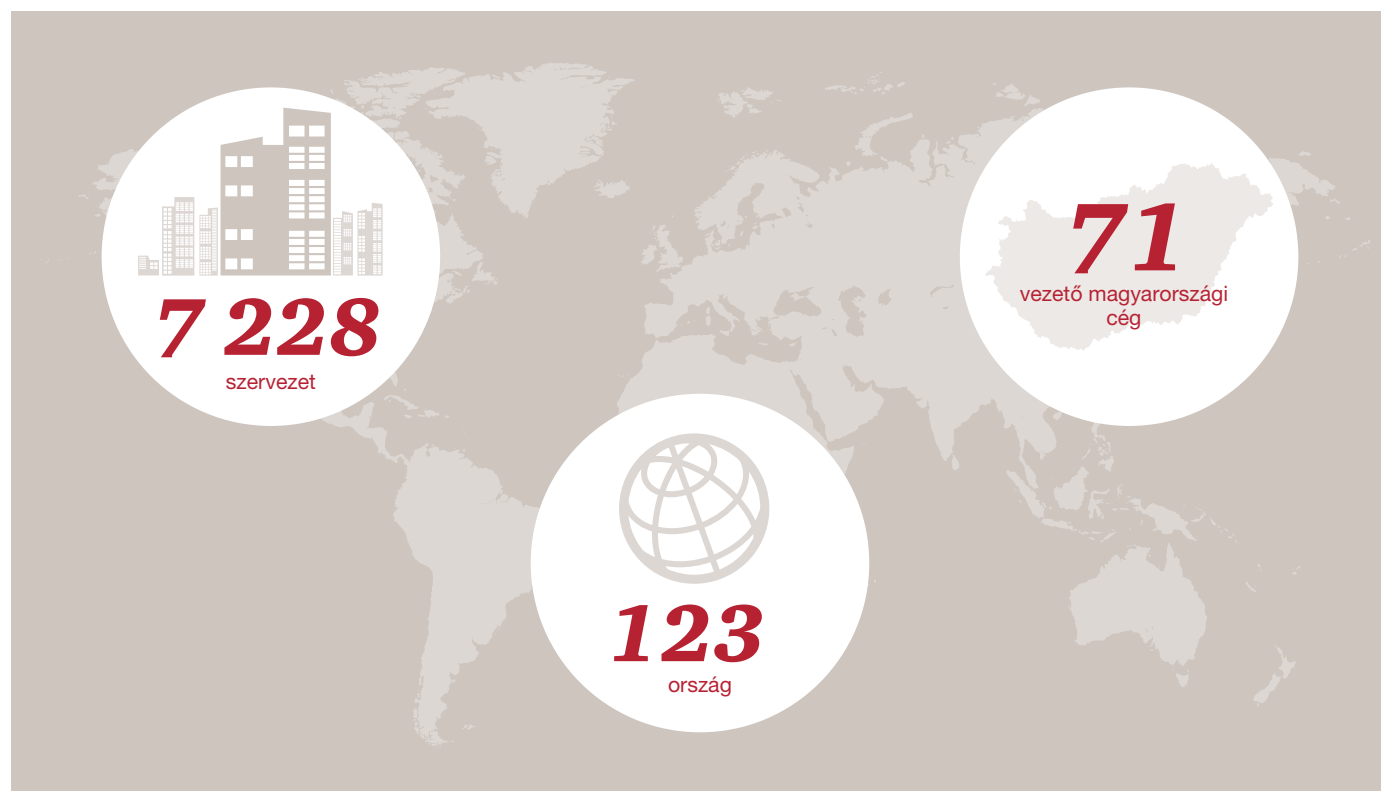
Felmérésünk eredményei azt mutatják, hogy számos vállalat belső, illetve külső okok miatt nincs kellően felkészülve a visszaélések kezelésére. Ezért fontos, hogy egy szervezet minden szintjén tisztában legyenek azzal, hogy mi minősül visszaélésnek, illetve milyen intézkedéseket lehet és kell tenni megakadályozásuk érdekében. A „vakfoltok” megszüntetése továbbá komoly lehetőségeket nyithat meg.

A visszaélések elleni küzdelem operatív, illetve jogi kérdésből mára üzleti problémává vált. A gazdasági bűnözés ma már fejlett technológiát használó, innovatív, opportunisták és mindenütt jelen lévő üzleti vállalkozássá vált. Úgy is felfog-

ható, mint az Ön vállalatának legjelentősebb, ezidáig ismeretlen versenytársa. Milyen út vezetett ide? A technika ugrásszerűen fejlődött; a visszaélések elkövetői egyre jelentősebb célokat tűznek ki, módszereik pedig egyre kifinomultabbak; a szabályozási rendszerek viszont sokkal robusztusabbá váltak – a világ nagy részén fokozódik a bűnüldözési tevékenység, gyakran nemzetközi együttműködések keretében.

Itt az idő, hogy a szervezetek a visszaélésekhez egy új, holisztikusabb szemléletmóddal közelítsenek, felismerve, hogy azok nem pusztán kellemetlenséget, a vállalkozás „járulékos költségeit” jelentik, hanem egy valódi árnyék-iparágat képeznek. Mivel a visszaélések rejtve zajlanak, veszélyes nem ismerni a szervezeten belüli hatásmechanizmusukat. Ezért a lényeges kérdés nem az, hogy az Ön cége visszaélés áldozata-e, hanem, hogy Ön tisztában van-e azzal, hogy az hogyan érinti az Ön cégét: vakon vagy nyitott szemmel veszi fel a harcot ellene?

Végül szeretnénk köszönetet mondani a felmérés résztvevőinek, amiért megosztották velünk tapasztalataikat és meglátásaikat. Külön köszönjük a felmérésben való részvételt a magyarországi válaszadóknak. A felmérés résztvevői mindannyian osztják azt a meggyőződésünket, hogy a gazdasági bűnözés túlságosan költséges ahhoz, hogy szemet hunyjunk felette.



Kiadványunk kiemelt témái



A gazdasági bűnözés jelenlegi környezete Magyarországon

- A felmérésünk szerint a globális szervezetek 49%-a ismerte fel, hogy visszaélés, illetve gazdasági bűncselekmény áldozatává vált. Magyarországon ez az arány még magasabb, 51%.
- A magyarországi felmérés válaszadói továbbra is a hűtlen kezelést (42%) jelölték meg a leggyakrabban elkövetett gazdasági bűncselekményként. Ezt követik az „újfajta” visszaélések, melyek jelentősége olyan mértékben nőtt, hogy a felmérésben első alkalommal tüntettük fel azokat külön kockázati tényezőkként. Ilyenek például a fogyasztók által elkövetett visszaélések (39%) és az üzleti szabályszegés (28%), melyek a válaszokban megjelölt összes visszaélés közül a második, illetve negyedik helyen állnak.
- Az egyik legnagyobb kockázati tényezőt az üzletfelek jelentik. A felmérés alapján a vállalatokat legérzékenyebben érintő visszaéléseket Magyarországon többnyire külső felek követik el (58%), ami szembetűnő változás a korábbi felmérésünkhöz képest (33%). Azokban az esetekben, amelyekben a visszaélést külső fél követte el, a „külső felek” csoportjának jelentős hányadát valójában „hamis barátok” („frenemies”), vagyis harmadik felek – megbízottak, szállítók – és ügyfelek alkotják.
- A visszaélések továbbra is jelentős költségeket okoznak: a felmérésben részt vevő gazdasági bűncselekményeket elszenvedő vállalatok 45%-a hozzávetőlegesen 100 000 amerikai dollárt veszített Magyarországon.



Kiberbűnözés

- A kiberbűnözés bűnözés felnőttkorba lépett és a 2016-ban készült legutóbbi felmérésünk óta jelentősen nőtt – ez a harmadik leggyakrabban elkövetett gazdasági bűncselekmény.
- A válaszadók 31%-a tapasztalt valamilyen számítógépes bűnözéssel kapcsolatos visszaélést, és Magyarország ebben a tekintetben elérte a globális szintet. A gazdasági bűncselekmények közül a kiberbűnözés területén mértük az eddig legnagyobb mértékű növekedést.

- Számos fajtája közül Magyarországon leggyakrabban a kártevő szoftverek (44%) és az adathalászat (37%) fordul elő.
- A magyar vállalkozások egyre inkább tisztában vannak ezzel a fenyegetéssel, amit az is mutat, hogy egyre többen rendelkeznek kiberbiztonsági programmal a kibertámadások elhárítására. A 2016-os felmérésben mért 42%-kal szemben idén a megkérdezettek 72%-a nyilatkozta, hogy saját cége rendelkezik kiberbiztonsági programmal a támadások elhárítására.
- Ugyanakkor a magyarországi válaszadók 10%-a úgy nyilatkozott, hogy cége nem rendelkezik ilyen tervvel, és még csak nem is fontolgatja annak elkészítését.



Etika és megfelelés

- A közvélemény és a hatóságok egyre inkább a felső vezetőket tartják személyesen felelősnek a gazdasági bűncselekményekért és a visszaélésekért. Erre utal az is, hogy a magyarországi válaszadók 17%-a szerint elsődlegesen a vezérigazgatók felelősek a vállalat formális üzleti etikai és megfelelési programjáért.
- A vállalatok egyre több visszaélést derítenek fel rendszerszintű mechanizmusokon keresztül: a 2016. évi felméréshez képest 42%-ról 54%-ra emelkedett azoknak a magyarországi vállalatoknak az aránya, amelyek a vállalati kontrollokra támaszkodnak a visszaélések felderítésében.
- A gazdasági bűncselekmények 21%-ára azonban még mindig olyan módon derül fény Magyarországon, amelyre a vállalat vezetésének nincs befolyása.

