EMPIRICAL ANALYSIS OF THE INFORMATION SECURITY CHARACTERISTICS IN THE HUNGARIAN BUSINESS ORGANIZATIONS

A MAGYARORSZÁGI GAZDÁLKODÓ SZERVEZETEK INFORMÁCIÓBIZTONSÁGI JELLEMZŐINEK EMPIRIKUS ELEMZÉSE

HORVÁTH Ádám Béla[1]

Abstract

This publication is based on a questionnaire survey conducted in 2019-2020 among Hungarian for-profit organizations. 498 respondents participated in this research, 99% of them can be considered small or medium-sized enterprises. The sub-research examines the question of whether information security incidents are indeed discrete events, or whether the (Bayesian) stochastic relationship can be between them statistically confirmed. One sub-question of this research, if the compliance issues can be perceived as a security incident. The research also confirms the fact that systemic and non-systematic risks can be identified among IT risks, similarly to the financial world, thus sophisticate the previous picture of operational risks. One of the unexpected results of the research is that countermeasures against certain risks may indeed reduce the probability of a given risk occurring, but in the case of other risks it has the exact opposite effect: it increases the chances of the risk realisation.

Keywords

Empirical analysis, modelling, small and medium enterprises, information security, security incidents, compliance

Absztrakt

Jelen publikációm alapjául egy 2019-2020-ban, a magyarországi gazdálkodó szervezetek körében végzett kérdőíves felmérés szolgál. Ebben a lekérdezésben 498 válaszadó adott választ, amelyeknek 99%-a kis- vagy középvállalkozásnak tekinthető. Az itt bemutatott részkutatása azt a kérdéskört vizsgálja, hogy az információbiztonsági incidensesek valóban diszkért események-e, vagy ezek közötti (bayesi) sztochasztikus kapcsolat statisztikailag igazolható-e? Ennek egyik alkérdése, hogy a compliance problémák felfoghatóak-e biztonsági incidensként? A kutatás igazolja továbbá azt a tényt, hogy informatikai kockázatok között azonosítható – a pénzügyi világhoz hasonlóan – szisztematikus és nem szisztematikus kockázatok, így árnyalva a működési kockázatokról alkotott korábbi képet. A kutatás egyik váratlan eredménye, hogy bizonyos kockázatok ellen meghozott ellenintézkedés valóban csökkentheti az adott kockázat bekövetkezési valószínűségét, viszont más kockázatok esetében pont ellentétes hatással jár: megnöveli a kockázat realizálódásának esélyét.

Kulcsszavak

Empirikus elemzés, modellezés, kis- és középvállalatok, információ biztonság, biztonsági incidensek, compliance

[1] kutatas@horvath-adam.hu | ORCID: 0000-0001-5136-9316 | PhD-hallgató / PhD Student | Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

Asta Tarutė és szerzőtársa 2014-es tanulmányában [1] tanulmányában bemutatta, hogy egy „hagyományos" ellátási láncban elhelyezkedő gazdálkodó szervezet életében milyen előnyökkel járhat az IT-megoldások minél szélesebb körű integrálása: a szerzőpáros által azonosított előnyök operatív jellegű hatékonyságnöveléstől kezdve egészen a stratégiai előnyökig terjed. Ugyanebben a tanulmány az Egyesült Királyságban működő kisvállalkozások elemzésén keresztül bemutatták, hogy IT-megoldások egyre szélesebb spektrumát nem az egyszeri implementáció révén integrálják, hanem egy fejlődési út vezet az első üzelti alkalmazásokról az első átfogóbb rendszer alkalmazásáig. Neirotti Paolo [2] és szerzőtársai 284 vállalat fejlődését elemezve mutatta ki, hogy kifejezetten a korai fejlődési szakaszukban marginálisan ruháznak az IT-infrastruktúrájukban. Részben ez lehet az oka, hogy egy ausztrál felmérés [3] szerint a 100 főnél kevesebb munkavállaló vállalatok egyharmada semmilyen megelőző óvintézkedést nem tesz az kiber-bűncselekmények megelőzése ellen, és a vállalatok 87%-a elegendőnek tartja mindössze az végponti biztonság (antivírus programok) telepítését.

