Stressz, opportunizmus és bizalom a szervezeti információs és kommunikációs technológiabiztonság tükrében

A globalizáció és a technológiai fejlődés következtében a digitális infrastruktúra amellett, hogy jelentős hatással van a szervezetek teljesítőképességére, növeli azok sebezhetőségét. A kutatás célja annak feltárása, hogy az információbiztonsággal kapcsolatos kockázatok hogyan értelmezhetők, illetve mérsékelhetők, kezelhetők a tranzakciós költség elméletet meghatározó opportunizmus, illetve a tranzakciós elmélet keretrendszerében értelmezhető stressz, valamint technostressz megközelítést alkalmazva, továbbá ezek hatásainak egyfajta csökkentésére irányuló bizalom szerepét elemezve. A tanulmány rámutat, hogy az IKT-eszközök (információs és kommunikációs technológia) használata, illetve azok folyamatos fejlődése a munkavállalók részéről nem csak végeláthatatlan tanulást igényel, hanem ebből fakadóan nyomást helyez az egyénre, állandó versenyhelyzetet teremtve, melynek következtében kontraproduktivitás jelenik meg, azaz csökken a biztonságtudatosságuk. Ebből következően nemcsak az IKT-eszközök alkalmazása, hanem az információbiztonsági intézkedések és folyamatok tervezése és implementálása során is elengedhetetlen az információs aszimmetria és az opportunista viselkedés csökkentése, melynek révén várhatóan növekszik a bizalom és a szervezeti reziliencia, teljesítmény.

Kulcsszavak: *információbiztonság, tranzakciós elmélet, tranzakciós költség elmélet, opportunizmus, stressz, bizalom*

Szerzői információ

Bak Gerda, Óbudai Egyetem, Biztonságtudományi Doktori Iskola
https:// orcid.org/0000-0001-5912-3716

Kelemen-Erdős Anikó, Budapesti Műszaki és Gazdaságtudományi Egyetem, Gazdaság- és Társadalomtudományi Kar
https://orcid.org/0000-0001-7202-5870

Így hivatkozzon erre a cikkre:

Bak Gerda, Kelemen-Erdős Anikó. „Stressz, opportunizmus és bizalom a szervezeti információs és kommunikációs technológiabiztonság tükrében”.
Információs Társadalom XXIII, 3. szám (2023): 9–26.
https://dx.doi.org/10.22503/inftars.XXIII.2023.3.1

Stress, Opportunism and Trust in the Context of Organisational Information and Communication Technology Security

As a result of globalization and technological advances, digital infrastructure not only has a significant impact on the performance of organizations but also increases their vulnerability. The aim of this research is to explore how information security risks can be managed using a transaction cost theory and transactional theory framework. Accordingly, opportunism, stress, and technostress are treated as negative influencing factors but the role of trust may mitigate some of these effects. The study shows that the use and development of information and communication technology (ICT) tools not only requires continuous learning on the part of employees but also puts pressure on individuals, creating competitive situations that may be counterproductive and reduce security awareness. Consequently, it is essential to reduce information asymmetry and opportunistic behaviour when using ICT tools, and to design and implement information security measures and processes that can increase the trust, resilience and performance of organizations.

Keywords: *information security, transactional theory, transaction cost theory, opportunism, stress, trust*

Bevezetés

A digitális gazdaság egyik fontos elemét az adatok és az információs rendszerek alkotják, amelyek elengedhetetlenek mind az egyének, mind a szervezetek számára. A digitális eszközökre való nagy fokú támaszkodás, valamint a fokozódó összekapcsoltság miatt az adatok és információk biztonsága kihívást jelent. Mivel a fizikai oldalon a technológiai biztonsági pontokat, ellenőrzéseket nehéz kijátszani, a támadók gyakran igyekeznek kihasználni a virtuális tér és az információs rendszerek felhasználóinak gyengepontjait a felhasználók cselekedeteinek, magatartásának manipulálásával. A támadók megtévesztik és meggyőzik az egyéneket, hogy hozzáférést biztosítsanak az informatikai erőforrásokhoz vagy a szükséges információkhoz, amelyekhez egyébként nehéz hozzáférni (Dalal et al. 2022). Még a technikai ellenőrzések kudarca is gyakran összefügg az emberi hibákkal és gondatlansággal (Gratian et al. 2018), illetve az opportunizmussal (Lowry et al. 2019). A jelentések szerint a felhasználók, alkalmazottak könnyű célpontjai a kiberbűnözőknek (Gratian et al. 2018; Chatterjee 2021). Számos kibertámadás abból ered, hogy az egyén fogékony a különböző kibertámadási technikákra (Im és Baskerville 2005).