1. Magyarországi körkép-körkép

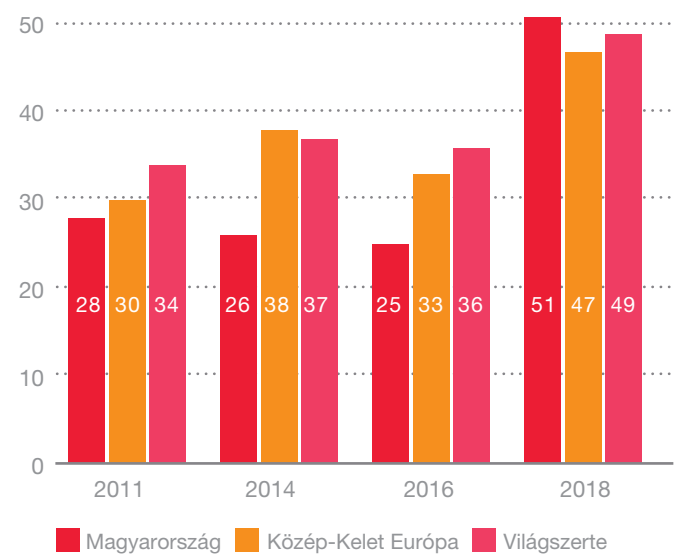
A visszaélések gyakoribbá váltak – vagy csak javult az azokkal kapcsolatos tudatosság?

A PwC 2018. évi magyarországi gazdasági bűnözésről és visszaélésekről szóló felmérése szerint a megkérdezett hazai vállalatok több mint fele tapasztalt valamilyen gazdasági bűncselekményt az elmúlt 24 hónapban, ami a legutóbbi felméréshez képest 100%-os növekedést jelent.

Ez az eredmény azonban félrevezető: valószínűleg nem a tényleges visszaélések száma nőtt ilyen mértékben, hanem az azokkal kapcsolatos tudatosság javult. Jelentésünkkel erre a tudatossági hézagra igyekszünk felhívni a figyelmet. Nem csak azt vizsgáljuk, ami látható, hanem azokat a „vakfoltokat” is, amelyektől a vállalatok nem veszik észre a körükben zajló visszaéléseket, illetve azt, hogy mit lehetne és kellene tenniük azok ellen.

1. ábra

Kérdés: Az elmúlt 24 hónapban tapasztalt vállalatánál gazdasági bűncselekményt? Igen válaszok aránya (%)



„Vakfoltok”: mi az, amit nem látunk?

Ahogy azt jelentésünkben kifejtjük, minden vállalatnál előfordulhatnak „vakfoltok” – olyan tudatossági vagy felelősségi hézagok, amelyek még a legjobban vezetett cégek számára is problémát jelenthetnek. Leggyakrabban ezekre csak valamilyen incidens kapcsán derül fény – legyen az kibertámadás, hatósági vizsgálat, bűnüldöző szerv intézkedése, kínos tartalmú sajtóanyag, vállalaton kívülről,

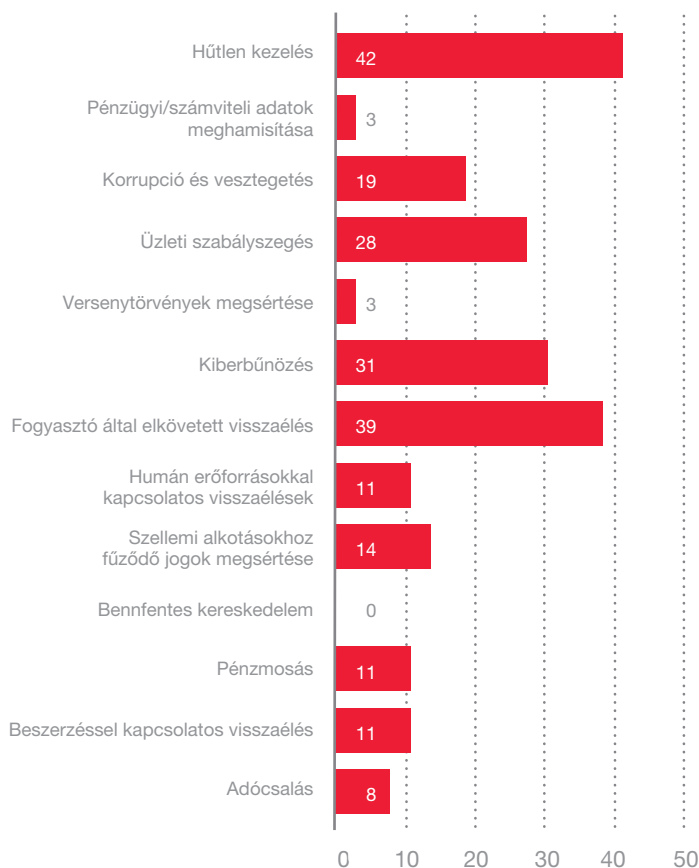
illetve belülről érkező figyelmeztetés. Ugyanakkor az ilyen vakfoltok feltérképezése nyomán megelőző intézkedések tehetők, illetve jelentősen javítható a visszaélések elleni erőfeszítések hatékonysága. Ez a magyarországi és a globális gazdasági bűnözésről készült idei felmérésünk egyik központi témája.

Milyen visszaélésekkel szembesültek a magyar vállalatok?

A magyarországi felmérés válaszadói továbbra is a hűtlen kezelést (42%) jelölték meg a leggyakrabban elkövetett visszaélésként. Ezt követik az „újfajta” visszaélések, melyek jelentősége olyan mértékben nőtt, hogy a felmérésben első alkalommal tüntettük fel azokat külön kockázati tényezőkként. Ilyenek például a fogyasztók által elkövetett visszaélések (39%) és az üzleti szabályszegés (28%), melyek a válaszokban megjelölt összes visszaélés közül a második, illetve negyedik helyen állnak. Véleményünk szerint részben e két kategória megjelenésének tudható be a hűtlen kezelés szélesebb kategóriájában tapasztalt csökkenés (2016-ban 46%, 2018-ban 42%). A kiberbűnözés, amit a válaszadók 31%-a jelölt meg, a harmadik helyre került. Ez összhangban áll a kelet-európai és a globális eredményekkel: a hűtlen kezelés, a kiberbűnözés és a fogyasztók által elkövetett visszaélések mindenhol jelen vannak.

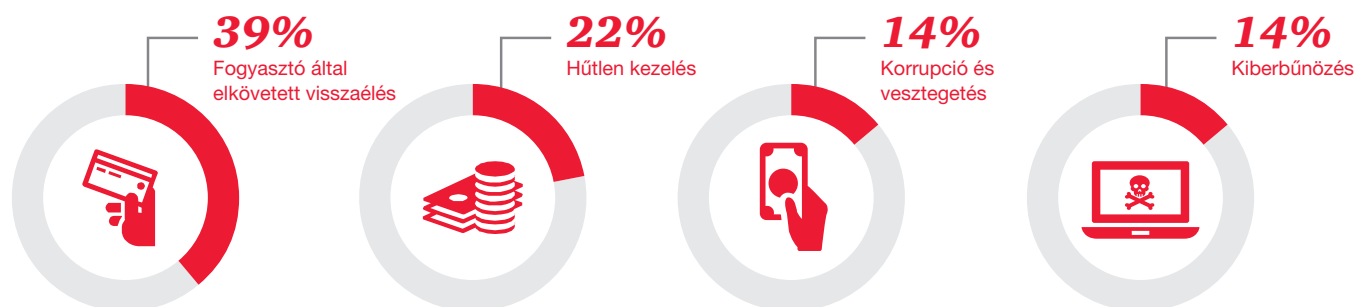
2. ábra

Kérdés: Milyen típusú visszaélés és/vagy gazdasági bűncselekmény történt az Ön vállalatánál az elmúlt 24 hónapban? (%)



3. ábra

Kérdés: Az elmúlt 24 hónapban az Ön vállalata által Magyarországon elszennvedett csalások és/vagy gazdasági bűncselekmények közül melyik érintette (pénzügyileg vagy egyéb módon) az Ön vállalatát a LEGINKÁBB érzékenyen/komolyan?

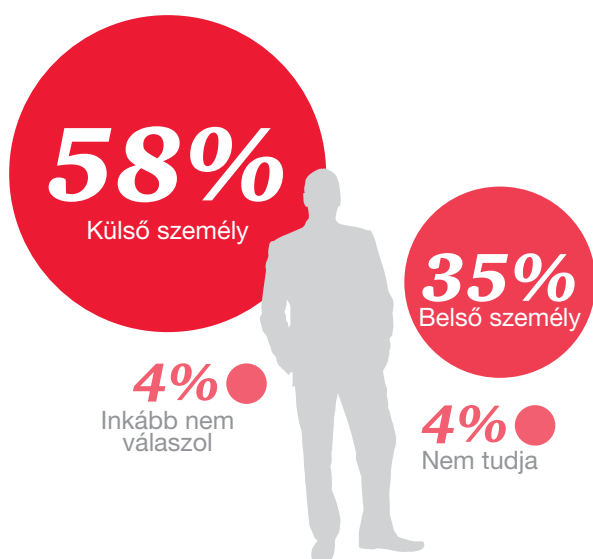


Válogassa meg üzletfeleit!

Az egyik legnagyobb „vakfoltot” – és az egyik legnagyobb kockázati tényezőt – az üzletfelek jelentik. A felmérés alapján a vállalatokat legérzékenyebben érintő visszaéléseket és/vagy gazdasági bűncselekményeket Magyarországon nagyobb valószínűséggel követték el külső felek (58%), ami a 2016-os felmérésünk eredményéhez képest (33%) szembetűnő különbség. Azokban az esetekben, amelyekben a visszaélést külső fél követte el, a külső felek csoportjának jelentős hányadát valójában „hamis barátok” („frenemies”), vagyis harmadik felek – megbízottak, szállítók – és ügyfelek alkotják. Más szóval azok a személyek és gazdálkodók, amelyekről kölcsönös bizalom lenne elvárható, de akik valójában meglopják a társaságot.