Az elégtelen információ-biztonsági intézkedésekre (is) visszavezethető információbiztonsági incidenseknek számos több következménye lehet: a legkézenfekvőbb következménye az operatív kár, amely az esemény bekövetkeztéből ered. Ehhez kapcsolódnak olyan stratégiai károk, mint a piaci image és pozíció romlása, és ennek gyakran van egy vállalaton belüli következménye: gátként hat a jövőben meghozandó infokommunikációs megoldásokhoz kapcsolódó innovációs döntések során. Ez pedig hosszabb távon gátolhatja a gazdálkodó szervezetek fejlődését. [4]

A KUTATÁS ELMÉLETI HÁTTERE

A különböző kockázat-értékelési és kezelési eljárásokat többféleképpen csoportosíthatjuk (kvalitatív vs. kvantitatív [5], szakértői becslésen [6] vs. veszteség-adatbázison alapuló, mint amilyet a Bázel-II AMA eljárása is ajánl [7].). Amennyiben sikerül megbecsülni vagy explicit módon meghatározni az egyes kockázatok bekövetkezési valószínűségét és várható kárérték mértét / mértékeit (a kárértéket gyakran az információbiztonsági dimenziók mentén határozzák meg, tehát egy kockázat teljes kárértéke az egyes dimenziók szerinti körtékék összege), akkor a kockázatokat el lehet helyezni egy kockázati-mátrixban, és mindezek alapján megfelelő ellenintézkedéseket lehet foganatosítani. Ez a megközelítés implicit módon a következő feltételezésekkel él:

- Az egyes kockázatok bekövetkezési valószínűsége és a lehetséges kárértéke egymástól független, tehát nincs szinergia hatás
- A kockázatokkal szemben meghozott ellenintézkedések csak az adott kockázatra hatnak, tehát a kereszthatás nem mutatható ki.

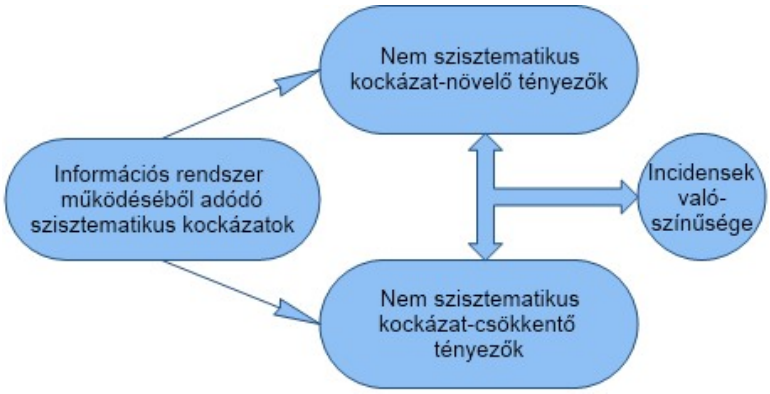
Ezzel szemben több szerző (angol nyelven [8], magyar nyelven: [9]) azzal a feltételezéssel él, hogy ezek a premisszák nem igazak, és felállítottak olyan elméleti modelleket, amelyekben az egyes kockázatok között mégiscsak léteznek kapcsolatok. Ez a feltételezés azzal a következménnyel jár, hogy ha egy hipotetikus „A" kockázat realizálódása sztochasztikus módon indukálja „B" kockázat bekövetkeztét, akkor az „A" kockázat kárértéke már nemcsak a saját kárértéke, hanem ehhez hozzáadódik „B" kockázat feltételes valószínűség-

gel korrigált kárértéke. Egy bayes-i feltételes valószínűségen alapuló kockázatkezelés azonban azzal a nehézséggel jár, hogy amint számos kutatás igazolta, a feltételes valószínűség mértéken kvantitatív módon, szakértői becsléssel csak nagyon pontatlanul határozható meg [10] [11], pontos becsléshez kvalitatív veszteség-adatbázisra van szükség. [A jelen publikációban bemutatott rész-kutatás a következő kérdésekre keresi a választ:

- Kimutathatóak-e a kérdőívet kitöltők körében az egyes realizálódott kockázatok (biztonsági incidensek) között sztochasztikus kapcsolat?
- Amennyiben kimutatható sztochasztikus kapcsolat, elkülöníthetőek-e
- Kimutathatóak-e a kockázatokkal szemben foganatosított ellenintézkedések körében „másodlagos", nem szándékolt hatás?
- A jogszabályoknak való megfeleltségre (compliance) tekinthető e a hatodik információ-biztonsági dimenzióként.

A KUTATÁS ÉS AZ EREDMÉNYEK

A gazdálkodó szervezetek informatikai infrastruktúrája és információbiztonsági érettsége között nyugvó összefüggéseket feltárni célzó kvantitatív kutatás, illetve annak a jelen publikációban bemutatásra kerülő részkutatás alapjául szolgáló adatbázis egy kérdőíves lekérdezés útján jött létre, illetve az egyes gazdálkodó szervezetektől beérkezett válaszok mellett a válaszadók pénzügyi beszámolóiból származó adatokkal kerültek kiegészítésre. A most bemutatott részkutatás elméleti modelljét a következő ábra segítségével foglalom össze.



1. Ábra: A részkutatás elméleti modellje (forrás: saját szerkesztés).