Az egyén stressztűrő, és azt leküzdő képességének mértéke az egyik fontos személyiségjegy, amely hozzájárul a munkavállalók kívánt és tényleges viselkedése közötti eltéréshez az információs rendszerek használata során (D'Arcy, Herath és Shoss 2014; Hwang, Kim és Rebman 2021; Trang és Nastjuk 2021). A jelentősebb stresszkeltő növeli a munkavállalóra nehezedő általános jellegű megterhelést. Ilyen nyomást eredményező tényező lehet például a technológia használata miatti stressz, a munkakörből adódó feladatok, határidők, a munka és a család közötti konfliktus, a személy–munkahely összeférhetetlenség és a szervezeti politika. Számos tanulmány vizsgálta a stressz és az IKT-eszközök használata közötti összefüggést. A kutatók azonban a vizsgált mintától függően különböző, olykor akár eltérő összefüggést figyeltek meg a stressz és az IKT-eszközök használatához kapcsolódó magatartás között (Hauk, Göritz és Krumm 2019; Spiess et al. 2021; Trang és Nastjuk 2021), ennek alapján kijelenthető, hogy az IKT-eszközök használata a felhasználók körében mint stresszforrás jelentkezik, azonban annak mértéke és fajtája eltérő. Ezt támasztja alá Qi (2019) középiskolás diákok körében folytatott kutatása is, mely szerint a diákok mobilkészülék-használata nem vezet technostresszhez, viszont segít a tanulmányi teljesítmény javításában, illetve mobil eszköz használatához köthető jártasság és az abból fakadó magabiztosság mértéke jelentősen befolyásolja a technostresszt. Ennek kapcsán megemlítendő, hogy több kutatás (Suharti és Susanto 2014; Tarafdar, Pullins és Ragu-Nathan 2015) is vizsgálta a technostressz és a teljesítmény kapcsolatát, melyek rámutattak, hogy a stressz mértéke, illetve az egyéni jellemzők növelhetik, illetve ronthatják is a munkavállalók teljesítményét. Ninaus és munkatársai (2015) az IKT-val kapcsolatos stresszorokat és a munkahelyi előnyöket vizsgálták a munkavállalók körében, és megerősítették azt a feltételezést, hogy az IKT-kat egyszerre érzékelik előnyösnek és hátrányosnak, ami alátámasztja azt az elképzelést, hogy az IKT kétélű kard (Diaz et al. 2012; Reinke és Ohly 2021). A legygyakrabban előforduló stresszfaktorok kategóriái az állandó elérhetőség, a kapcsolati nyomás, a belső elérhetőségi kötelezettség és a megnövekedett munkaterhelés,

míg a jobb kommunikáció, az azonnali elérhetőség és a nagyobb rugalmasság az előnyöket jelentik (Ninaus et al. 2015).

Nyilvánvaló, hogy a folyamatos rendelkezésre állás egyszerre tekinthető stresszornak és előnynek is, melyek hatását a mobil eszközök és a mobilinternet csak felerősít. Meg kell jegyezni, hogy míg korábbi tanulmányok (Ayyagari, Grover és Purvis 2011; Diaz et al. 2012) azt mutatják, hogy a munkával kapcsolatos IKT-használat a munkaidőn kívüli időszakban összefügg a munka és a magánélet felborulásával és az ebből eredő konfliktussal, Ninaus és munkatársainak (2015) tanulmánya arra hívja fel a figyelmet, hogy az IKT-eszközök az életterületek közötti egyre inkább elmosódó határok kapcsán lehetőséget teremthetnek a munka és a magánélet jobb összehangolására a nagyobb rugalmasság révén. Ezek az előnyök pedig hozzájárulnak a munkavállalók munkahatékonyságának javításához, ami pedig – a stresszhatás ellenére – hozzájárulhat a munkavállalók jólétéhez. A jelen tanulmány célja a digitálisinfrastruktúra-használat kapcsán fellépő stressz, illetve az ezzel összefüggő információbiztonsági kérdések, illetve a szervezet kitettségének elemzése. A kutatási kérdések megválaszolásához ez a tanulmány a tranzakciós költség elmélet szerinti opportunizmusra, a stressz tranzakciós modelljére, valamint ezek hatásainak ellensúlyozásaként a digitális eszközökhöz kapcsolódó bizalom tényezőjére támaszkodik. Lazarus és Folkman (1984) tranzakciósstressz-modelljének alaptétele, hogy a stressz pszichológiai értékelési folyamatokból ered, amelyek során az egyének úgy érzik, hogy erőforrásaik nem elegendőek a stresszhatások kezeléséhez. A modell széles körben elismert, és bizonyítottan alkalmas a pszichológiai és viselkedési válaszok magyarázatára (Karimikia, Singh és Joseph 2020; Schmidt, Frank és Gimpel 2021; Venz és Shoshan 2021).

Kutatásunkat a következő három kutatási kérdés vezérli:

- K1. A digitális eszközökbe vetett bizalom hogyan befolyásolja az egyéneken keresztül a szervezet információbiztonságát?
- K2. Hogyan csökkenthető a kapcsolatok bizonytalanságával jellemezhető opportunista magatartás negatív hatása, illetve információbiztonsági kockázata?
- K3. A digitális/okoseszközök használata során felmerülő technostressz hogyan hat az egyén szervezeti, illetve információbiztonsági magatartására?

