A BIZTONSÁGI KULTÚRA

SECURITY CULTURE

LAZÁNYI KORNÉLIA egyetemi docens
Óbudai Egyetem, Keleti Gazdasági Kar, Szervezési és Vezetési Intézet

ABSTRACT

The problem of organisational safety and security exists ever since organisations do. Each era had its own defence, security and coping strategy for crisis situations. The aim of present article is to introduce and explore the various approaches of organisational safety. Besides the short description of the managerial and HR approach of organisational safety and security, safety culture, as a possible solution is presented. The paper is structured in a way that endeavours to display, how the weaknesses of one approach led to the emergence of the next theory. However, it is also presented that safety culture, although being the state-of-the-art solution, still has its deficiencies and has a wide space for further development.

1. Bevezetés

A szervezetek alapfeladata önmaguk fenntartása és a tulajdonosi érdekek kiszolgálás a profit termelés, valamint a vevői érdekek kiszolgálása termékek, vagy szolgáltatások előállítása révén. Ezt a feladatot akkor tudják rendeltetésszerűen ellátni, ha az alap- és támogató folyamatok zavartalanul valósulnak meg, a makro környezet stabilitása mellett, mely a válság hatására jelentős mértékben megváltozott (Csiszárik-Kocsir – Fodor, 2013), új feladatok, szerepek elé állítva a szervezeteket. Ennek előfeltétele, hogy a szervezet erőforrásainak sértetlensége, rendelkezésre állása, bizalmassága ne sérüljön; fenyegetettségük minimális legyen. A globalizáció következtében a nemzetközi pénzügyi integrációval kialakult kockázatmegosztás, illetve az átjárhatóságból adódó kockázatok tovaterjedése is jelentős mértékben hozzájárult a szervezetek biztonsági sérüléséhez, azaz kríziséhez (Timár – Borzán, 2013). Elengedhetetlen feltétele tehát az optimális működésnek a szervezet biztonsága. Jelentőségét jól mutatja, hogy a biztonsággal összefüggő tényezőket a gazdasági mutatókba is integrálták (Szigeti, 2105).

A szervezeti biztonság a nemzetközi szakirodalomban a külső fenyegetettségtől való védettséget, valamint a mentális és fizikai sérülés létének/veszélyének hiányát egyaránt magába foglalja. Célja, a szervezetek zavartalan működésének és az ahhoz szükséges peremfeltételek megteremtésén túl a személyzet, a fizikai környezet és a vállalati hírnév védelme. A szervezet biztonsága azonban csak akkor biztosítható, ha az erre irányuló intézkedések, integráltan, egyértelmű és egysé-

ges szempontok mentén kerülnek kialakításra és végrehajtásra (BAH, 2005). Jelen cikk célja, hogy bemutassa a szervezeti biztonsággal kapcsolatos megközelítéseket és eszközeiket, valamint rávilágítson azok hiányosságaira.

2. A szervezeti biztonság funkcionalista megközelítése

A szervezeti biztonság kérdésköre a szervezetekkel egyidős. Minden kornak megvolt a maga védelmi/védekezési és krízishelyzetekkel való megküzdési stratégiája. A korai elméletek a problémát funkcionalista módon közelítették meg (Kontogiannis, 2010). Hittek abban, hogy a külső veszélyek és a szervezeti működés gyenge pontjainak minél alaposabb feltárása, valamint a védelmi rendszer működtetése megteremti a szervezeti biztonságot. Melyen belül két fő irányzatot – a vezetői, illetve az emberi erőforrás alapú megközelítést – különböztethetünk meg.