4. ábra

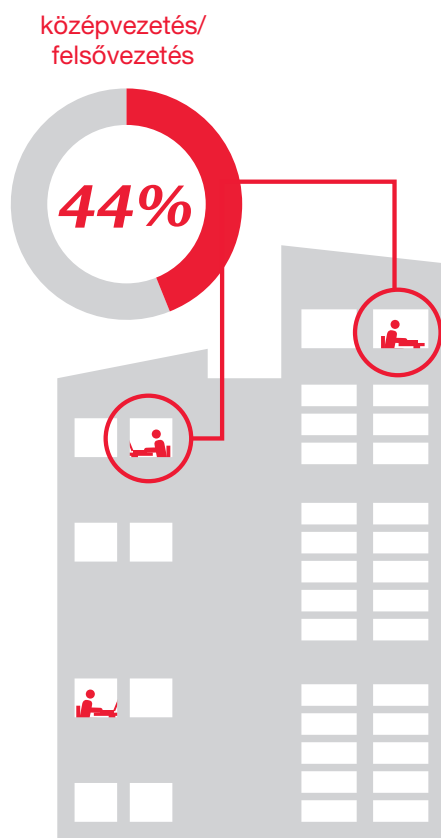
Kérdés: Az Ön vállalatánál az elmúlt 24 hónapban előfordult (pénzügyi veszteségek szempontjából) legsúlyosabb gazdasági bűncselekménynek ki volt a fő elkövetője? (%)



Az elkövetőket bemutató statisztikát közelebbről megvizsgálva az is kiderül, hogy az elkövetők jellemzően az üzemeltetési és gyártási területeken dolgoznak, de a szervezet bármelyik szintjéről kikerülhetnek. A magyar minta alapján az esetek 44%-ában az elkövető a közép-/felső vezetéshez tartozott.

5. ábra

Kérdés: A vállalaton belül milyen szinthez tartozott a belső visszaélés FŐ elkövetője? (%)



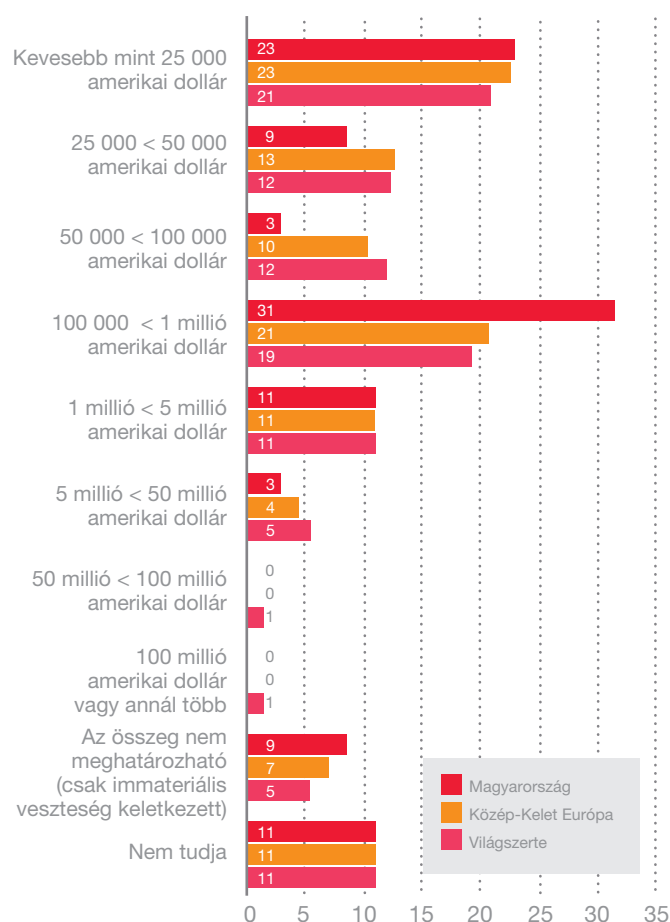
A visszaélések továbbra is jelentős költségeket okoznak

A vállalatok arra a kérdésre adott válaszából, hogy az elmúlt két évben a vállalatot legérzékenyebben érintő bűncselekmény mekkora közvetlen pénzügyi veszteséget okozott, az derült ki, hogy a gazdasági bűncselekményeket elszenvedő vállalatok 45%-a 100 000 amerikai dollárnál többet veszített Magyarországon. Globális szinten a válaszadók 64%-a nyilatkozott úgy, hogy a veszteség 1 millió dollárt is elérhetett; 16% esetében a veszteség 1–50 millió dollár között mozgott. Az egyedüli szembetűnő különbség az, hogy egyetlen magyarországi válaszadó sem számolt be 50 millió dollár feletti veszteségről.

A járulékos költségek, például a vizsgálatok és beavatkozások költségei azonban lényegesen megnövelhetik az összköltséget. Magyarországon minden második vállalat legalább ugyanannyit költött vizsgálatokra vagy egyéb beavatkozásokra, mint amennyibe maga a visszaélés került. Ez jól mutatja, hogy a korrekciós intézkedések (mint például a vizsgálatok, peres ügyek) költsége könnyen meghaladhatja egy visszaélés kivédését szolgáló erős rendszer kialakításának költségét.

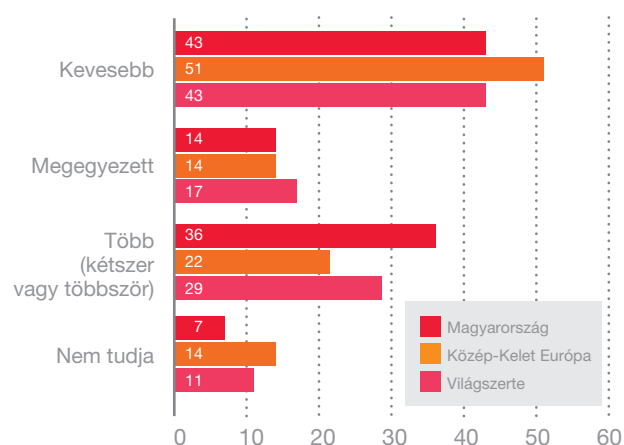
6. ábra

Kérdés: Véleménye szerint vállalatának az elmúlt 24 hónapban hozzávetőlegesen mekkora közvetlen pénzügyi vesztesége keletkezhetett az Ön vállalatát legsúlyosabban érintő visszaélés miatt? (%)



7. ábra

Kérdés: Az elmúlt 24 hónapban az Ön vállalatát legsúlyosabban érintő visszaélés következményeként az Ön szervezete által a vizsgálatokra és/vagy egyéb beavatkozásokra fordított összeg magasabb vagy alacsonyabb volt-e az elszenvedett veszteség összegénél, vagy megegyezett azzal? (%)



A költségeken túl: akár jogosan, akár nem, a vezérigazgató és az igazgatóság felelőssége megkerülhetetlen

Amikor a visszaélésből származó költség az eredményre is kihat, természetes, hogy azt az igazgatóság és a tulajdonosok a felső vezetésen kéri számon. Manapság a felelősség nem ér itt véget: valójában itt kezdődik.

„A vezérigazgatókra egyre inkább a vállalatok megtestesítőiként tekintenek, akiktől azt várják el, hogy állandóan figyelemmel kísérik a vállalati kultúra és működés minden vonatkozását. Etikai vagy megfelelési gondok esetén pedig – a közvélemény és egyre inkább a hatóságok is – az üzleti vezetőket tartják személyesen felelősnek.”

Polacsek Csaba
Cégtárs, Üzleti tanácsadás
PwC Magyarország

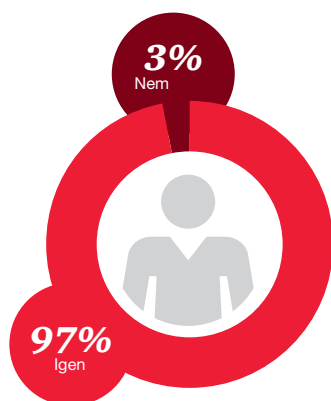


Bárhogyan értékeljük is ezt az agresszív választ, a felső vezetők aligha hozhatják fel mentségül a tudatlanságukat. Felmérésünkéből kiderül, hogy Magyarországon a felső vezetők a legsúlyosabb visszaélésekről szinte minden esetben (97%) értesülnek.

Továbbá a magyarországi válaszadók 81%-a jelezte, hogy vállalata rendelkezik hivatalos üzleti etikai és megfelelési programmal, ezen belül 17% nyilatkozta, hogy a program első számú felelőse a cég vezetője.

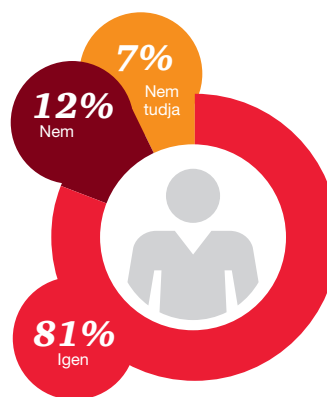
8. ábra

Kérdés: Az elmúlt 24 hónapban történt legsúlyosabb visszaélés eskalálásra került-e az igazgatóság szintjére?



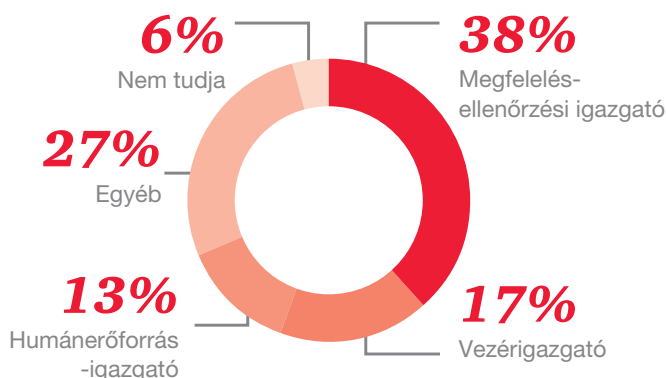
9. ábra

Kérdés: Rendelkezik az Ön vállalata formális etikai és megfelelési programmal?



10. ábra

Kérdés: Etika szabályzat elsődleges felelőse



Ez ráirányítja a figyelmet arra, hogy az ügyfelekkel közvetlenül érintkező (front office) területek hogyan kezelik a válságot – továbbá arra, hogy a kockázati profiljukat átalakítják-e, és ha igen, milyen mértékben. A 2018. évi 21. Vezérigazgató Felmérésünk is ezt támasztja alá: a cégvezetők a növekedést leginkább veszélyeztető tényezőként a bizalom és az elszámoltathatóság kérdését jelölték meg.