A tanulmány további részeit a következők szerint építettük fel. Először is, a tanulmány elméleti megalapozását az opportunizmus és a stresszelmélet áttekintésével biztosítjuk szervezeti kontextusban. Erre építve bemutatjuk a tranzakciós költség elméletet és a tranzakciós elméletet mint fogalmi keretet. Az utolsó szakasz az alapozó kutatás eredményeként felvázolt modellt, a tanulmány megállapításait tárgyalja, összefoglalva azokat vezetői implikációkat adva, és felvázolva a tanulmány korlátait, amelyek a jövőbeli kutatás irányaira mutatnak rá.

Szakirodalmi áttekintés

A kibertámadásoknak számos különböző negatív következménye lehet a vállalatra, köztük anyagi jellegű veszteségek, így például csökkenhet a vállalat piaci értéke, de

akár a nem pénzbeli veszteségek is jelentősek lehetnek, mert csökkenhet a bizalom, negatív vásárlói vélemény alakulhat ki, illetve sérülhet a hírnév, mely további anyagi veszteségekhez vezet (Furnell et al. 2020). A munkavállalók viselkedését széles körben a szervezet biztonsági rendszerére jelentett legnagyobb fenyegetésnek tekintik (Crossler et al. 2013; Hooper és Blunt 2019). Az alkalmazottak hozzáféréssel rendelkeznek a belső szervezeti folyamatokhoz, ami lehetővé teheti a hekkerek számára a gyengepontok kihasználását. Az információbiztonsági fenyegetések csökkentésének egyik legfontosabb eszköze az információbiztonsági politikák kialakítása és végrehajtása, amelyek célja a munkavállalók biztonsági magatartásának szabályozása. Az alkalmazottak tényleges biztonsági magatartása azonban gyakran eltér a szabályzatban előírtaktól (Siponen, Mahmood és Pahnila 2014; Hooper és Blunt 2019), ami jelentős kockázatot jelent a szervezeti biztonságra nézve. A mögöttes tényezők feltárására a tranzakciós költség elmélet és a tranzakciós elmélet keretrendszerét alkalmazzuk.

A tranzakciós költség elmélet

A tranzakciós költség elmélet alapjait Williamson (1975) határozta meg. Az elmélet azokra a szerződéskötést megelőző ex ante, és az azt követő ex post jellegű költségekre vonatkozik (Williamson 1975), amelyek befolyásolhatják a szervezeti folyamatok hatékonyságát és a szervezet teljesítményét (Bellotti da Fonseca, Vanalle és Camarotto 2018).

A tranzakciós költségek lehetnek ex ante és ex post költségek egyaránt, melyek csökkentésére a szervezet törekszik (Williamson 1975). Ezek körébe tartoznak az IKT működésével összefüggő költségek, valamint a szervezeti kapcsolatok, hálózatok menedzsmentje, melyek meghatározhatják egy vállalkozás hatékonyságát, piaci teljesítményét. Az, hogy ezeknek a költségeknek a hatása mennyire jelentős, a tényezők komplexitásától, a hálózatokhoz, illetve egyéb kapcsolatokhoz való kötődésétől, valamint a tranzakció intenzitásától, a teljesítménymérés nehézségeitől – ideértve a jelenség, illetve szituáció előfordulásának, alkalmazásának a gyakoriságát, tartósságát – függ (Gottschalk és Solli-Sæther 2005).

A tranzakciós költségek elmélete szerint az érintettek kapcsolatrendszerét áthatja az opportunizmus, mely alapvetően a korlátozott racionalitással összefüggő, kiszámíthatatlan magatartásra, akár a szereplők szándékos félrevezetésre vonatkozik (Pathak, Ashok és Tan 2020; Hill 1990). Az egyéni érdek előtérbe helyezése, akár mások érdekeinek megsértésével (Williamson 1975).

A komplex társadalmi–gazdasági rendszerek mint keretrendszer, illetve az ebben működő entitások interdependenciája a bizalom szerepét helyezik előtérbe. A bizalom ellensúlyozhatja az opportunizmus negatív hatásait (Schmidt és Wagner 2019), azonban nem feltétlenül jelentős mértékben (Lehota et al. 2020). Mi több, növelheti a szervezet és az egyén sebezhetőségét (Valociková 2022), egyfajta kockázatvállalási hajlandóságon keresztül, mely az opportunista viselkedés ellenpontjaként a hitet fejezi ki abban, hogy adott, jellemzően valamilyen negatív hatással járó bizonytalan magatartás nem következik be (Kováts 2019).