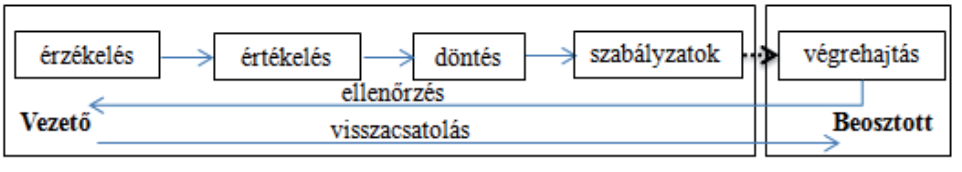
2.1. Vezetői megközelítés

A szervezeti biztonság megteremtése évezredeken keresztül a vezetők feladata volt. Nekik kellett gondoskodniuk arról, hogy ki legyen alakítva a szükséges folyamatok és rendszerek, ezekhez legyenek hozzárendelve az emberi és materiális erőforrások, valamint, hogy ki legyenek nevezve a felelősök. Ez volt a szervezeti túlélés záloga. A szervezetek hatékony működése szempontjából nagy jelentősége van tehát a szervezeti – vezetési – magatartási kockázatok kezelésének (Kovács et al. 2014, Szabó et al. 2014). A koronként változó vezető megközelítésekkel párhuzamosan, a megvalósítás eszköztára is igen változatos volt. A centralizált, panoptikon jellegű, „tökéletes” kontrollt biztosító totális rendszerek mellett, a szervezeti méret növekedésével, és a tevékenységek diverzifikálódásával párhuzamosan megjelentek a végrehajtás mellett az ellenőrzés feladatát is delegáló rendszerek.

Számos szervezet hozott létre biztonsági szabályzatot, rögzítette a munkavállalóktól elvárt viselkedést szervezeti működési szabályzatban, illetve állandó érvényű utasításokban (SOP). A szervezeti szintű biztonsági irányelvek helyi biztonsági tervekkel egészültek ki, készenléti, vészhelyzeti tervek kerültek kidolgozásra. Mindezek a rendszermegoldások a vezetői kontrollt voltak hivatottak kiterjeszteni, megerősíteni. A rendszer általános logikai modelljét az 1. ábra vázolja.

1. ábra: A szervezeti biztonság vezetői megközelítése

Graph 1: Managerial approach of organisational safety



A szervezet vezetőjének nem csupán létre kell hoznia egy működő struktúrát, szabályozási rendet, de személyes jó példával is élen kell járnia, elkötelezettséget kell mutatnia a szabályok minél teljesebb körű érvényessége érdekében. A példamutató magatartás mellett azonban nagyon fontos, hogy úgy fogalmazza meg a biztonsági szabályokat, hogy a szervezeti tagok számára egyértelműek és követhetőek legyenek. Felelősségi köröket kell definiálnia, melyeken belül a munkavállalók (csoportja) felelőssé tehető a krízis helyezetek, vagy más szervezeti biztonságot veszélyeztető események kialakulásáért. Folyamatosan vissza kell csatolnia a munkavállalóknak. A biztonsági előírásokat követő egyéneket díjaznia, a vonatkozó szabályokat áthágókat pedig büntetnie kell. Mint ahogyan az az 1. ábrán is jól látszik, a szervezeti biztonsággal kapcsolatos feladatok nagy része tehát a vezetőé. A szervezeti tagok felelőssége, és főleg a szervezeti biztonság iránti elkötelezettsége egy ilyen rendszerben igen alacsony. Kérdéses a szabályok betartása, az előírások követése. Éppen ezért kiemelt jelentősége van a vezető által működtetett motivációs rendszernek, – az ellenőrzésnek, a folyamatos felügyeletnek, valamint az erre épülő jutalmazási, büntetési rendszernek, mely a szabályzatok betartását hivatott elérni.