A részkutatás abból a feltételezésből indul ki, hogy az informatikai rendszereknek – átvéve a terminológiát a pénzügyi világból - vannak szisztematikus kockázatai, amely egy adott informatikai megoldásokat használók között minden felhasználóra – használat mértékétől függően – azonos módon, de eltérő mértékben hatnak: ide értendőek többek között azokat a hibák, amelyeket hibajavításokkal (patch) vagy frissítésekkel (update) szokott a gyártó javítani; ezzel szemben állnak azok a felhasználás egyedi módjából nem szisztematikus tényezők (például: erős jelszókövetelmény, biztonsági másolat megszervezése), amelyek egyedi módon növelik vagy csökkentik az információ-biztonsági incidensek realizálódásának valószínűségét. (Nem ebben a kutatásban használják fel a szisztematikus kockázat és nem szisztematikus kockázat fogalmát nem pénzügyi kontextusban [12].)

A kvalitatív kutatás alapjául egy online kérdőív-rendszer segítségével lebonyolított adatfelvétel révén előállít adatbázis szolgál. A kérdőív eredeti koncepciója – első változata – szerint a fent bemutatott modell mindhárom elemét (szisztematikus kockázatok, nem szisztematikus kockázat-növelő és csökkentő tényezők) az információ-biztonsági dimenziók (bizalmasság, integritás, rendelkezésre állás, letagadhatatlanság, reprodukálhatatlanság) szemszögéből kerülnek felmérésre, de a kérdőív első változatával lebonyolított próbakiötöltetések során kapott visszajelzések alapján több, a jelen publikáció szempontjából releváns kérdést törölni kellett, és így alakult ki a kérdőív végleges változata, amelyben a válaszdóknak mindösszesen 75 kérdésre kell választ adniuk. A kutatásba legalább kettő éve létező, nem digitális termékeket és / vagy szolgáltatásokat gyártó, illetve forgalomba hozó gazdálkodó szervezetek kerültek bevonásra. A kutatásba bevont gazdálkodó szervezetekkel e-mailen történt a kapcsolatfelvétel, és a kutatást támogatta több szakmai vagy területei alapon szerveződő kamara, illetve érdekvédelmi szervezet is. A kérdőív felépítésébe során szempont volt, hogy lehetőleg egyetlen vezető beosztású személy is ki tudja tölteni. A lekérdezéshez használt LimeSurvey nevű rendszer a beállításaival lehetővé teszi, hogy minden kérdést ne meg kelljen válaszolni, így biztosítható volt, hogy a kérdőívben ne maradjon megválaszolatlan kérdés. Ennek az is lett következménye, hogy nagyon sok félbehagyott kitöltésre került sor, 1 teljesen kitöltött kérdőívre nagyságrendileg 3-4 félbehagyott kérdőív jutott. A kutatásba közel 22.000 vállalat került bevonásra, és mindösszesen 498 értékelhető válasz érkezett. Az online kérdőív-rendszer lehetővé teszi a válaszok széles körben elterjedt fájlformátumban történő exportálását, egy táblázatkezelő szoftverrel készítettem elő statisztikai elemzéshez az adatokat és generáltam az ábrákat, valamint kereszttáblás lekérdezéseket, és az R keretrendszerét és annak több modulját használtam a statisztikai elemzésekhez. A nem szisztematikus kockázat-növelő és tényezők kérdéseit és az arra kapott válaszokat, a következő, táblázatban foglaltam össze:

Kérdés azonosítója	Kérdés szövege	Nem jellemző	Részben jellemző	Jellemző
C1/4	A GDPR hatályba lépését megelőző négy évben történt jelentős mértékű informatikai eredetű üzemzavar.	330		40
C1/5	A GDPR hatályba lépését megelőző négy évben volt a cégünkben több gépet érintő vírustámadás/-fertőzés.	294		76
C1/7	A GDPR hatályba lépését megelőző négy évben történt a vállalat életében jelentős mértékű meghibásodásból származó adatvesztés.	331		39
C1/9	Nehézséget jelentett a következő események valamelyike: GDPR bevezetése, online pénztárgépek bevezetése, NAV- hoz bekötött számlázó alkalmazás használata	262		108
C1/3	Problémát jelent, hogy különböző alkalmazások között adatokat kell manuálisan át/feltölteni.	186	142	42