Az információbiztonság tekintetében különösen jelentős az egyéni, illetve a szervezeti magatartáshoz kapcsolódó bizonytalanság csökkentése annak érdekében, hogy a biztonsági rendszerek sebezhetőségét mérsékelhessük. Miután az információbiztonságot az opportunista viselkedés tovább veszélyeztetheti (Flowerday és von Solms 2006), lényeges a tranzakciós költség elmélettel megalapozott opportunizmus mint jelenség vizsgálata. Még akkor is, ha a technológiai fejlődés, így például a tranzakciókkal kapcsolatos információt rögzítő blockchain visszaszoríthatja az opportunista viselkedést (Rindfleisch 2019).

A bizalomépítés, illetve a bizalom megőrzése hozzájárulhatnak az információbiztonság fokozásához, illetve korlátozhatják a biztonságot veszélyeztető opportunista viselkedést (Flowerday és von Solms 2006). Amellett, hogy a bizalom egyfajta fogódzót biztosít, mások cselekedeteinek, képességeinek, kommunikációjának elfogadása révén.

A stressz és a bizonytalanság csökkenti az információbiztonságot, illetve a szervezetek hatékonyságát (Chiu et al. 2018). Ugyanakkor a bizalom, ha közvetlenül nem is járul hozzá az opportunizmus visszaszorításához, az attól való félelemérzetet csökkentheti (Ferdousi 2020).

Tranzakciós elmélet

A digitalizáció számos munkakört formált át, szüntetett meg vagy járult hozzá létrejöttéhez (Forrester Research 2019). Ennek következtében a digitális képességek, készségek jelentősége felértékelődött, azonban a munkavállalók közel fele nem, vagy nem megfelelő szinten rendelkezik ezekkel (World Economic Forum 2018). Digitális készségek hiányában a munkáltatók hátráltatják az innovációt és a vállalati növekedést, hiszen a digitalizáció nagyban függ a munkavállalók képességeitől és készségeitől (Vigren, Kadefors és Eriksson 2022). A digitális átalakulás, az IKT-eszközök azonban hatással vannak a munkavállalók pszichoszociális munkakörnyezetére, ami lehet negatív (túlterheltség, tisztázatlan vagy nem egyértelmű előírások, hiányos ismeretek) vagy akár pozitív (jobb munkaszervezés, könnyebb munkavégzés, digitális támogatás) (Graveling 2020; Jenei és Módosné Szalai 2022). Az új technológia munkavégzéshez történő használatát már az 1980-as években stresszként azonosították, a jelenséget pedig technostresszként határozták meg (Brod 1982). Azóta számos tanulmány vizsgálta és megerősítette, hogy az IKT-eszközök mind a munkavállalók egészségére, mind a munkahelyi stresszre nagy hatással vannak (Tarafdar, Cooper és Stich 2017; Ninaus, Diehl és Terlutter 2021).

A tranzakciós elméleten alapuló IKT-kutatások egy speciális területre, a stressz tranzakciós elméletére koncentrálnak (Kamal et al. 2020; Hauk, Göritz és Krumm 2019; Hosking és Livingstone 2022). Az IKT-eszközhasználat egyénre gyakorolt hatásrendszerét, az informatikai eszközhasználat okozta stresszt emelik ki. A legújabb kutatások hangsúlyozzák a stressz és a biztonsági magatartás közötti kapcsolat vizsgálatának fontosságát. Pham és munkatársai (2016) arra a következtetésre jutottak, hogy a biztonsági megfelelés fokozható a stresszes biztonsági követelmények minimalizálásával.

Technostressz

A technológia és a munkavégzés módjának fejlődése, változása megköveteli a munkavállalóktól a szinte állandó elérhetőséget az e-mail és a telefon gyakori használatával. Ez a munkaidőn túli munkavégzéshez vezet, ami stresszt vált ki az egyénből. Ez az egyik fő oka a munkával kapcsolatos elégedetlenségnek, ami negatív érzéseket vált ki a technológiával szemben (Weil és Rosen 1997; La Torre et al. 2019). A munkahelyi IKT-val kapcsolatos technológiaalapú stresszt kiváltó tényezőket, technostresszorokat a következőképpen osztályozhatjuk: technotúlterhelés (nyomás, hogy sokkal gyorsabban és hosszabb munkaidőben kell dolgozni), technoinvázió (állandó összeköttetés, ami a szakmai és a családi élet közötti határ elmosódását okozza), technokomplexitás (az IKT-val kapcsolatos nem megfelelő tudás és készségek érzése, valamint a tanulási és fejlődési kényszer), technoszorongás (az új IKT-fejlesztések vagy a munkatársak tudása miatti munkahelyi bizonytalanság) és technobizonytalanság (a gyakran változó IKT-vel való lépéstartás nehézsége) (Tarafdar et al. 2014). Reicher (2018) kutatásában rávilágított, hogy az Y generáció tagjai erősen függenek az internetelérétől, az interneten keresztül elérhető alkalmazásoktól, melyeket akár naponta többször is ellenőriznek. Ez a fajta viselkedés tovább fokozza a technoterhelést a fiatal munkavállalók körében (Reicher 2018).