Megfelelés ellentétés elvárásoknak

A vállalatoknak sokszor ellentétes elvárásoknak kell megfelelniük: egyrészt a piac elvárja tőlük az innovációt, másrészt a részvényesek a minél magasabb eredmény elérésében érdekeltek, harmadrészt pedig a társadalom etikai elvárásokat támaszt. Amikor egy vállalat pénzügyileg jól teljesít, a piac hajlamos időnként szemet hunyni bizonyos visszásságok felett. A felső vezetők azonban ezt nem tehetik meg. A vállalatok könnyen ringatják magukat hamis biztonságérzetbe, amikor minden rózsásnak tűnik, és amikor a felső vezetés a megfelelő szölamokat hangoztatja.

A piac kedveli ugyan az újítókat és a kiemelkedően teljesítőket, azonban a nem megfelelő magatartást nem tolerálja. Nem érdekes, mennyire számít egy vállalat a tőzsde kedvencének – ha a magatartási kockázatokat nem kezeli kellő óvatossággal és megfontoltsággal, a vállalat és annak vezetői egyaránt nagyon könnyen elveszthetik a piac bizalmát.

A start-up generáció ugyanakkor sok ígéretet rejt. Ezeket a gyorsan növekvő cégeket gyakran fiatalabb vállalkozók irányítják, döntő többségüknek természetes az etikus szemlélet. Mivel nem kell elavult folyamatokkal és gyengén integrált rendszerekkel küzdeniük, kezdettől ideális helyzetben vannak a visszaélések felderítésére szolgáló korszerű adatelemzési módszerek alkalmazásához – ami óriási versenyelőnyt biztosít számukra a visszaélésektől egyre fertőzöttebb környezetben. E frissen létrejött cégek segítségével beköszönhet egy olyan új korszak, amelyben az átláthatóság és nyereségesség nem zárják ki egymást.

2. Visszaélések napjainkban

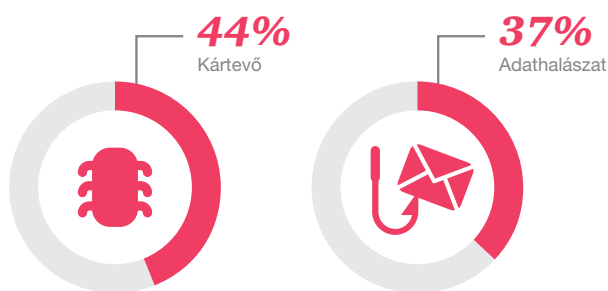


2.1 Kiberbűnözés: a célok és eszközök nincsenek összhangban egymással

A kiberbűnözés felnőttkorba lépett. A mai kiberbűnözők éppen olyan hozzáértők és professzionálisak, mint az általuk megtámadott vállalatok. Új szemléletmódra van tehát szükség arra nézve, hogy ez az új érettség milyen módon vezethet veszélyes visszaélésekhez.

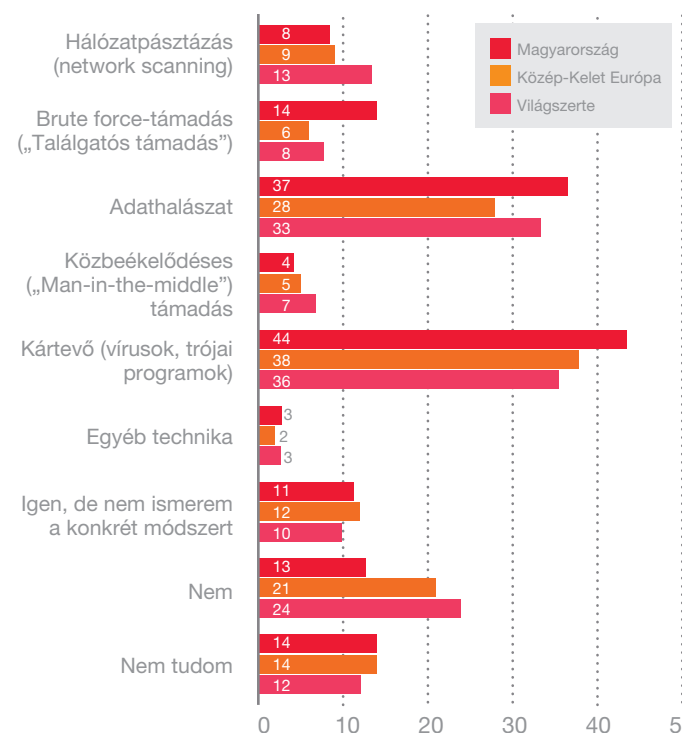
A fenti állítás Magyarországra is érvényes, mivel a kiberbűnözés a 2016-ban készült legutóbbi felmérésünk óta jelentősen növekedett. A válaszadók 31%-a tapasztalt valamilyen számítógépes bűnözéssel kapcsolatos visszaélést, e tekintetben Magyarország pontosan elérte a globális szintet. A gazdasági bűncselekmények közül ebben a kategóriában itt volt eddig a legnagyobb mértékű növekedés. A kiberbűnözés magyarországi növekedéséhez hozzájárult a zsarolóprogramok globális megjelenése is (például Petya és WannaCry), amelyek az elmúlt 24 hónapban számos helyi vállalatot érintettek.

Nem meglepő módon a kiberbűnözés számos fajtája létezik, ezek közül sok Magyarországon is előfordul, a leggyakrabban kártevő szoftverek (44%) és adathalászat (37%) formájában.



11. ábra

Kérdés: Az elmúlt 24 hónapban érte-e az Ön vállalatát az alábbi módszerek valamelyikét alkalmazó kibertámadás? (%)



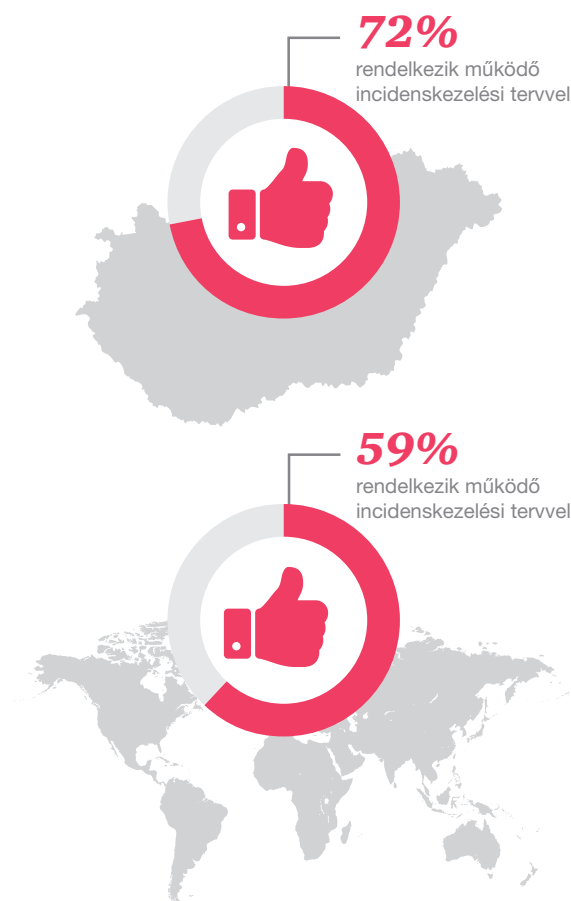
Meg kell említeni továbbá, hogy a magyar vállalkozások egyre inkább tisztában vannak ezzel a fenyegetéssel, amit az is mutat, hogy egyre többen készítenek a kibertámadásokra vonatkozó incidenskezelési tervet. A megkérdezettek 72%-a nyilatkozta, hogy saját cége rendelkezik működő incidenskezelési tervvel a kibertámadások elhárítására, ami a 2016-os felmérésben mért 42%-hoz képest jelentős növekedés, sőt a globális átlagot (59%) is meghaladja.

Ugyanakkor azok a cégek, amelyek nem rendelkeznek ilyen tervvel, és hasonló készítését még csak nem is fontolgatják (a magyarországi válaszadók 10%-a) súlyos kockázatnak teszik ki magukat.

Egy vállalatnál az első jele annak, hogy valami rendszerszinten nincs rendben, gyakran valamilyen kibertámadáson keresztül mutatkozik meg. E támadások növekvő gyakorisága, kifinomultsága és veszélyessége arra készíti a cégeket, hogy belső működésüket felülvizsgálva módot találjanak a támadások megelőzésére. Ez azzal az előnnyel jár, hogy több figyelmet fordítanak a visszaélések megelőzésére. Itt ismét egy potenciális „vakfolttal” találkozunk, ami a megelőzésen túl a szemléletmód hiányosságairól árulkodik. Míg korábban minden fajta kibertámadást egy kalap alá vettek, a visszaélések szempontjából fontos különbséget tenni a biztonsági incidens (az ártó szándékú felhasználók általi betörés, illetve behatolás) és annak vállalatra gyakorolt hatása között. Manapság már nem a betört ajtó az érdekes, hanem az, hogy mi történt azután, hogy az elkövető bejutott – és hogyan akadályozhatjuk ezt meg a jövőben.

12. ábra

Kérdés: Rendelkezik-e az Ön vállalata a kibertámadások kezelésére szolgáló (megelőző/felderítő célú) kiberbiztonsági programmal? (%)





2.2 Üzleti szabályszegés és a mögöttes üzletviteli kockázat

„Az üzletviteli kockázat viszonylag új jelenség, amelyre a szabályozó hatóságok az utóbbi években, néhány nagy horderejű botrányt követően – például pénzügyi referenciaértékek manipulálása, termékek hibás értékesítése – kezdtek nagyobb figyelmet fordítani, de ennek jelentősége nem korlátozódik a pénzügyi szolgáltatási ágazatra.”

Polacsek Csaba

A visszaéléseket könnyen a szőnyeg alá söprik, vagy a „nem az én dolgom” kategóriájába sorolják. Azt tapasztaltuk, hogy a megfelelés, az etika és a vállalati kockázatkezelés a legtöbb cégnél nem csak külön funkciók, de gyakran mintha külön univerzumban léteznének. A „siló” mentalitás miatt a legritkább esetben alkotnak stratégiai egészet.