Kérdés azonosítója	Kérdés szövege	Nem jellemző	Részben jellemző	Jellemző
C1/13	Fenn kell tartani valamilyen elavult informatikai rendszert, mert a rajta futó alkalmazást nem tudjuk frissíteni / helyettesíteni.	226	105	39
C1/19	Elegendőnek érezzük, hogy csak megvásárolható biztonsági alkalmazásokat (antivírus + tűzfal) telepítjük.	84	149	137
C1/2	Több évre visszamenőleg minden adat biztonsági mentés formájában a rendelkezésünkre áll, bármikor el tudjuk érni.	13	83	274
C1/6	A számítógépes hálózatunkat (LAN, WIFI) legalább egy haladó szintű védelemmel biztosítjuk	24	50	296
C1/8	Nyomon tudjuk követni a bejelentkezett felhasználók tevékenységét: ellenőrizzük napló-állományokat vagy behatolás-figyelő rendszert telepítünk.	106	129	135
C1/10	Képesek vagyunk az üzleti szempontból fontos állományokat titkosítva tárolni.	60	113	197
C1/14	Lemondunk valamelyik kényelmi szolgáltatásról a nagy biztonság érdekében: nem használunk laptopokat / USB- adathordozókat stb.	298	58	14
C1/15	Telepítettünk a legfontosabb informatikai eszközökhöz szünet-mentes tápegységet.	46	50	274
C1/16	Gondoskodunk arról, hogy szoftverek frissítései minél gyorsabban telepítésre kerüljenek.	21	97	252
C1/17	A legfontosabb eszközökből vannak tartalékaink meghibásodás esetére.	58	149	163
C1/20	Inkább használunk komplex biztonsági alkalmazásokat (antivírus + tűzfal), mint egyesével külön telepített megoldásokat.	54	118	198

1. táblázat: A biztonsági incidensek korrelációs mátrixa (forrás saját szerkesztés)

A kérdőívben lehetőség volt a „Nem tudom / nincs válasz" megjelölésére is. A kitöltések kiértékeléséből kitűnik, hogy erre megoldásra szükség volt, hiszen csak 370 olyan kitöltésre került sor (az összes kitöltés bő háromnegyede, pontosabban: a 74,30%-a), ahol egyetlenegy esetben sem adott „Nem tudom / nincs válasz"-t. Tekintettel arra, hogy a kérdőív további kérdései nem tették lehetővé, hogy következtetni lehessen, hogy mi motiválta a „Nem tudom / nincs válasz" megjelölését, ezért ebben a részkutatásban csak azt a 380 kitöltések vonom be az elemzésbe, ahol a válaszadó nem adott ilyen választ. Az 1. ábrán logikát követve:

- Nem szisztematikus kockázat-növelő tényezőkre a C1/2, C1/6, C1/8, C1/10, C1/14, C1/15, C1/16, C1/17 és a C1/20 jellegű kérdések vonatkoztak. Az adatfeldolgozás

során a „nem jellemző” válasz 0-as értéket kapott, a „részben jellemző” érték 0,5-ös értéket kapott és a jellemző érték 1-es értéket kapott.;

- nem szisztematikus kockázat-csökkentő tényezőkre a C1/3, C1/13 és a C1/19 jelű kérdések vonatkoztak. Az válaszok elemzésbe történő bevonása az előbbiekhez hasonlóan történt.
- információbiztonsági incidensekre a C1/4, a C1/5, C1/7 és a C1/9 jellegű kérdések vonatkoztak. A részkutatásba bevont 370 válaszadóból 191 (51,62%) nem számolt be információ-biztonsági incidensről, 120 válaszadó (32,43%) jelölt be 1 incidenst, 39-en (10,53%) jelöltek be 2, 15-en (4,05%) 3, és 5-en (1,35%) számoltak be mind a négy incidens bekövetkeztéről. Tekintettel arra, hogy eredmény-változóként azt vizsgáltam, hogy következett-e be bármilyen mértékű incidens, ennél a válasznál 0-as értéket kapott a „nem jellemző” válasz, és mind a „részben jellemző” és „jellemző” válasz 1-es értéket kapott.

Az elemzés első lépésében megvizsgálom az egyes kategóriákon belüli korrelációk alakulását. A biztonsági incidensek közötti korrelációs mátrixot a 2. táblában foglaltam össze (mindhárom mátrix esetében a cellák felső sorában a számított korreláció, az alsó sorban a számított p-érték került feltűntetésre).

	C1/4	C1/5	C1/7	C1/9
C1/4	1,00	0,25 (0,0000)	0,39 (0,0000)	0,14 (0,0069)
C1/5	0,25 (0,0000)	1,00	0,20 (0,0002)	0,06 (0,2813)
C1/7	0,39 (0,0000)	0,20 (0,0002)	1,00	0,05 (0,3313)
C1/9	0,14 (0,0069)	0,06 (0,2813)	0,05 (0,3313)	1,00

2. táblázat: A biztonsági incidensek korrelációs mátrixa (forrás saját szerkesztés)

Ahogy a korrelációs mátrixból leolvasható, a lehetséges 6 változó-párból kettő esetében nem mutatható ki szignifikáns korrelációs. Mindkét nem szignifikáns korreláció egyik tagja a C1/9 kérdés, amely nem klasszikus információ-biztonsággal kapcsolatos incidensekre kérdez rá, hanem a törvényi előírásoknak való megfeleltséggel (compliance) kapcsolatos problémákra kérdez rá. A szignifikáns korrelációk megerősítik azt a feltételezést, hogy a biztonsági incidensek nem diszkért események, hanem ezek a káresemények bekövetkezte egymásra hatással vannak.