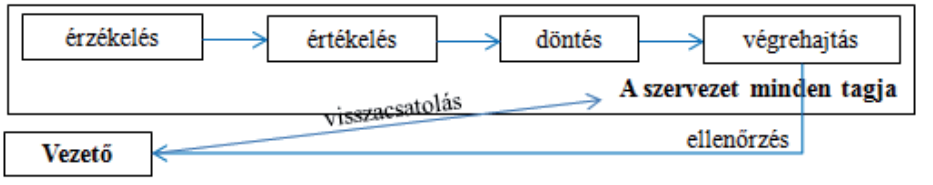
2.2. Emberi erőforrás szempontú megközelítés

Az alkalmazottak biztonság iránti elkötelezettségének fontosságából kiindulva, az 1980-as évektől egyre nagyobb tért nyertek a szervezeti biztonságot emberi erőforrás oldalról megközelítő rendszerek. A megközelítés lényege, hogy a szervezeti biztonság csupán a szervezeti tagok tudatos odafigyelése, felkészültsége és tevőleges részvétele mellett érhető el, mert a pusztán technikai védelmi eszközök számos esetben elégtelenek (Keszthelyi, 2013; 2014). Ennek értelmében a szervezet tagjait fel kell készíteni a várható krízis helyzetekre és vészhelyzeti problémákra, és lehetőséget kell biztosítani számukra, hogy ne csupán információkkal (előírások, SOP, …) rendelkezzenek, de meglegyenek a megfelelő kompetenciáik – elméleti és gyakorlati képességeik, készségeik – hogy felismerjék, azonosítsák, és megfelelő módon kezeljék a szervezeti biztonságot fenyegető tényezőket, helyzeteket. Ez a fajta kollektív tudás nem csak szervezeti, de társadalmi szinten is egyre fontosabb (Reisinger, 2012; 2013).

A verseny olyan működési teret jelent a vállalkozások számára, amelyet nem kerülhetnek meg, abban helyt kell állniuk és mindezt a képességeik határozzák meg. (Varga, 2014)

Az emberi erőforrás szempontú megközelítés előnye, hogy nem csupán a vezetőn múlik a rendszer biztonsága, de a szervezet minden szintje és tagja részt vesz a megfelelően működő rendszer kialakításában és működtetésében. A szabályzatokat közösen írják, az előírásokat együtt dolgozzák ki. A biztonsági előírások betartatása, valamint annak ellenőrzése azonban továbbra is a vezető, illetve az általa megbízott/kijelölt felelősök feladata; és pont ebben rejlik a rendszer legnagyobb hátránya is. A rendszer működési modelljét a 2. ábra szemlélteti.

2. ábra: A szervezeti biztonság emberi erőforrás szempontú megközelítése
Graph 2: Human resource approach of organisational safety



Az emberi erőforrás szempontú megközelítés előfeltételezi, hogy a szervezeti tagok képesek mindazon feladatok (észlelés, értékelés, döntés) megfelelő színvonalú elvégzésére, melyek korábban kizárólag a vezető(k) hatáskörébe tartoztak, tehát az ilyen szervezeti biztonsági rendszer csak megfelelő munkavállalói érettség mellett vezethető be. Fontos, hogy az alkalmazottak szakképzettsége, ismeretei a végzett munkának megfelelőek legyenek. Mindemellett azonban a szervezetnek (vezetőnek) biztosítania kell a megfelelő oktatást a szervezeti biztonsággal kapcsolatos explicit tudáselemek minél szélesebb körben való terjesztésére, és tréningeket kell szerveznie a rendszer működtetéséhez szükséges tacit kompetenciák átadására. Az emberi erőforrás szempontú megközelítés további hátránya, hogy bár a szervezet tagjai megkapják a felhatalmazást a biztonsági irányelvek és procedúrák kialakítására, – a saját személyes biztonságukat érintő kérdéseken túl – nem érdekeltek a rendszer működtetésében. Ugyan a döntésben való részvétel és a felhatalmazás a hagyományos vezető központú rendszerekénél nagyobb mértékű munkavállalói elkötelezettséget generál, a rendszer még mindig nem önműködő, öntanuló.