A megnövekedett munkahelyi követelményeket eredményező technológiai változások nyomást gyakorolnak az egyénre, amely negatív hatással van az egyén IKT-használattal kapcsolatos megítélésére, mivel a versenyben való helytállás érdekében a folyamatos tanulásra, fejlődésre kényszerülnek (Ayyagari, Grover és Purvis 2011; La Torre et al. 2019). Ugyanakkor a feladatok elvégzése érdekében a munkavállalók folyamatosan nyomás alatt vannak, illetve rákényszerülnek, hogy új technológiákat alkalmazzanak, így verseny és a technikai bizonytalanság érzése alakul ki. Továbbá a stressz hatására az egyének gyakrabban követnek el olyan hibákat munkavégzés közben, melyek következményeként a vállalat információs infrastruktúrája könnyen hozzáférhetővé válik a külső támadók számára (Mészáros és Tick 2022). Azok az egyének, akik a munkahelyük elvesztésétől tartanak, illetve folyamatos teljesítési kényszer alatt állnak, nagyobb szorongást és frusztrációt élnek át. A technostressznek számos megfigyelt hatása van, mint például a szakmai hatékonyság csökkenése, alacsony teljesítmény, több konfliktus, valamint a munkavállalók nagyobb fluktuációja (Tarafdar, Pullins és Ragu-Nathan 2015; Pirkkalainen et al. 2019). Ez azt jelenti, hogy szükség van a technostressz káros hatásainak tudatosítására és hatékony intézkedésekre, valamint a technostressz kezelésére irányuló kívánt gyakorlatok és stratégiák végrehajtására. A technológia okozta szorongás mellett gyakran kötődés alakul ki az egyén és az IKT-eszközök között (Rab és Török 2020).

Bizalom

Az algoritmusok és a digitális eszközök iránt egyes felhasználókban kialakul egy bizonyos szintű bizalom az objektivitás, pontosság, automatizáltság és az emberi beavatkozás nélküli működése miatt (Kaplan és Haenlein 2020). Az interperszonális

bizalom az egyik leginkább elterjedt definíciója „olyan pszichológiai állapot, amely magában foglalja a sebezhetőség elfogadásának szándékát, amely a másik fél szándékaival vagy viselkedésével kapcsolatos pozitív várakozásokon alapul" (Rousseau et al. 1998, 395). Az interperszonális bizalomhoz hasonlóan a technológiába vetett bizalom megfogalmazható úgy, mint az a meggyőződés, hogy az adott digitális technológiai eszköz rendelkezik bizonyos kívánatos vagy kedvező tulajdonságokkal, amelyek kielégítik az emberek elvárásait (Gefen, Benbasat és Pavlou 2014).

A kezdeti bizalomkutatásokat követően a bizalom fogalmát kiterjesztették a technológia kontextusára (Benbasat és Wang 2005), melynek során a kutatók felismerték, hogy az emberek alapvetően bíznak a technológiában (Lankton, McKnight és Tripp 2015). Ebben a kontextusban azt vizsgálták, hogy a felhasználók bizalma miként változik a technológia első használata és a további használata során (Bhattacherjee és Lin 2017; McKnight, Liu és Pentland 2020), mely vizsgálat azt mutatja, hogy a negatív benyomások, hírek csökkentik az egyének bizalmi szintjét, pozitív események hatására pedig ennek növekedése figyelhető meg.

A kognitív bevonódás, abszorpció szerepe is kiemelhető, amit Guo és Ro (2008) új technológia használata esetén a felhasználó bevonódásának és elkötelezettségének állapotaként definiált. A kognitív abszorpció alapja a kognitív elköteleződés (Webster és Ho 1997) és a flow elmélet (Csikszentmihalyi, Abuhamdeh és Nakamura 2014) fogalmára épül. A kognitív elkötelezettség inkább az ember–gép interakcióval és a szubjektív élménnyel foglalkozik, amelyet a felhasználó ebből merít (Webster és Ho 1997). A kognitív abszorpciós elméletet eredményesen alkalmazták a technológiával kapcsolatos területeken. Korábbi tanulmányok alátámasztották, hogy a kognitív abszorpció képes kiváltani a technológiai adaptációs viselkedést (Agarwal és Karahanna 2000; Tourinho és de Oliveira 2019). A technológiába vetett bizalom a pozitív technológiai tulajdonságoktól és a felhasználó-specifikus elvárásoktól (McKnight et al. 2011), illetve a technológia révén nyújtott szolgáltatásokkal való elégedettségtől függ (Johnson, Bardhi és Dunn 2008). A használat a bizalmi szint növekedéséhez, illetve akár szélsőséges helyzethez is vezethet, melynek során az egyén élete szorosan összefonódik a digitális világgal, a mesterségesen kialakított digitális identitás meghatározhatja énképét.