A nem-szisztematikus kockázatnövelő-tényezők közötti kapcsolatot az alábbi mátrix mutatja meg:

	C1/3	C1/13	C1/19
C1/3	1,00	0,16 (0,0022)	0,01 (0,8707)
C1/13	0,16 (0,0022)	1,00	-0,06 (0,2593)
C1/19	0,01 (0,8707)	-0,06 (0,2593)	1,00

3. táblázat: A biztonsági incidensek korrelációs mátrixa (forrás saját szerkesztés)

Ahogy a korábbiakban bemutattam, a kutatás sikere érdekében jelentős körültekintéssel kellett eljárnom az információbiztonsági incidensekre vonatkozó kérdés feltételekor. A három kérdőívben maradt kérdés mindegyike olyan kockázatnövelő-tényezőre kérdez rá, amelyhez kapcsolódó incidensek bekövetkeztének esetében valószínűsíthetőek a vis maior jellegű esemény, azaz nem kell a jogellenes magatartást feltételezni. Az egyetlen szignifikáns korrelációt eredményező kérdéspár (C1/3 és C1/13) mindkét párja a „rendelkezésre állás" biztonsági dimenzióját érintő kockázat-növelő tényező. Sajnálatosan nagyon nagy kockázattal járt volna, a kockázat-növelő tényezők szélesebb körű felmérésének kísérlete. Abból a tényből, hogy a tényezők között vagy egyáltalán nincs szignifikáns korreláció, vagy a szignifikáns korreláció is gyenge kapcsolatot mutat, arra lehet következtetni, hogy a válaszadók kockázati térképe egymástól jelentős mértékben eltér.

Az információ-biztonsági-incidensek és a nem-szisztematikus kockázatnövelő-tényezők analógiájára megvizsgáltam a nem-szisztematikus kockázatcsökkentő-tényezők tényezők korrelációs kapcsolatát. Olvashatósági okokból kifolyólag a 9×9 dimenziójú korrelációs mátrix nem kerül itt bemutatásra, a 36 lehetséges változó párból csak azok változópárok nem mutattak szignifikáns korrelációt, ahol az egyik változó-pár egyik tagja a C1/14 jelű kérdés. A szignifikáns korrelációt mutató kérdések-párok körében a korreláció mértéke 0,16 és 0,35 közötti értékeket vett fel.

Bármely két kérdésre kapott választ reprezentáló változó között kimutatott korrelációs kapcsolat, pusztán a köztük fennálló lineáris kapcsolat erősségének mérésére szolgál. [14] Az előbbiekben bemutatott korreláción alapuló elemzések eredményéből azt valószínűsítik, hogy lehetséges olyan szignifikáns regressziós modell felállítása, amelynek általános képlete az 1. ábra alapján:

$SZR + NSZR^{+} - NSZR^{-}$ = Incidensek bekövetkezési valószínűsége
ahol:
SZR: a szisztematikus kockázatok összesége
$NSZR^{+}$:a nem szisztematikus kockázatnövelő tényezők összessége
$NSZR^{-}$: a nem szisztematikus kockázatcsökkentő tényezők összessége

a modell igazolására az konstruktív ökonometriai iskola [13] eljárás-mintáját követve az un. stepwise regressziós modell felállításával kerül sor. Az így felállított négy regressziós modell mindegyike szignifikánsak bizonyult, amint azt alábbiakban bemutatott ANOVA-táblázatokról is leolvasható (a táblázatban csak a szignifikáns változók kerülnek feltüntetésre):

R^2:		0,2188				
Korrigált R^2:		0,2037				
F-próba		14,49				
Szabadságfok:		7 és 362				
p-érték:		2,2e-16				
Változó neve		Becsült érték	St. hiba	t-érték	Pr(>|t|)	szig.
Tengelymetszet	(β_0)	0,1951	0,0665	2.936	0,0035	**
C1/2	(β_1)	-0,1447	0,0574	2,519	0,0122	*
C1/4	(β_2)	0,3650	0,0476	7,667	1,64e-13	***
C1/5	(β_3)	0,0634	0,0368	1,721	0,0860	.
C1/6	(β_4)	-0,2089	0,0551	-3,791	0,0001	***

Változó neve		Becsült érték	St. hiba	t-érték	Pr(>|t|)	szig.
C1/16	(β_5)	0,1024	0,0518	1,978	0,0487	*
Szignifikancia kódok:		”***”: 0,001	”**”: 0,01	”*”: 0,05	”.”: 0,1	” ”: 1

4. táblázat: Regressziós-model (eredmény-változó: C1/7) ANOVA-táblázata (forrás: saját szerkesztés)