3. Biztonsági kultúra

A szervezetek biztonsági rendszere, akár a vezetői, akár az emberi erőforrás alapú megközelítést alkalmazzák, tele van lyukakkal, biztonsági kockázatokkal. A szervezeti biztonság szövetén ugyanis hasadások keletkeznek akkor: amikor egy biztonságot fenyegető helyzet észlelése, és/vagy értékelése nem megfelelő; ha nincsenek, vagy nem megfelelőek a kezelésére vonatkozó szabályzatok; amennyiben a szervezet tagjai nem ismerik azokat; abban az esetben is, amikor az alkalmazottak (vagy akár a vezető) nem képesek, vagy nem hajlandóak a veszélyt – még a veszhelyzet felismerése után, a rá vonatkozó protokollok ismeretében sem – elhárítani.

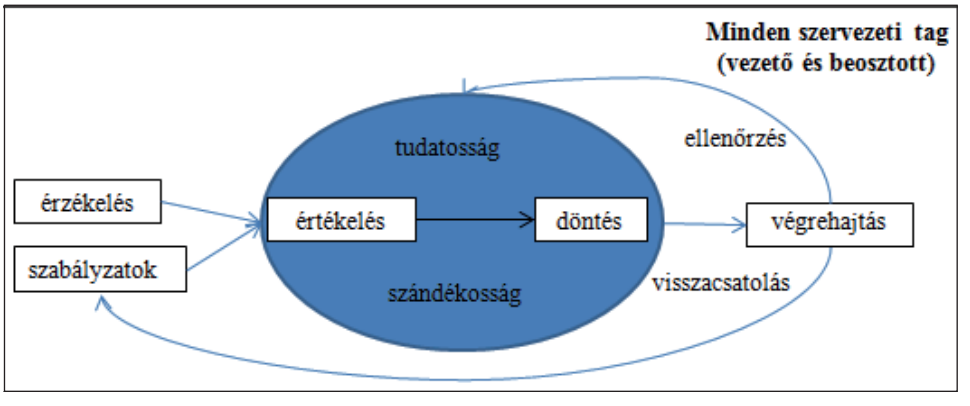
Ugyan minél több biztonsági szintet helyezünk egymásra, – minél többrétegű a szervezeti biztonság szövete – annál kevésbé valószínű, hogy a hasadások (hiányosságok) ugyanarra a területre esnek, a fenyegetettség lehetősége azonban továbbra is fennáll. Nem elég tehát a szervezet biztonságot technikai eszközökkel biztosítani, és az is kevés, ha csupán a vezető az, aki tisztában van a szervezetre leselkedő külső és belső fenyegetésekkel. Fontos, hogy a szervezet minden tagja tudatosan keresse, és felismerje a szervezeti biztonságot fenyegető helyzeteket, és

elkötelezettek legyenek azok megoldására. Ez a megközelítés jól működik más területeken is, pl. a környezettudatos vállalatirányításnál, ahol empirikus kutatások alapján még gazdasági megtérülést is hozhat (Tóth, 2002; 2006). A cél tehát egy olyan szerezeti megoldás kialakítása, melyben a szervezeti biztonság biztosítása a munkavállaló második természetévé válik (Hinson, 2009).