Az IKT vonatkozásában a bizalom a gép–ember interakciót tekintve az egyik kulcsfontosságú aspektus (Levitt 2015). Ez alól a tárgyak internete (Internet of Things – IoT) sem kivétel, hiszen a biztonság ebben az esetben is összefügg azzal, hogy a felhasználók mennyire képesek megbízni a környezetükben (Fortino et al. 2020). Minden rendszert az elektronikus informatikai rendszerek biztonságát szem előtt tartva, a fő biztonsági célokat teljesítve szükséges megtervezni a bizalmasság, a sértetlenség és a rendelkezésre állás mentén (confidentiality, integrity, availability, azaz a CIA-elv alapján) (Muha és Krasznay 2018).

A gépekhez kapcsolódó bizalom azt jelzi, hogy megbízható eszközökkel kell interakcióba lépni (Daubert, Wiesmaier és Kikiras 2015). Ez kihívást jelent az IoT-környezetben, mivel nem mindig lehetséges az eszközökkel szembeni bizalom kialakítása. Ráadásul minden entitás másképp értékelheti a bizalmat adott eszközzel szemben. Az IoT-egységek bizalma a felhasználók vagy szolgáltatások elvárt viselkedését jelzi. Bár az eszközökbe vetett bizalom a megbízható technológiával,

előírásokkal is kialakítható, azonban ez nagyobb kihívást jelent. Az eszközbizalom a szabványosított eljárások, a technológia és a paraméterek mentén alakítható ki (Vasilomanolakis et al. 2015).

A tárgyak internetével kapcsolatos egyik legfontosabb bizalmi kérdés, amelyet figyelembe kell venni, a heterogenitással kapcsolatos. A tárgyak internetének eszközei a fizikai világgal sok különböző objektumon keresztül lépnek kölcsönhatásba, amelyeknek csak egy interfészük van a kommunikációhoz. Az ezek közötti különbségek lehetnek az operációs rendszer, az I/O (input–output) csatorna, a csatlakoztathatóság és a teljesítmény, mely különbségek oka a használt hardverre vezethető vissza, amely eltérő tárolókapacitáshoz, számítási teljesítményhez és energiafogyasztáshoz vezet (Ahmed et al. 2019). Ezeknek a különbségeknek a kezelése nagy kihívás az IoT-környezetben. Ezt nehezíti az IoT-hez csatlakoztatott eszközök növekvő száma, melyek egyre több kommunikációt, tranzakciót és adatot eredményeznek (Sharma et al. 2020).

Továbbá a bizalmi követelmények teljesítése szorosan kapcsolódik a hozzáférés kérdéseihez, a hozzáférés-ellenőrzéshez és a személyazonosság-kezeléshez (Sicari et al. 2015). Ez kulcsfontosságú, mivel az IoT-környezetben különböző eszközök léteznek, amelyeknek fel kell dolgozniuk és közvetíteniük az adatokat a felhasználói igényeknek és jogoknak megfelelően.

A bizalom kialakulásának egyik eredményeként ugyanakkor amellett, hogy a felhasználó és az IKT-eszközök közötti kapcsolat rugalmasabbá, gördülékennyé válik, a rendszer sérülékenysége is növekedhet. Ilyen esetekben fordulhat elő, az úgynevezett „Mount Stupid" jelenség, mely a felhasználó érzékelt, nem megfelelő kompetenciákon alapuló tudására, és az ezzel együtt megnövekedett önbizalmára vonatkozik (El-Kafafi et al. 2022). Amennyiben a látszólagos tudás növeli a kliens önbizalmát a rendszer használatakor, gyakran jelentősen csökken a kiberbiztonsággal kapcsolatos óvatosság, mely egyéni és szervezeti problémákat egyaránt okozhat.