E különálló területek megközelítésének a legjobb módja, ha egy nagyobb, átfogó rendszer összetevőiként tekintünk rájuk. Ez az üzletviteli kockázat, vagyis annak kockázata, hogy a munkavállalók cselekedetei ellentétesek azokkal a viselkedésmintákkal, amelyeket képzésük során megtanultak. Innentől

kezdve ezek a területek horizontálisan mérhetők és kezelhetők, és integrálhatók a vállalatok szélesebb stratégiai döntéshozatali folyamataiba. A működési zavarokkal vagy a külső fenyegetésekkel ellentétben, amelyeket a belső kontrollokkal és folyamatokkal gyakran féken lehet tartani, az üzletviteli kockázat holisztikusabb megközelítést igényel – és szemléletváltást. Amikor a problémákat magatartási kockázatnak tekintjük, elfogulatlanul tudjuk őket kezelni, vagyis a mindennapok olyan velejárójaként, amellyel kivétel nélkül minden vállalatnak szembe kell néznie.

Amennyiben az üzletviteli kockázatot sikerül rendszerszintű (és realisztikus) módon szemlélni, nem csak költséghatékonyságot érhetünk el az etikai, visszaélés- és korrupcióellenes megfelelési programok között, hanem azokat az érzelmeket is lecsillapíthatjuk, amelyek az etikai szabályok megsértését gyakorta kísérik. De a legfontosabb, hogy a visszaélés-ellenes funkciókat ne elkülönülten kezeljük, máskülönben nem leplezhetők le a visszaélések.

Magyarországon a nem szabálykövető viselkedés másik oka a megfelelő tréning és kultúra hiánya, a felsővezetés megfelelő felügyeletének hiánya. A kis- és középvállalkozások és a kezdő vállalkozások hajlamosak a gyors növekedésre, anélkül, hogy megfelelő hangsúlyt fektetnének a megfelelésre és a védelmi vonalak kialakítására, márpedig ennek elmulasztása a visszaélések melegágya.





2.3 Vesztegetés és korrupció – egy valószínű „vakfolt”?

Meglepő módon a vesztegetés és korrupció 2007 óta először nem került a három leggyakoribb magyarországi gazdasági bűncselekmény közé; ehelyett csak az ötödik helyet foglalja el, köszönhetően annak, hogy a válaszadók mindössze 19%-a találkozott korrupcióval a saját cégénél az elmúlt 24 hónapban – a kissé emelkedő kelet-európai és globális trendek ellenére.

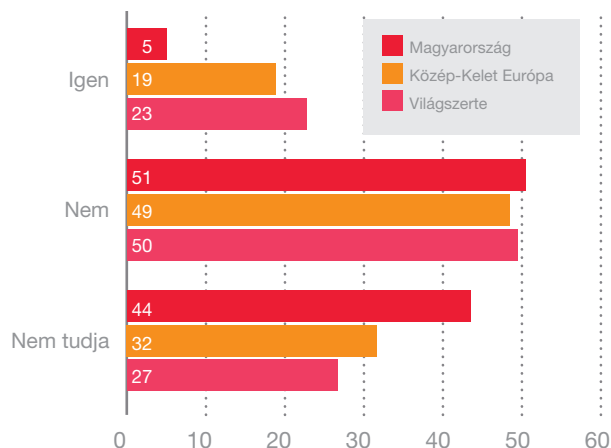
Emellett, a fokozódó bűnüldözési tevékenység (a nemzetközi akciókat is ideértve), a korszerűsített OECD keretrendszer, és az újonnan elfogadott nemzeti korrupcióellenes jogszabályok (például az új francia korrupcióellenes törvény) az elkövetkező hónapokban sok munkát adnak majd a vesztegetés- és korrupcióellenes intézkedésekkel foglalkozó compliance osztályoknak.

„Jelentős ugyanakkor azon magyarországi válaszadók aránya, akik nem biztosak benne, hogy az elmúlt 24 hónap során kértek-e vállalatuktól kenőpénzt (44%), illetve a szervezet került-e hátrányba kenőpénzt fizető versenytárral szemben (59%), ami komoly aggodalomra, illetve gyanúra ad okot. A fentiek jól illusztrálják a korrupció rejtett jellegét – ezért tekintjük a korrupciót egy valódi vakfoltnak Magyarországon.”

Polacsek Csaba

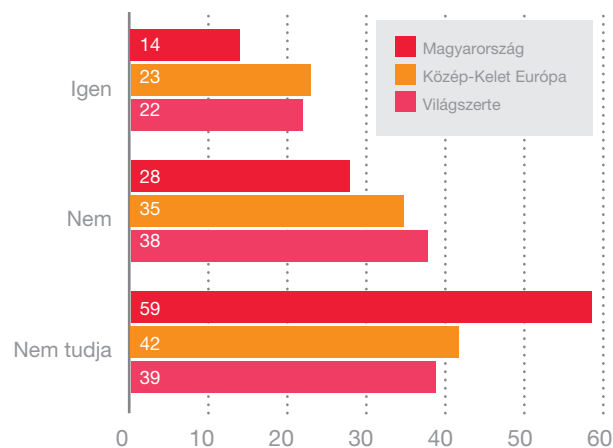
13. ábra

Kérdés: Kértek-e az Ön vállalatától kenőpénzt az elmúlt 24 hónapban? (%)



14. ábra

Kérdés: Került-e az Ön vállalata hátrányba kenőpénzt fizető versenytárral szemben az elmúlt 24 hónap során? (%)





2.4 Pénzmosás – a jogszabályi változások hatására gyakoribbak a pénzmosás megakadályozásával kapcsolatos kockázatértékelések

Legutóbbi felmérésünk óta az Európai Parlament elfogadta a negyedik pénzmosás elleni irányelvet. Az uniós tagállamoknak, így Magyarországnak is, 2017. június 26-ig kellett ezt az irányelvet átültetniük nemzeti jogrendjükbe. Úgy véljük, hogy főként ennek a jogszabályi változásnak köszönhető az AML/CFT (a pénzmosás és a terrorizmus finanszírozása megakadályozásával kapcsolatos) kockázatértékelések gyakoribbá válása: a magyarországi válaszadók 48%-a jelezte, hogy cége az elmúlt 24 hónapban végzett a vállalkozás teljes üzleti és földrajzi struktúrájára kiterjedő ilyen értékelést. Ez az arány kissé elmarad a kelet-európai (51%), illetve a globális (62%) átlagtól. Nehéz ezeket az eredményeket a válaszadók háttérének beható ismerete nélkül értékelni, mindazonáltal a közelmúltbeli pénzmosási botrányok egyik fő üzenete az volt, hogy számos nem pénzügyi szolgáltató társaság – kereskedelmi és gyártó vállalat – ki volt téve a pénzmosás veszélyének, és néhány közvetlenül is érintve volt a tevékenységben. A nem pénzügyi társaságok továbbá általában a hagyományos pénzügyi intézményeknél kevésbé óvatosan kezelik a pénzmosás és a terrorizmus finanszírozása megakadályozására vonatkozó előírásoknak való megfelelést, miközben a kereskedelmi alapú pénzmosásra (trade based money laundering) figyelmeztető jelek észlelése az egyik legnehezebb feladat.

Érdekes módon a magyarországi válaszadók mindössze 5%-a nyilatkozott úgy, hogy az elmúlt 24 hónapban szabályozói végrehajtási korrekciós programban vett/vesz részt, illetve vállalatánál szabályozói vizsgálat folyt, mely jelentős megállapításokat tett. Ezzel szemben ez az arány a kelet-európai válaszadók között 23%, világszerte pedig 32% volt. Nyugat-Európával és az Egyesült Államokkal ellentétben Magyarországon néhány kivételtől eltekintve nem szabtak ki a pénzmosás megakadályozásával kapcsolatos hiányosságok miatt súlyos bírságokat és büntetéseket. Ez azonban a jövőben változhat.

15. ábra

Kérdés: Azon vállalkozások aránya, amelyeknél az elmúlt 24 hónapban végeztek a vállalkozás teljes üzleti és földrajzi struktúrájára kiterjedően a pénzmosás és a terrorizmus-finanszírozás megelőzésével kapcsolatos kockázatértékelést (%)



3. Felkészültségből jeles?

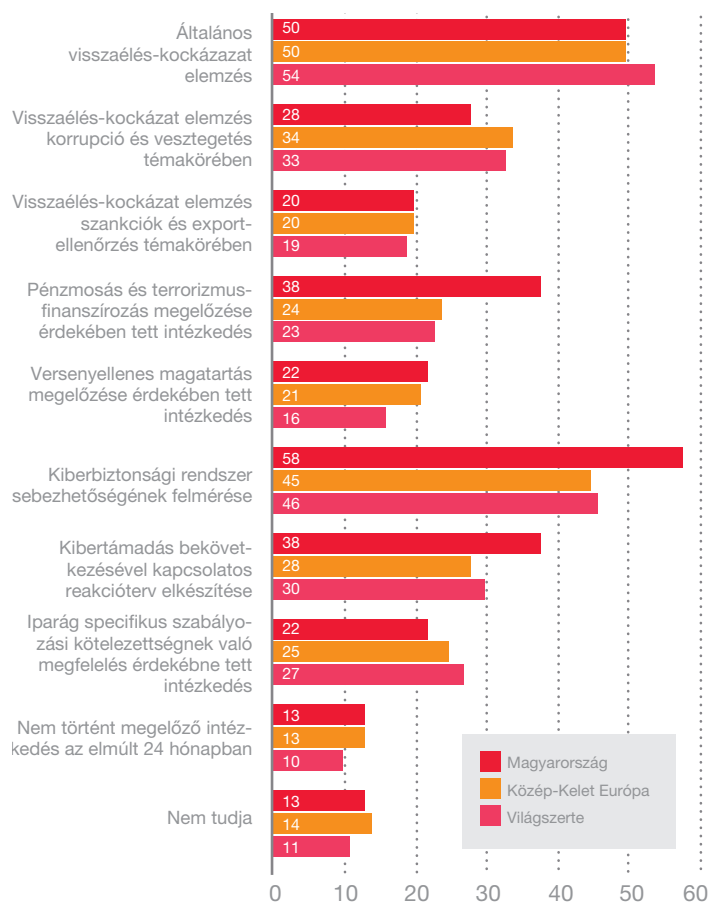
3.1 A visszaélés kockázata még mindig nagyobb, mint a felderített esetek száma

Legutóbbi felmérésünk óta azt tapasztaltuk, hogy a válaszadó cégek valamennyivel többet tesznek a visszaélések felderítéséért. Ez pozitív fejlemény, mert azon kívül, hogy a visszaélés kockázatának értékelése segít meghatározni azokat az egyedülálló és specifikus kockázatokat, amelyeket a cégeknek figyelemmel kell kísérniük, az ilyen jellegű értékeléseket a szabályozószervek is egyre inkább előnyben részesítik a bűnözés elleni fellépés során. Felmérésünk ennek ellenére azt mutatja, hogy bőven van még min javítani. A magyar vállalatok csupán 50%-a nyilatkozott úgy, hogy végzett visszaélések kockázatát felmérő általános értékelést (csodálkozunk-e azon, hogy a vállalatok hasonló hányada, vagyis 49%-a véli úgy, hogy őket nem érintette visszaélés?).