Amennyiben azonban olyan rendszerben gondolkodunk, mely a szervezeti tagoktól változást, a biztonsági rendszertől pedig a változás generálását várja el, tovább kell lépnünk a funkcionális elméletekről a radikális humanista megközelítések irányába (Burrel, Morgan, 1979). A radikális humanista elméletek szerint a szervezeti valóság, és folyamatok nem objektív, a vizsgálótól, illetve a szervezeti tagoktól függetlenül létező entitás, hanem a tagok által szubjektív módon érzékelt olvasatok halmaza. Amellett, hogy elfogadják, hogy nem létezik általános érvényű, mérhető valóság, törekszenek arra, hogy a helyzet, – jelen esetben a szervezet biztonsági állapota – folyamatosan javuljon, fejlődjön. A cél tehát nem egy részletekbe menő szabályozás és ellenőrzés kidolgozása, hanem egy olyan rendszer megalkotása, mely integráns módon képes kezelni az individuális és szituatív különbségeket, miközben arra sarkallja a szervezeti tagokat, hogy folyamatosan törekedjenek egy optimális, biztonságosabb szervezet létrehozására (Sharpanskykh, 2012). Éppen ezért, a szervezeti biztonság kérdéskörére kézenfekvő megoldásként adódott a szervezeti kultúra, mint bennfoglaló elem átalakítása, a biztonsági kultúra kialakítása (EU Comission, 2004). A szervezeti kultúra nem más, mint a szervezet tagjainak közös gondolkodása, amit a szervezeti problémák együttes megoldása során fejleszt ki (Heidrich, 2001; Rudolf, 2014; Bodor, 2003). A szervezet személyisége, mely befolyásolja az észlelést, az értékelést és a cselekvést is a szervezet szintjén éppen annyira, mint a szervezeti tagok és csoportok szintjén. A biztonsági kultúra szervezeti biztonság felfogása szerint tehát egy hatékony és hatásos szervezeti biztonsági rendszer akkor hozható létre, ha a személyes (értékek, attitűdök, hiedelmek, észlelés és felfogó készség) és a viselkedési tényezők (megértés, bizalom, elkötelezettség, motiváció/szándék és az éberség) egyszerre irányulnak a szervezeti biztonság megteremetésére, megtartására (McNamara, 2006). A biztonsági kultúrának tehát szükséges eleme tehát a tudás és kompetenciák mellett a tudatosság és a szándékosság. A biztonsági tudatosság nem más, mint az egyének veszélyérzete, mely nem csupán a személyes, de a szervezeti biztonságot fenyegető tényezőkre is kiterjed. A veszélyérzet hiánya az egyes viselkedési formák, cselekvések biztonsági kockázatának fel nem ismerését eredményez(-het)i, amely az üzleti cél és a rendeltetésszerű üzletmenet sérüléséhez vezethet. Elengedhetetlen tehát annak felismerése, hogy a biztonsági követelmények elfogadása a veszélyérzeten alapul (Szikora, 2012). A tudatosság azonban egyszerre vonatkozik a biztonsági események felismerésére, a szabályoknak és elvárásoknak ismeretére és a biztonsági események kezelésére. A szervezeti tagok tudatosság, a szabályok, eljárások ismerete nélkül sem megfelelő módon érzékelni, sem értékelni nem tudják a kialakuló helyzetet, ez által döntéseik, és az azokat követő

viselkedésük sem lehet biztonsági szempontból optimális. A tudatosság mellett a biztonsági kultúra másik alappillére a szándékosság. A biztonsági tudatosság ösztönösen biztonságosabb szervezeti magatartáshoz vezet, hiszen kizárja a biztonság kockázatot eredményező viselkedések szándékos előfordulását (Schneider, 2002), ami főleg ismétlődő, előre látható, tervezhető helyzetekben nagy segítség. Ugyanakkor a váratlan, nem programozott döntési helyzetekben a tudatosság mellett, szándékosságra is szükség van. A szervezeti biztonság esetében a szándékosság nem más, mint a szervezet biztonságáért való felelősségvállalás, biztonsági szempontból erkölcsös (helyes) döntések tudatos meghozatala és kivitelezése, ami pont azokban a helyzetekben szolgálja a szervezeti biztonságot, amikor nincsenek egyértelmű előírások, szabályok a krízis kezelésére vonatkozóan és a szervezeti tagoknak maguknak kell a felmerült problémára megoldást találniuk. Amennyiben a szervezeti tagok célja egy biztonságos szervezet megteremtése és fenntartása, döntéseiknél mindig a szervezeti normák által támogatott, a szervezeti erkölcs szerinti helyes viselkedési alternatívát fogják választani, még akkor is, ha az adott helyzetre nem vonatkozik külön előírás vagy szervezeti irányelv.