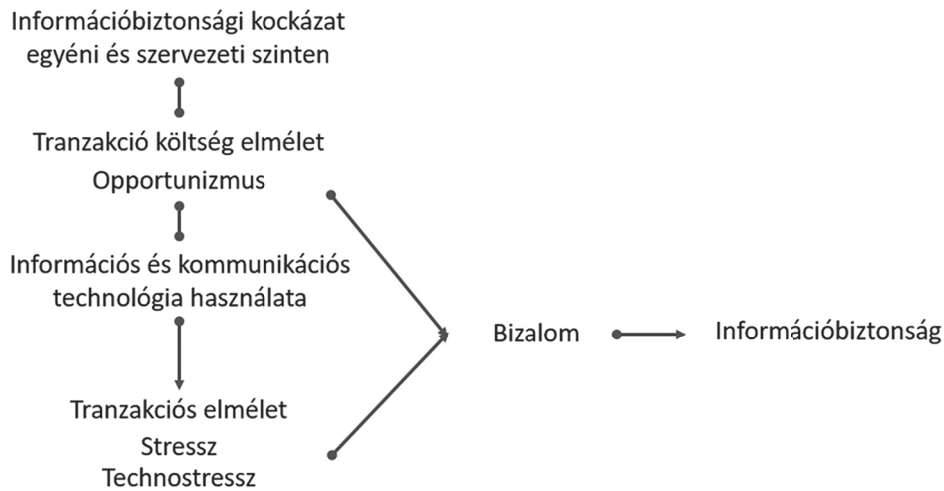
Diszkusszió

Bár számos tanulmány foglalkozott a kiberbiztonsággal kapcsolatos észlelt fenyegetettséggel, azaz az észlelt kockázatokkal, kevés kutatás vizsgálta a kiberbiztonságra való felkészültséget, mely hozzájárul a szervezeti rezilienciához. A kiberbiztonságot leegyszerűsítve technikailag úgy lehet értelmezni, mint a számítógépes biztonságot a hozzátartozó titkosítással (Hansen és Nissenbaum 2009). A kiberbiztonságra való észlelt felkészültség ugyanakkor túlmutat a technikai értelmezésen, mivel a kiberfenyegetések által kiváltott társadalmi hatások felismerését is tartalmazza (Nissenbaum 2005).

A kiberbiztonságra vonatkozó érzékelt felkészültséget különböző kognitív és pszichológiai tényezők befolyásolják. A múltbeli tapasztalatokat az észlelt biztonság kiemelten fontos és meghatározó tényezőjének tekintik, illetve a korábbi releváns tapasztalatok, különösen a számítógépes és internetes biztonságot érintő incidensek (kibercsalások, adathalászat áldozatává válás) összefüggést mutatnak az információbiztonsági fenyegetések észlelésével és az információbiztonság-tuda-

tos magatartással (Li et al. 2016; Bak és Kelemen-Erdős 2022). Egy közvetlen biztonsági incidens megtapasztalása negatív érzelmi állapotot, szorongást, stresszt okoz, ami csökkentheti az egyének kiberbiztonságba vetett hitét. Ezért a múltbeli tapasztalatok hatással vannak a fenyegetések súlyosságának és az észlelt fenyegetettségnek a mértékére.

A tanulmány főbb eredményeit az információbiztonsági kockázat, a tranzakciós költség elmélet, a tranzakciós elmélet, valamint a bizalom összefüggéseit az 1. ábrán szemléltetett modellben összegezzük. Az alapozó kutatás eredményeként épített modell alkalmas lehet hipotézisek alkotására, melyek további kutatások során tesztelhetők.



1. ábra: Az opportunizmus, a stressz és a bizalom szerepe az információbiztonság megítélésében (saját szerkesztés)

Az elemzés eredményeként a digitális eszközökbe vetett egyéni bizalom valamelyest csökkentheti a szervezetek információbiztonsági kitettségét, növelheti a rezilienciát (K1). A technológiába vetett bizalom alapja a kognitív abszorpció, amely meghatározza, hogy az egyén mennyire képes megbízni adott technológiában, melyet alapvetően befolyásolnak az egyén azzal kapcsolatos korábbi tapasztalatai, illetve az észlelt fenyegetettség mértéke (Johnson, Bardhi és Dunn 2008).

Az opportunista magatartás bizonytalanságot integrál a tranzakciókba, ezzel növelve az információbiztonsági kockázatot, melyet a bizalom csak részben ellensúlyozhat, hiszen ez önmagában kockázatvállalási hajlandóságot jelez (K2). Ugyanakkor a bizalomépítés, a vállalatok arculatának kialakítása, reputációja, a megbízhatóság megteremtése a biztonságérzetet, a bizalmat növelheti. Mindezek enyhíthetik az opportunizmus negatív hatásait, bár érdemes figyelembe venni a látszólagos tudás növekedésével kapcsolatos sérülékenységet is (Flowerday és von Solms 2006; Kováts 2019; Schmidt és Wagner 2019).

A társadalmi–gazdasági környezet, a szociális nyomás gyakorta stresszhelyzeteket eredményez, mely negatív hatással van az egyén pszichés állapotára. A technostressz erre a káros hatásra erősít rá azzal, hogy az IKT-infrastruktúra működésével, működtetésével összefüggő feszültséget kelt az egyénben. Ennek eredményeként az egyéni és a szervezeti reziliencia, teljesítmény is romolhat, az átélt stressz miatt opportunista magatartás, fluktuáció következhet be, mely alapvetően növeli az információbiztonsági kockázatot (K3). A technostressznek számos megfigyelt hatása van, mint például a szakmai hatékonyság csökkenése, alacsony teljesítmény, több konfliktus, valamint a munkavállalók fluktuációja (Tarafdar, Pullins és Ragu-Nathan 2015; Pirkkalainen et al. 2019).

Összegzés

Jelentős kihívást jelent az opportunista viselkedéssel és stresszel kapcsolatos kockázatok kezelése mind egyéni, mind szervezeti szinten, mert ezek a tényezők amellett, hogy sebezhetővé teszik a szervezetet és ezen belül az IKT-eszközök biztonságát, visszaélésre adnak lehetőséget, negatívan befolyásolhatják egy szervezet teljesítményét.