Ebben a regressziós modellben azt vizsgáltam, hogy milyen tényezők csökkentik, illetve növelik a válaszadók körében az adatvesztés bekövetkeztetét. Fel kell hívni a figyelmet arra, hogy a tengelymetszet és szignifikáns alkotóeleme a regressziós-modellnek, amely azért fontos, mert így a vállalati IT-környezet szisztematikus kockázata reprezentáltnak tekinthető. A modell verifikációjaként tekinthetünk arra körülményre, hogy kettő, nem szisztematikus kockázat-csökkentő tényező, a biztonsági másolatok megléte (C1/2), és hálózati infrastruktúra emelt szintű védelme is szignifikáns változó (C1/6 jelű kérdés), és mindkettő előjele negatív, így ezek az intézkedések valóban be tudják tölteni szerepüket. A hálózati infrastruktúra szignifikáns szerepe modellben azért két szempontból is jelentős eredmény: egyrészről ezzel sikerült bebizonyítani, hogy az egyes biztonsági intézkedéseknek nemcsak azokon a területeken jut jelentős szerephez, amelyre területen „magától értetődően” el kell látnia a feladatát, hanem kimutatható egyfajta „kereszt-hatás” is; másrészről, ha olyan hálózati adattárolási megoldásokra gondolunk, mint a NAS- és SAN-eszközök, akkor visszaköszönni látszik az a körülmény, hogy a helyi hálózati- és adattárolási megoldások egy komolyabb IT-környezetben egymástól nem választhatóak el [15].

Szintén a kutatás eredményének kell értékelni, hogy megjelent a magyarázó változókban megjelentek – bár eltérő súllyal és szignifikancia-szinttel - más információ-biztonsági incidensek (ebben az esetben az informatikai üzemzavarokra vonatkozó C1/4 jelű, és a vírustámadásokra vonatkozó C1/5 jelű kérdések). és ezzel sikerült igazolni, hogy a kutatás alapgondolata helyes, azaz egyes káresemények bekövetkezte nem függetlenek egymástól.

A kutatás érdekes eredménye, hogy egy olyan intézkedés (a frissítések telepítésére vonatkozó C1/16 jelű kérdés, amelyről eredetileg azt feltételeztem, hogy növeli az adott szervezetben az információ-biztonság szintjét (ha rendszeresen végrehajtott intézkedés), a regressziós modell eredménye alapján inkább a kockázati kitettséget növelő tényező.) Ennek sajnos létezik gyakorlati válasza is (például a Windows 10 frissítésével fellépő problémák 2020. októberében.), és ezt tudományos alapon vizsgálja Tudor Dumitras és szerzőtársa [16]

R^2:		0,2067				
Korrigált R^2:		0,1980				
F-próba		23,77				
Szabadságfok:		4 és 365				
p-érték:		2,2e-16				
Változó neve		Becsült érték	St. hiba	t-érték	Pr(>|t|)	szig.
Tengelymetszet	(β_0)	-0,0723	0,0498	-1,453	0,1471	
C1/5	(β_1)	0,1386	0,0366	3,789	0,0002	***
C1/6	(β_2)	0,1033	0,0515	2,006	0,0456	*
C1/7	(β_3)	0,3676	0,0486	7,564	3,2e-13	***
C1/9	(β_4)	0,0806	0,0320	2,521	0,0121	*
Szignifikancia kódok:		”***”: 0,001	”**”: 0,01	”*”: 0,05	”.”: 0,1	” ”: 1

5. táblázat: Regressziós-model (eredmény-változó: C1/4) ANOVA-táblázata (forrás: saját szerkesztés)

Ebben a regressziós modellben azt vizsgáltam, hogy milyen tényezők vezetnek az informatikai üzemzavarok bekövetkeztéhez (C1/4 jelű kérdés.) Ebben a modellben a konstans változó nem szignifikáns, így ebben az esetben a szisztematikus kockázat szignifikáns voltanem mutatható ki. a négy szignifikáns változóból három biztonsági kockázat – így ebben modellben ugyanígy érvényes az előző modell esetében tett megállapítás, miszerint a kutatás alapgondolata helyes, azaz egyes káresemények bekövetkezte nem függetlenek egymástól, azaz statisztikailag igazolható egy negatív irányú szinergia-hatás kialakulásának valószínűsége. Az előző modellhez hasonlóan kockázat-növelő tényezőként jelenik meg egy olyan elem, amely elméletileg kockázat-csökkentő hatással kellene bírnia (C1/6 kérdés):