3. ábra: A szervezeti biztonság biztonsági kultúra szempontú megközelítése
Graph 3: Safety culture approach of organisational safety



Amikor a szervezeti tagok tudatosan és szándékosan biztonságos döntéseket hoznak a szervezeti kultúra biztonsági kultúrává válik, melyben minden szervezeti tagnak egyetemleges a felelőssége a biztonság fenntartása. Ennek megfelelően biztonsági kultúra az a kultúra, amelyben a szervezeti tagok ismerik feladat- és hatáskörüket, valamint kötelezettségeiket és tudatosan és szándékosan döntenek mind egyéni, mind pedig csoportos szinten a szervezeti biztonságot megszilárdító viselkedés mellett. Nincs tehát szükség vezetői beavatkozásra a biztonsági intézkedések betartatásához, hanem a szervezet minden tagja saját magát motiválja és kontrollálja, mi több, folyamatos visszajelzésekkel segíti társait is a helyes viselkedés kialakításában. A biztonsági kultúra logikai modelljét a 3. ábra tartalmazza.

A biztonsági kultúra hátránya pont lényegéből, kultúra voltából fakad. Nem, vagy csak igen nehezen mérhető a szervezeti tagok illeszkedése, mi több, mivel számos tacit és explicit elemet tartalmaz, elsajátítása összetett, hosszú folyamat (Tóth-Bordásné, Bencsik, 2012). Emellett kialakulása erőteljes függvénye a bennfoglaló vállalat, régió és ország kultúrájának, társadalmi berendezkedésének. Beágyazott rendszerként tehát sohasem létezik a környező kultúráktól függetlenül. Mint minden kultúra, igen nehezen módosítható, változtatható, és így mindaz, ami az aktuális piaci, gazdasági, társadalmi, politikai és technológiai környezetben versenyelőny, az hosszabb távon az innováció és az adaptivitás kerékkötőjévé válhat.

4. Összefoglalás, következtetések

A szervezeti biztonság problémakörét az idők folyamán sokan és sokféleképpen igyekeztek megoldani. A korai elméletek a vezetőkre, illetve az általuk működtetett elméletekre helyezték a hangsúlyt. A biztonsági kultúra megközelítés ezzel szemben a rendszer holisztikus jellegét hangsúlyozva a szervezeti tagok szerepére hívja fel a figyelmet. Azonban, mint ahogyan a korábbi elméletek esetében is, a biztonsági kultúra megközelítés hatékony működéséhez is számos premisszának kell teljesülnie. A megengedő nemzeti és szervezeti kultúra mellett szükség van a szervezeti tagok szándékos és tudatos akcióira is. A biztonsági kultúra megközelítés tehát nem kínálhat megoldást minden szervezet biztonsági problémáira, csupán egy, a korábbiaktól eltérő megközelítés, mely a strukturális elemek mellett a szervezet puha elemeit is integránsan kezeli.

FELHASZNÁLT IRODALOM

Bodor, M. (2003): Erős szervezeti kultúra titka. IQ Consulting Szervezetfejlesztő, és tanácsadó Kft.

Booz, Allen, Hamilton (2005): Convergence of Enterprise Security Organizations. ASIS, ISSA.

Burrel, G., Morgan, G. (1979): Sociological Paradigms and Organisational Analysis, ASHGATE.

Csiszárik-Kocsir, Á.,Fodor, M. (2013): Mennyire befolyásolták a makrogazdasági mutatószámok a költségvetési helyzetképet a válság előtt és után? – eredmények a Visegrádi négyek országcsoport adatai alapján, Vállalkozásfejlesztés a XXI. században III., Óbudai Egyetem, pp. 91.-101.