16. ábra

Kérdés: Az elmúlt 24 hónapban történtek-e intézkedések a visszaélések megelőzésének érdekében az alábbiak közül? (%)



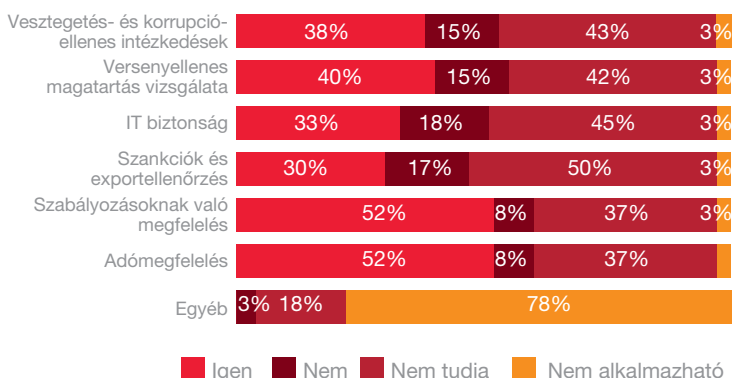
„Akvízió és egyéb ügyletek esetén – ahol felmerül annak kockázata, hogy a jogutód kötelezettségeket és nem megfelelő kontrollokat »vásárol« – még nagyobb fontossággal bír, hogy az ügyletkötést megelőző átvilágítás részeként értékeljük a visszaélések kockázatát.”

Polacsek Csaba

Az ilyen, a pénzügyi átvilágításnál tágabb hatályú átvilágítások pedig a magántőke-társaságok számára is relevánsak lehetnek, mely társaságoknak hasznos a „jó bizonyítvány” befektetés mellett exit esetén is. A visszaélések, a kibebűnözés és a korrupció megelőzését célzó átvilágítás lehetővé teszi a felvásárlók számára a kockázatok megismerését, és megmutatja, hogyan lehet ezeket a kockázatokat kezelni az ügylet keretében, illetve az ügyletkötést követően megszüntetni. Ráadásul mindkét lehetőség az eladói oldalon is jelentősen növelheti a megtérülést. Mindezen előnyök ellenére a magyarországi válaszadók kevesebb mint fele számolt be arról, hogy vállalata az akvizíciós folyamat részeként az alábbiakra irányuló kiegészítő átvilágításokat is elvégzi: vesztegetés- és korrupcióellenes intézkedések 38%, versenyellenes magatartás vizsgálata 40%, IT biztonság 33%.

17. ábra

Kérdés: Elvégzi-e az Ön vállalata a következő további átvilágítások bármelyikét az akvizíciós folyamat részeként? (%)



A visszaélések felderítése az első védelmi vonalba kerül

„Míg a visszaélések megelőzése és felderítése hagyományosan a vállalatok második védelmi vonalába – a kockázatkezelés, jog, megfelelés területéhez – tartozott, a visszaélések megelőzését célzó, újonnan megerősített intézkedések egyre inkább az első védelmi vonalba ágyazódnak.”

Polacsek Csaba

Felmérésünk eredményei is ezt támasztják alá: a válaszadók 17%-a szerint elsődlegesen a vezérigazgatók (mint az első védelmi vonal részei) felelősek a vállalat üzleti etikai és megfelelési programjáért, ezért fontosabb szerepet játszanak a visszaélések felderítésében és az arra adott válaszban.

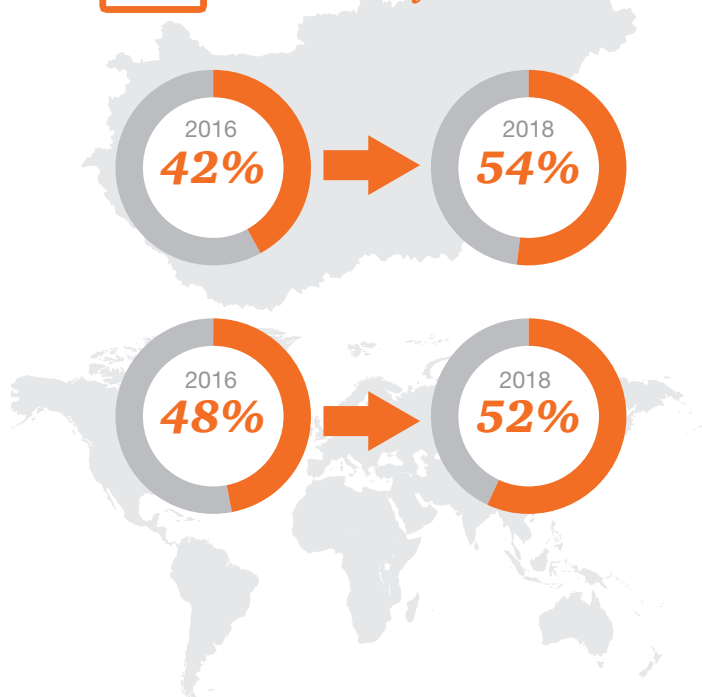
Ez valószínűleg csak a kezdete egy olyan jelentős elmozdulásnak, amelyben tovább érnek és erősödnek a visszaélések első védvonalbeli megelőzésének és felderítésének lehetőségei. Mindez lehetővé teszi, hogy a második védelmi vonal egy második vonalra jellemző hagyományosabb szemlélet – az irányítás és felügyelet, a kockázati tolerancia, keretrendszerek és politikák meghatározása – irányába mozduljon.

3.2 A rendszerszintű mechanizmusok fontos szerepet játszanak a visszaélések felderítésében

Az értékelésektől a kontrollok felé irányítva a figyelmet azt látjuk, hogy a vállalatok egyre több visszaélést derítenek fel rendszerszintű mechanizmusokon keresztül. Magyarországon 42%-ról 54%-ra emelkedett azoknak a vállalatoknak az aránya, amelyek a vállalati kontrollokra támaszkodnak a visszaélések felderítésében (ez az arány globálisan 48%-ról 52%-ra nőtt). Szembetűnő különbség érzékelhető azonban a vállalati kultúra szerepében, mivel az Magyarországon (15%) kisebb a jelentősége a visszaélések felderítésében, mint globális szinten (27%). Ezért annak az esélye, hogy a visszaélések a vezetés hatáskörén belül kerülnek felderítésre, jóval alacsonyabb, és Magyarországon a visszaélések 21%-ára még mindig olyan módon derült fény, amelyre a vállalat vezetésének nem volt befolyása.

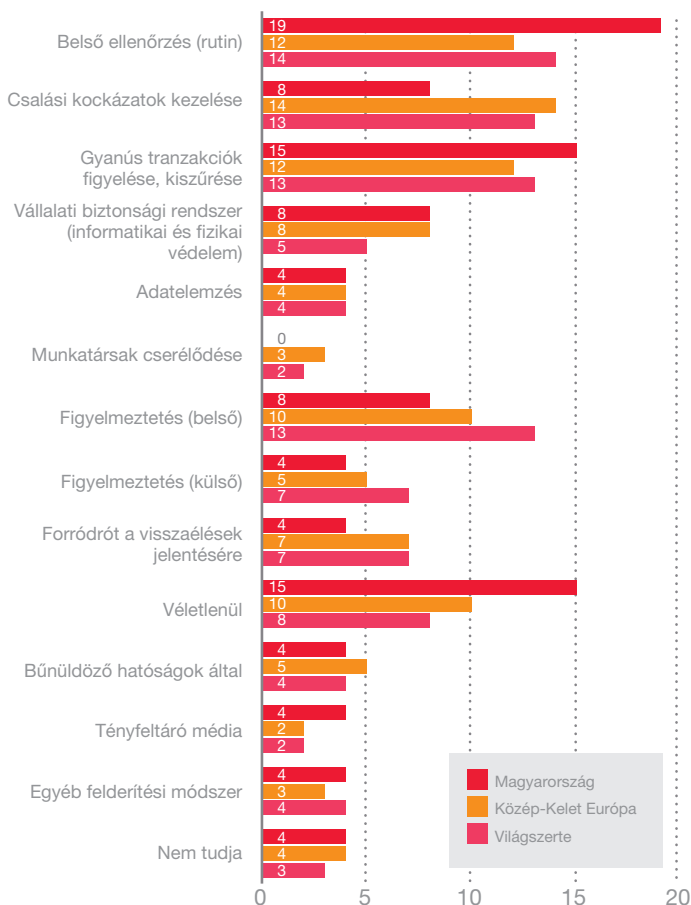


Vállalatok aránya, akik vállalati kontrollokra támaszkodnak a visszaélések felderítésében



18. ábra

Kérdés: Az Ön vállalatánál az elmúlt 24 hónapban előfordult legsúlyosabb gazdasági bűncselekményre eredetileg hogyan derült fény? (%)



3.3 Megfelelési programok, a visszaélések elleni küzdelemre fordított összegek

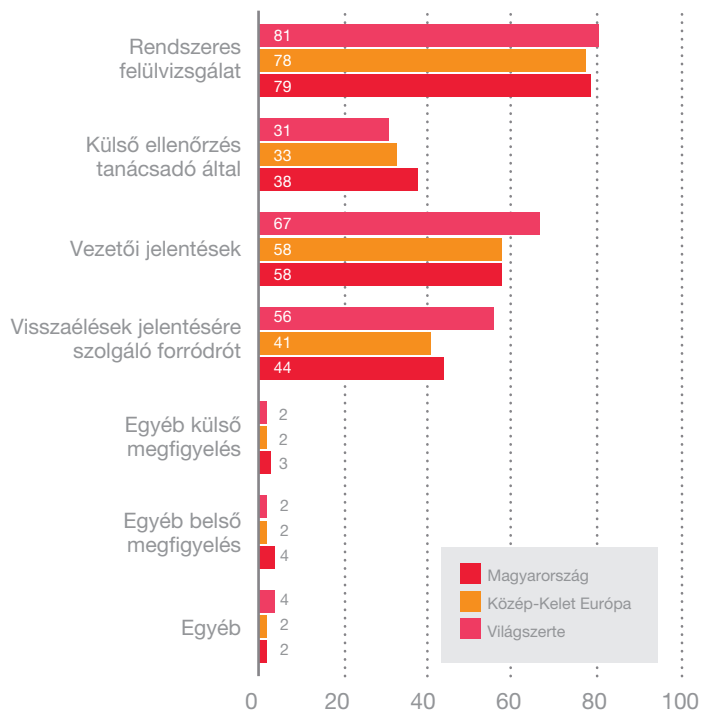
Felmérésünk szerint Magyarországon a válaszadók közel egynyolcada (12%) nem tudott arról, hogy vállalatánál létezne bármilyen formális etikai és megfelelési program – ebben kismértékű csökkenés mutatkozik a 2016. évi felmérés 19%-os eredményéhez képest. A vállalati megfelelési és üzleti etikai program hatékonyságának biztosítására a vállalatok 81%-a belső ellenőrzéseket, 67%-a vezetői jelentéseket, 31%-a pedig külső ellenőrzéseket alkalmaz.