R^2:		0,1143				
Korrigált R^2:		0,0996				
F-próba		7,805				
Szabadságfok:		6 és 363				
p-érték:		6,491e-08				
Változó neve		Becsült érték	St. hiba	t-érték	Pr(>|t|)	szig.
Tengelymetszet	(β_0)	0,0982	0,0626	1,568	0,1178	
C1/4	(β_1)	0,2584	0,0700	3,692	0,0002	***
C1/7	(β_2)	0,1535	0,0708	2,169	0,0308	*
C1/10	(β_3)	-0,1435	0,0564	-2,546	0,0113	*
C1/14	(β_4)	-0,1582	0,0794	-1,993	0,0470	*
C1/15	(β_5)	0,1134	0,0598	1,895	0,0589	.
C1/20	(β_6)	0,6270	0,0570	2,227	0,0266	*
Szignifikancia kódok:		”***”: 0,001	”**”: 0,01	”*”: 0,05	”.”: 0,1	” ”: 1

6. táblázat: Regressziós-model (eredmény-változó: C1/5) ANOVA-táblázata (forrás: saját szerkesztés)

A jelen publikációban bemutatásra kerülő harmadik modell azt vizsgálja egy számítógép-vírus fertőzés elterjedését. Itt is találkozhatunk kettő olyan jelenséggel, amellyel a korábbi kettő modell esetében, azaz, ebben a modellben sem mutatható ki a szisztematikus kockázat (azaz a tengelymetszet) szignifikáns volta, és itt is kimutatható statisztikailag a többi incidens bekövetkeztének kockázat-növelő hatása. Szintén találkozunk azzal jelenséggel, hogy két olyan elem tölt be kockázat-növelő hatást, amelynek az információ-biztonság szintjét kellene elméletileg növelnie: a jelen kérdőívek nem ad rá választ, hogy miért mutatható ki – alacsony szignifikancia-szintű és együtthatójú, de ettől független figyelembe veendő – kapcsolat a szünetmentes-tápegységek és a vírusfertőzések között. Lehetséges okként merül, hogy mindkét tényező egy, a kérdőívben nem vizsgált harmadik tényezővel áll szignifikáns kapcsolatban. Az eredetileg kockázat-csökkentő tényezőnek C1/20-as kérdés kockázat-növelő hatásában sajnos vissza-igazolódik az jelenség, hogy tisztán a végpontokre telepített biztonsági alkalmazások nem jelentenek valós megoldásokat – erről a jelenségről írtam a cikkem bevezetőjében is.

R^2:	0,0967
Korrigált R^2:	0,0893
F-próba	23,77
Szabadságfok:	3 és 366
p-érték:	4,069-08

Változó neve		Becsült érték	St. hiba	t-érték	Pr(>|t|)	szig.
Tengelymetszet	(β_0)	0,1443	0,0336	4,292	2,27e-05	***
C1/3	(β_1)	0,1851	0,0673	2,750	0,0063	**
C1/4	(β_2)	0,1667	0,0731	2,280	0,0232	*
C1/13	(β_3)	0,2956	0,0675	4,378	1,56e-05	***
Szignifikancia kódok:		”***”: 0,001	”**”: 0,01	”*”: 0,05	”.”: 0,1	” ”: 1

7. táblázat: Regressziós-model (eredmény-változó: C1/9) ANOVA-táblázata (forrás: saját szerkesztés)

A negyedik regressziós modellben ismét szignifikáns lett a tengely-metszet, amely a szisztematikus kockázatokat hivatott reprezentálni, és ebben az egye modellben kockázatnövelő tényezőként megjelenik egy olyan tényező, amely önmagában nem biztonsági incidens. Ezzel a modellel sikerült igazolni a biztonsági incidensek és compliance-jellegű vállalati nehézségek közötti kapcsolatot.

A KUTATÁS ÉS AZ EREDMÉNYEK

A kutatásomban négy regressziós modellt állítottam fel, amelyek igazolták a kutatási kérdéseket. Meglátásom szerint sikerült elkülöníteni a „szisztematikus” és „nem szisztematikus” IT-kockázatokat – ezért tartom jó körülménynek, hogy a négy modellből kettő esetben szignifikáns volt, és kettő esetben nem volt szignifikáns a tengelymetszet. Sikerült továbbá bebizonyítani, hogy bizonyos intézkedések vannak kockázat-növelő hatása, és egy biztonsági incidens katalizálható hatással járhat egy másik biztonsági incidens tekintetében.

A kutatás járt nem várt eredménnyel is: egyik ilyen nem várt eredmény, hogy bizonyos biztonsági intézkedés, részben vagy egészben pont a szándékolttal ellentétes hatást idézhet elő.