EU Commission (2004): On the implementation of the Preparatory Action on the enhancement of the European industrial potential in the field of Security research.. Commission Communication.

Heidrich, B. (2001): Szervezeti kultúra és interkulturális menedzsment. Human Telex Consulting Kft.

Hinson, G (2009): The True Value of Information Security Awareness. IsecT Publication.

Keszthelyi, A. (2014): Paradigmaváltás – biztonság – emberi tényező, VIKEK, közlés alatt

Keszthelyi, A. (2013): Netháborúk kora, In: Juhász et al. (szerk.), Új kihívások a tudományban és az oktatásban Selye János Egyetem, Révkomárom, pp: 149-170.

Kovács, N., Szabó, D.R., Páthy, Á., Tóth, P. (2014): Főbb kockázat-típusok és ezek megítélése a hazai építőiparban, InThe Publications of the MultiScience XXVIII. microCAD International Multidisciplinary Scientific Conference. Miskolc: University of Miskolc, 2014. Paper F9. 8 o.

McNamara, C. (2006): Organizational culture. www.managementhelp.org

Rudolph, K., Warshawsky, G, Numkin, L. (2014): Security Awareness, In Bosworth and Kabay Whyne Eds. Computer Security Handbook. John Wiley and Sons, Hoboken.

Schneider, W. E. (2002): Why Good Management Ideas Fail – The Neglected Power of Organizational culture. The CEO Refresher Archives.

Szigeti, C. (2015): Az ökolábnyom és egyéb fenntarthatósági indikátorok mérési tartományának értelmezése Journal of Central European Green Innovation 3 (1) pp. 49-68.

Szikora, P. (2012): A racionalitás szerepe a vállalkozások fejlesztésében. In: Nagy Imre Zoltán (szerk.) Vállalkozásfejlesztés a XXI. században II.. Budapest: Óbudai Egyetem, pp. 179-200.

Tóth-Bordásné Marosi, I., Bencsik, A. (2012): Szervezeti magatartás avagy a bizalom ereje. Universitas-Győr Nonprofit Kft.

Kontogiannis, T. (2010): A contemporary view of organizational safety: variability and interactions of organizational processes. Cognition Techology and Work 12, pp. 231–249

Reisinger Adrienn (2012): A társadalmi részvétel a helyi fejlesztési politikában Magyarországon – fókuszban a civil/nonprofit szervezetek. Civil Szemle, 1. pp. 23–44.

Reisinger Adrienn (2013): Social responsibility: the case of citizens and civil/nonprofit organisations. Tér Gazdaság Ember, 3. pp. 75–87.

Sharpanskykh, A. (2012): A Systemic Approach to Organizational Safety Modeling and Analysis. International Journal of Information Systems for Crisis Response and Management, pp.42-56

Szabó, D.R., Kovács, N., Páthy, Á., Tóth, P. (2014): Risks in the Hungarian construction industry: Interpretations, evaluations and patterns In: Human Capital without Borders; Knowledge and Learning for Quality of Life: Proceedings of the Management, Knowledge and Learning International Conference 2014., ToKnowPress, 2014. pp. 597–603.

Timár, I.Z., Borzán, A. (2013): A bankok és biztosítók együttműködése napjainkban. In: Beszteri Béla (szerk.). A felfedező tudomány. Széchenyi István Egyetem Kautz Gyula Gazdaságtudományi Kar, Győr, Paper 34. 16 p

Tóth Gergely (et. al.) (2002-2006): Ablakon bedobott pénz–Magyarországi szervezetek esettanulmányai környezeti és gazdasági megtakarítást egyszerre hozó intézkedésekről, KÖVET, Budapest. (I. – V. kötet)

Varga, J.(2014): Üzleti agilitás és versenyképesség a XXI. század vállalkozásainál. Vállalkozásfejlesztés a XXI. században IV. Óbudai Egyetem, Budapest. pp. 189-205.