Ezen kívül a magyar felmérés válaszadóinak 56%-a nyilatkozott úgy, hogy vállalata bejelentő forrádróttal biztosítja a megfelelési rendszer hatékony működését, ami 12%-os növekedést jelent a 2016. évi felmérés 44%-os eredményéhez képest. Bár a belső ellenőrzés fontos eszköz a megfelelési programok hatékonyságának mérésére, önmagában nem elegendő a megfelelés biztosítására, mivel tevékenysége alapvetően időszakos jellegű és a múltbeli eseményekre irányul. Emellett a visszaélési kockázatok profilja megváltozott (így például növekszik az új típusú visszaélések és a kiberbűnözés aránya), továbbá bizonyos típusú vállalatoknál egyes visszaélési típusok gyakorisága növekszik vagy állandó.

Érdekes módon a magyarországi válaszadók csupán 38%-a jelezte, hogy vállalata magasabb összeget fordít a visszaélések elleni küzdelemre, míg 62% arról számolt be, hogy az erre a célra fordított összeg nagysága nem változott (vagy éppen csökkent), miközben jelentősen emelkedett a gazdasági bűncselekmények előfordulásának gyakorisága.

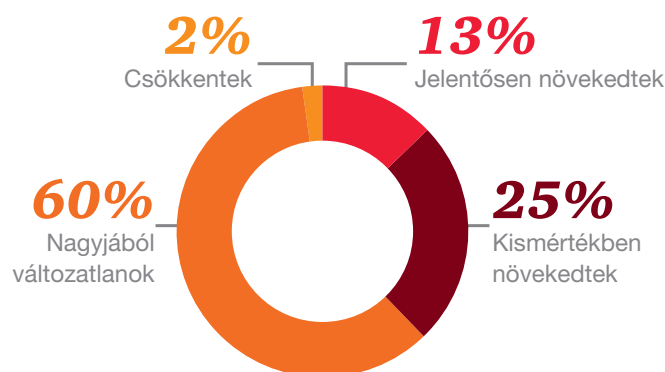
19. ábra

Kérdés: Az Ön vállalata hogyan biztosítja megfelelési és üzleti etikai programjának hatékonyságát? (%)



20. ábra

Kérdés: Hogyan alakultak az Ön vállalatánál a visszaélések elleni küzdelemre fordított összegek az elmúlt 24 hónapban? (%)



4. Állítsuk a technológiát a visszaélések elleni küzdelem szolgálatába!

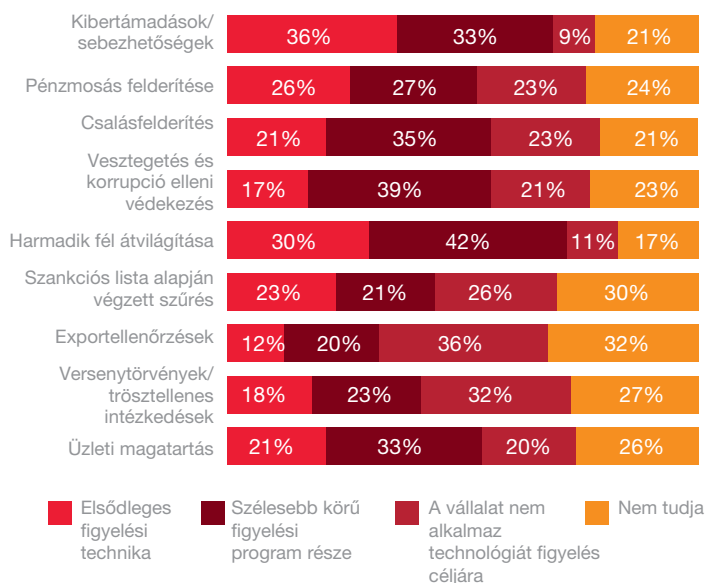
A visszaélések kapcsán gyakran felmerül, hogy a technológia kétélű fegyver: egyszerre jelent fenyegetést és védelmet a vállalkozásoknak. A technológia hagyományosan a vállalkozások működési szintjéhez tartozik – a második védelmi vonalat képviseli. Ugyanakkor olyan mértékben jelen van minden üzleti folyamatban, beleértve az ügyféloldali területeket is, hogy a visszaélések elleni küzdelemben történő felhasználása – hogyan alakítunk ki egyensúlyt a biztonság és a túlzott óvatosság között – immár központi kérdés az ügyfélelégedettség szempontjából. Ezért ez a felső vezetés számára is alapvető fontosságú kérdés. A cégek alapján véve felismerik, hogy a visszaélés annak bármely formájában elsődlegesen üzleti probléma, amely komolyan hátráltathatja a cég növekedését. Erre válaszul számos vállalkozás stratégiai váltást hajtott végre a külső visszaélésekkel kapcsolatos szemléletmódjában, és új beruházásokat tervez a visszaélések felderítése, azonosítása és az ügyfelekkel való konfliktusok mérséklése érdekében.

A visszaélésekkel szembeni védekezésben innovatív és fejlett technológiák gazdag tárháza áll a cégek rendelkezésére, amelyek lehetővé teszik az emberi viselkedés felügyeletét, elemzését, az abból való tanulást, valamint annak előrejelzését. Az adatok azt mutatják, hogy ezeket a technológiákat a vállalatok használják is, az adott szektortól függően különböző mértékben. E technológiák beszerzése és alkalmazása egy nagyobb vállalatnál meglehetősen költséges – egyes cégek nem is engedhetik meg maguknak. Ráadásul nagyfokú körültekintést igényel, hogy mit és mikor érdemes beszerezni. Egyes vállalatok olyan kialakulóban lévő vagy diszruptív technológiákba fektetnek, amelyeket aztán nem alkalmaznak optimálisan. Más vállalatok túl későn fognak hozzá, ezért alulmaradnak a visszaélések felderítésében, illetve a lehetséges gócpontok megtalálásában. A magyarországi felmérésre adott válaszok is hasonló

tapasztalatokat támasztanak alá. Míg a vállalatok felkarolják a technológiát a visszaélések és/vagy a gazdasági bűncselekmények elleni küzdelemben, és pozitívan ítélik meg az így elérhető képességeket, a megkérdezett cégek közel egyötöde (19%) „egyetért” vagy „teljes mértékben egyetért” azzal az állítással, hogy a náluk alkalmazott technológiai megoldások túl sok riasztást vagy vakriasztást eredményeznek. E cégek számára jó hírrel szolgálhatunk: valószínűleg nincs szükség újabb költséges technológiai befektetésekre, csak a meglévő rendszereiket kell megfelelően kalibrálniuk, finomhangolniuk.

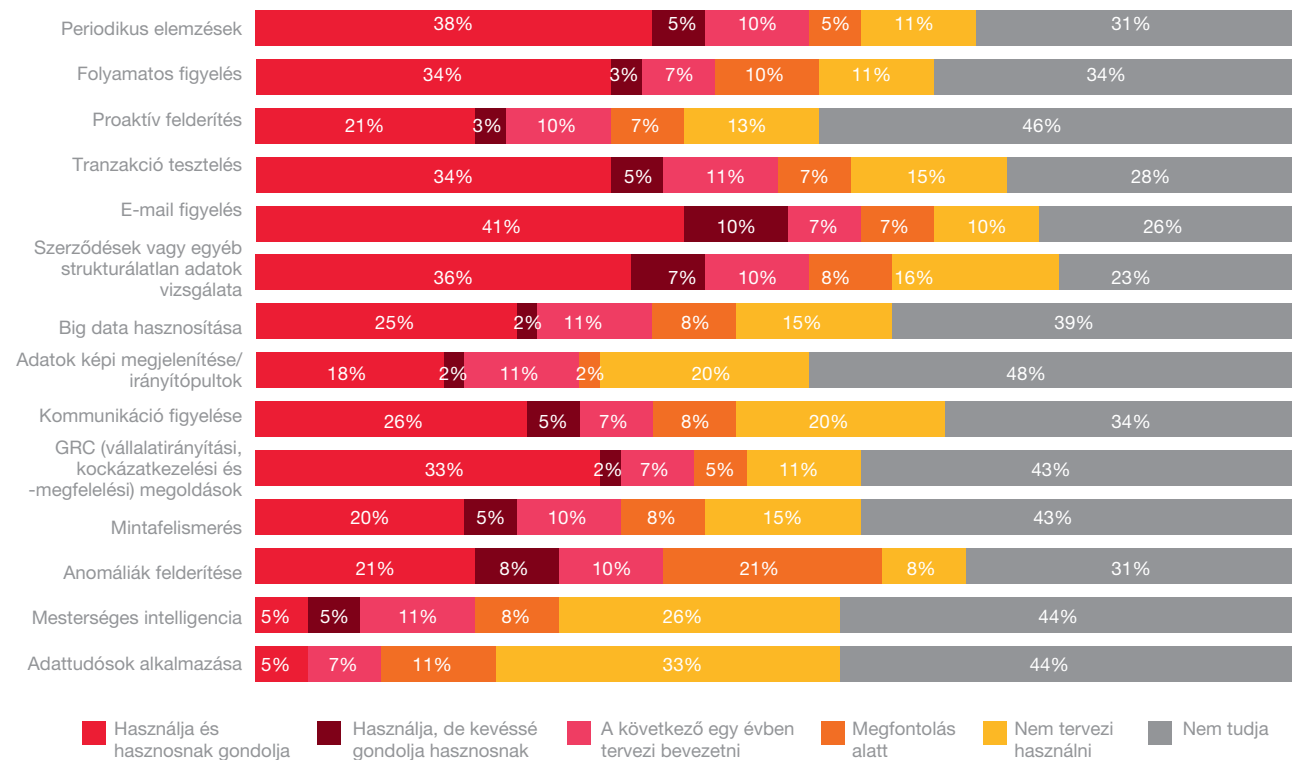
21. ábra

Kérdés: Mire használja a technológiát a visszaélések elleni küzdelemben? (%)