Kényszerűségből a kutatás alapjául szolgáló kérdőív nem foglalhatta magában mind az öt biztonsági dimenziót felmérni tudó kérdéseket. Meglátásom szerint a jelen részkutatás eredményei, illetve a további még publikálásra váró eredmények kiértékelése alapján szükséges lenne Magyarországon megvalósítani egy olyan, nagyobb legitimációval (tehát nem ismeretlen megkeresésre alapuló) bíró kutatást, amely mélységében méri fel az informatikai infrastuktúra és az információ-biztonság szinte közötti összefüggést. Azért lenne lényeges egy ilyen megismételt kutatás, mert tudatosító erővel bírni, hogy informatikai beruházások mérlegelésekor ne csak a várható előnyöket vegyék figyelembe, hanem jobban tudatosuljon a leendő informatikai infrastruktúra magában hordozott kockázata, azaz, amikor ár / érték arányról gondolkodunk, akkor kiegyensúlyozottabb viszonyba kerüljön a várható hasznosság (benefit) és kockázat.

KÖSZÖNETNYILVÁNÍTÁS

A jelen kutatás létrejöttét a 2017-1.3.1-VKE-2017-00031 azonosítószámú, „Nagy pontosságú burkolat vizsgáló mérési technológia alapjainak kutatási programja” pályázat támogatta. Külön köszönöm a Budapesti Kereskedelemi- és Iparkamara erkölcsi és operatív támogatását!

FELHASZNÁLT FORRÁSOK

[1] Asta Tarutė and Rimantas Gatautis, „ICT Impact on SMEs Performance" in Contemporary Issues in Business, Management and Education 2013 in Procedia - Social and Behavioral Sciences Volume 110, January 2014, pp. 1218-1225, DOI: 10.1016/j.sbspro.2013.12.968

[2] Neirotti, Paolo, Elisabetta Raguseo, and Emilio Paolucci, How SMEs develop ICT-based capabilities in response to their environment: past evidence and implications for the uptake of the new ICT paradigm, Journal of Enterprise Information Management, Vol. 31 No. 1, pp. 10-37., 2018.

[3] Office of the Australian Small Business and Family Enterprise Ombudsman, „Cyber Security: The Small Business Best Practice Guide", Commonwealth of Australia 2017

[4] Ponemon Institute LLC, „THE IMPACT OF DATA BREACHES ON REPUTATION & SHARE VALUE", USA, May 2017.

[5] Wangen, G., Hallstensen, C. & Snekkenes, E, „A framework for estimating information security risk assessment method completeness" Int. J. Inf. Secur. 17, 681–699 (2018). https://doi.org/10.1007/s10207-017-0382-0

[6] Fumika Ouchi, „A Literature Review on the Use of Expert Opinion in Probabilistic Risk Analysis", World Bank Policy Research Working Paper 3201, February 2004

[7] Shevchenko, Pavel V. and Peters, Gareth, Loss Distribution Approach for Operational Risk Capital Modelling Under Basel II: Combining Different Data Sources for Risk Estimation (2013). Available at SSRN: https://ssrn.com/abstract=2980464 or http://dx.doi.org/10.2139/ssrn.2980464

[8] Figini, Silvia and Gao, Lijun and Giudici, Paolo, „Bayesian operational risk models". Journal of Operational Risk. Vol 10. pp. 45-60. (2015) 10.21314/JOP.2015.155.

[9] Horváth Ádám, „ Gondolatok az informatikai kockázatok kapcsán" in: Prof. Dr. Rajnai Zoltán (ed), Rajnai, Zoltán (szerk.) Kiberbiztonság - Cyber Security : Tanulmánykötet a Biztonságtudományi Doktori Iskola kutatásaiból. pp. 109-120. ISBN: 978-963-449-131-6 2018)

[10] Alexander Pollatsek and Arnold D Well and Clifford Konold and Pamela Hardiman, George Cobb, „Understanding conditional probabilities", Organizational Behavior and Human Decision Processes vol. 40 No.2., pp. 255-269. DOI: 10.1016/0749-5978(87)90015-X

[11] André C. R. Martins, „Probability biases as Bayesian inference", Judgment and Decision Making, Vol. 1, No. 2, November 2006, pp. 108–117

[12] Yang-Byung Park and:Hyung-Seok Kim, „Simulation-based evolutionary algorithm approach for deriving the operational planning of global supply chains from the systematic risk management", Computers in Industry Volume 83, pp. 68-77. DOI: 10.1016/j.compind.2016.09.003.

[13] ÁCS Pongrác: SPORT ÉS GAZDASÁG. Pécs, 2015. ISBN 978-963-642-372-8

[14] Alireza Dorestani and Sara Aliabad, „Academy of Accounting and Financial Studies Journal" Vol. 21, No 3, pp 1-13 (2017).

[15] Roland Döllinger and Reinhard Legler and Duc Thanh Bui: Praxishandbuch Speicherlösungen. dpunkt.verlag, 2010. ISBN: 978-3-89864-588-1

[16] Tudor Dumitras and and Priya Narasimhan: „Why Do Upgrades Fail and What Can We Do about It? - Toward Dependable, Online Upgrades in Enterprise System” in: J.M. Bacon and B.F. Cooper (Eds.): Middleware 2009, LNCS 5896, pp. 349–372, 2009