21. ábra

Kérdés: Az Ön vállalata milyen mértékben alkalmazza ellenőrzési mechanizmusai között az alábbi alternatív/diszruptív technológiákat és módszereket a visszaélések elleni küzdelem érdekében, illetve tervezi-e ezek alkalmazását? (%)



Technológia-adaptációs trendek: az arany középut megtalálása

Felmérésünk meglepő módon azt mutatja, hogy a feltörekvő piacokon működő vállalatok a fejlett országokhoz képest gyorsabb ütemben fektetnek be fejlett technológiákba, így például a mesterséges intelligenciába – ennek oka valószínűleg az, hogy így kívánnak felzárkózni olyan területeken, ahol más országok már jelentős összegeket investáltak az infrastruktúrába. A magyarországi válaszok is ezt a vélekedést támasztják alá: a fejlett technológiák számos típusát használják különböző célokra.

Mindenesetre világos, hogy az innovatív technológiák visszaélések elleni használata ma már világméretű jelenség. A technológia elterjedtsége és a visszaélések lopakodó növekedése kettős kihívást jelent a vállalkozások számára: meg kell találniuk az arany középutat a hatékonyság és a költségek között, ugyanakkor nem hagyhatják, hogy a technikai eszközökben és felkészültségben egyaránt élen járó családok felülkerekedjenek.

Az ügyfelek nem csak egy tényezőt jelentenek a sok közül – nélkülük nem létezhetnének a vállalkozások

Az ügyfelek a vállalkozás éltető elemei. Miközben az üzleti modelleket a digitális forradalom folyamatosan alakítja, sokan először találkoznak pénzforgalmi csalással. Nem mindegy, hogyan kezeljük az ilyen típusú visszaéléseket, hiszen döntően befolyásolják cégünk sorsát.

A digitális visszaélések okozta kihívások főbb jellemzői a következők:

- Az új digitális termékek új támadási felületet teremtenek. A termékek piaci bevezetésekor a vállalatok korábban jól bevált vállalkozási (business-to-business, B2B) folyamatokat követték, amelyek részei voltak a viszonteladók, forgalmazók és kiskereskedők. Napjaink innovatív B2B digitális platformjai azonban sokkal nagyobb támadási felületet adnak, ami lényegesen megnöveli a visszaélések lehetőségét.
- Az iparágak közötti választóvonalak elmosódnak. A digitális gazdaságban azt tapasztaljuk, hogy egyes nem pénzügyi szolgáltatásokat nyújtó vállalatok átnyúlnak a fizetési rendszerek területére. Míg hagyományosan a pénzügyi szolgáltatási szektor rendelkezett a legfejlettebb visszaélések elleni intézkedésekkel és a legtöbb visszaélési és pénzmosással kapcsolatos tapasztalattal, a fizetési rendszerek piacára újonnan belépőknek nincs ilyen tapasztalatuk és szaktudásuk. Ezáltal az új belépők és rendszereik a visszaélési és a szabályozási kockázatoknak egyaránt ki vannak téve.
- Az elkövetők technikailag egyre kifinomultabbak. A digitális visszaélések egyre kifinomultabbá, alaposabbá

és pusztítóbbá válnak. Emlékezzünk például arra, amikor 2017-ben egyetlen zsarolóprogram-támadás elég volt ahhoz, hogy megbénítsa a brit nemzeti egészségügyi szolgálatot (és még világszerte több százezer számítógépet), emberek életét sodorva veszélybe. Vagy amikor 2016-ban a nemzetközi bankrendszer egyik pillérét, a SWIFT bankközi tranzakciós rendszert kompromittálták támadók – azt a rendszert, amelyen keresztül a bankok nap mint nap dollármilliárdokat utalnak egymásnak –, és ezáltal a bangladesi nemzeti banktól közel 100 millió amerikai dollárt loptak el.

- A hitelkártyaszámot meg lehet változtatni, a születési időnkét viszont már nem. A visszaélések megakadályozására korábban használt tudásalapú hitelesítési eszközök mára elavultak, a legtöbb cég azonban még nem cserélte le ezeket. Amikor például egy intézményt súlyos biztonsági incidens ér, nem pusztán pótolható vagyontárgyat (pénzeszközt) tulajdonítanak el, hanem olyan egyedi személyi azonosítókat, mint például a születési idő vagy a TAJ-szám. Mivel ezeket az adatokat jellemzően éppen a visszaélések megelőzésére használják, azok ellopása a személyi adatokkal való további visszaélést tesz lehetővé. Sajnos sok vállalkozás még nem vezette be az új módszereket (pl. digitális eszközazonosító, hang- és más biometrikus azonosítók), amelyek ügyfeleik javainak védelmét lennének hivatottak biztosítani.

Mi történik az ügyfelek pénzével?

Jóllehet az ügyfelek elégedettségének biztosítása első számú feladat, a visszaélések megelőzésének mélyebb dimenziói is vannak. Többek között ide tartozik a visszaélésekre szakosodott alvilág, és az azt kontrollálni hivatott szabályozási és büntetőrendszerek. Képzeljünk el egy olyan esetet, amikor ellopják egy ügyfél személyes adatait – egy csaló az ügyfél nevében hitelkártyát igényel és jelentős tartozást halmoz fel. A veszteséget a bank vagy a kereskedő megtéríti, mentesítve az ügyfelet a további felelősség alól. Eddig ez volt a külső felek által elkövetett visszaélések orvoslásának módja, és ezt valamennyi fél – a bankok, kereskedők, fogyasztók és hatóságok – az üzleti együttműködés velejárójaként fogadta el.

A probléma azonban az, hogy a visszaélés itt nem ér véget. Bizonyos tekintetben ez a bűncselekmény csak a kezdet. Hiszen miközben az ügyfél kára minden bizonnyal megtérült, a lopott pénz már a visszaélések mélyebb rendszerében kering. Ezek a pénzek egyre inkább bűncselekmények, például terrorizmus, emberkereskedelem, illetve szervezett bűnözés finanszírozására szolgálnak. Bár ezek a visszaélések a pénzmosás

megelőzéséről szóló törvényre (Pmt.) és hasonló szabályozásokra válaszként létrehozott, meglévő tranzakciófigyelő rendszerekkel felderíthetők, valószínűleg sem a bankok, sem a pénzügyi szolgáltatók nincsenek tisztában azzal, hogy az ilyen tranzakciók hogyan jelennek meg a rendszerben – ahogyan arra nemrégiben rávilágított egy olyan esethez kapcsolódó szabályozói eljárás, amelyben egyik vállalatípusnál sem észlelték az emberkereskedelem finanszírozására utaló jeleket. A nem pénzügyi társaságok is könnyen követhetnek el törvényszegést, annak ellenére, hogy rájuk nem a pénzügyi szolgáltatókkal azonos szabályozói kötelezettségek vonatkoznak. Ennek oka, hogy a szabályozó és büntetőszervek a bűncselekmények – például a hamisított áruk kereskedelme – elsődleges hatásánál távolabbra tekintenek, és azt vizsgálják, hogy a lopott eszközöket milyen tiltott tevékenységek finanszírozására használják. Feladatuk részeként azt is alaposan vizsgálják, hogy a nem pénzügyi társaságok által a megfelelés és a visszaélések kivédése érdekében tett intézkedések nem tartalmazzak-e az ilyen bűncselekményekkel kapcsolatos, tudatos vagy akaratlan bűnsegélyre utaló jeleket – ami szintén az ágazatok közötti elmosódott határvonalakat mutatja a visszaélések

Üzleti indokoltság

A visszaélések kivédésére szolgáló technológiába történő beruházást üzletileg nemcsak a hírnév romlása, illetve a szabályozási kockázat vagy pénzügyi károk elleni védekezés indokolja. A technológia használatával a hatékonyság révén csökken a visszaélések megelőzésének költsége; digitális platformon biztonságosan hozhatók létre és értékesíthetők új

termékek és szolgáltatások; az ügyfelekkel való konfliktusok mérséklése érdekében finomhangolható a visszaélések kivédését szolgáló program, ami lehetővé teszi, hogy a jóindulatú ügyfelek szabadabban, a visszaélések megelőzését célzó kontrollaktól nem akadályozva használhassák a vállalati platformokat.

Kapcsolat



Polacsek Csaba

Cégtárs
Üzleti tanácsadás
+36 1 461 9751
csaba.polacsek@hu.pwc.com



Pataki Ferenc

Vezető tanácsadó
Üzleti tanácsadás
+36 30 958 3604
ferenc.pataki@hu.pwc.com



<http://www.pwc.com/hu/gazdasagibunozes>

© 2018 PricewaterhouseCoopers Magyarország Kft. Minden jog fenntartva.
Ebben a dokumentumban a „PwC” kifejezés a PricewaterhouseCoopers Magyarország Kft.-re utal, egyes esetekben pedig a PwC hálózatra vonatkozik.
Minden tagvállalat önálló jogi személy. További információért, kérjük keresse fel a <http://www.pwc.com/structure> weboldalt.
Ez a kiadvány kizárólag általános tájékoztatásul szolgál és nem minősül szakmai tanácsadásnak.