A tranzakciós költség elmélet keretet biztosít az egyéni és különösen a szervezeti kockázatok megértéséhez, mely hozzájárulhat a menedzsmentfolyamatok optimalizálásához. Az opportunizmus természetének megértése, kiszámíthatatlanságának, a bizonytalanság faktornak integrálása a folyamatokba, elősegítheti a szervezeti működés mélyebb megértését, menedzsmentjét. Ez ugyanakkor jelentős kihívást igényel, hiszen az opportunizmus mibenléte csak korlátozott hatásmechanizmus-becslést tesz lehetővé.

A tranzakciós elmélet szerint értelmezhető stresszhez mint rizikófaktorhoz vezető tényezők azonosítása, elemzése mind egyéni, mind szervezeti szinten hozzájárulhat azok menedzsmentjéhez, kezeléséhez. Ez a szervezet kockázatoknak való kitettségét csökkentheti amellett, hogy az információbiztonság, illetve az IKT-infrastruktúra használatának biztonságát is növelheti.

A technostresszorok kezelésével csökkenthetők a negatív hatások, melyben a munkáltatók szerepe jelentős. Lényeges a munkaidő lehatárolása, tiszteletben tartása. Az alkalmazottakat fel kell készíteni az IKT-infrastruktúra használatára. Technológiai fejlesztés esetén érdemes már a beszerzési döntésbe bevonni az infrastruktúra potenciális használóit, illetve a technológia bevezetése esetén képzést kell szervezni, melyen a szükséges készségek elsajátíthatók.

A döntési folyamatba való bevonást az információs aszimmetria elkerülése miatt is érdemes alkalmazni, mivel ezáltal az opportunista viselkedés előfordulása is csökkenthető. Továbbá az információmegosztás jobb teljesítményhez vezet, ami megnyilvánul mind a munkavállalók munkavégzésében, elköteleződésében, mind az információbiztonsági intézkedések betartásában. További előnyt jelenthet, hogy az információmegosztás átláthatóbbá teheti az egyének cselekedeteit a vállalat számára is, ezáltal minimalizálva az opportunizmust, hozzájárulva az információbiztonság fokozásához.

Irodalom

Agarwal, Ritu és Elena Karahanna. "Time Flies When You're Having Fun: Cognitive Absorption and Beliefs about Information Technology Usage." *MIS Quarterly* 24, no. 4 (2000): 665–694. https://doi.org/10.2307/3250951

Ahmed, Abdelmuttlib Ibrahim Abdalla, Siti Hafizah Ab Hamid, Abdullah Gani, Suleman Khan és Muhammad Khurram Khan. "Trust and reputation for Internet of Things: Fundamentals, taxonomy, and open research challenges." *Journal of Network and Computer Applications* 145 (2019): 102409. https://doi.org/10.1016/j.jnca.2019.102409

Ayyagari, Ramakrishna, Varun Grover és Russell Purvis. "Technostress: Technological Antecedents and Implications." *MIS Quarterly* 35, no. 4 (2011): 831–858. https://doi.org/10.2307/41409963

Bak Gerda és Kelemen-Erdős Anikó. "Információbiztonság-tudatosság az Y generáció szemszögéből, kvalitatív megközelítés alapján." *Hadmérnök* 17, 3. szám (2022): 81–95. https://doi.org/10.32567/hm.2022.3.6

Benbasat, Izak és Weiquan Wang. "Trust In and Adoption of Online Recommendation Agents." *Journal of the Association for Information Systems* 6, no. 3 (2005): 72–101. https://doi.org/10.17705/1jais.00065

Bhattacherjee, Anol és Chieh-Peng Lin. "A unified model of IT continuance: three complementary perspectives and crossover effects." *European Journal of Information Systems* 24, no. 4 (2017): 364–373. https://doi.org/10.1057/ejis.2013.36

Brod, Craig. "Managing Technostress: Optimizing the Use of Computer Technology." *Personnel Journal* 61, no. 10 (1982): 753–757.

Chatterjee, Dave. *Cybersecurity readiness: A holistic and high-performance approach.* USA: SAGE Publications, 2021.

Chiu, Tao-Sheng, Wen-Hai Chih, Jaime Ortiz és Chia-Yi Wang. "The contradiction of trust and uncertainty from the viewpoint of swift guanxi." *Internet Research* 28, no. 3 (2018): 716–745. https://doi.org/10.1108/IntR-06-2017-0233

Crossler, Robert E., Allen C. Johnston, Paul Benjamin Lowry, Qing Hu, Merrill Warkentin és Richard Baskerville. "Future directions for behavioral information security research." *Computers & Security* 32 (2013): 90–101. https://doi.org/10.1016/j.cose.2012.09.010

Csikszentmihalyi Mihaly, Sami Abuhamdeh és Jeanne Nakamura. "Flow." In Mihaly Csikszentmihalyi (Szerkesztő). *Flow and the Foundations of Positive Psychology*, 227–238. Dordrecht: Springer, 2014.

da Fonseca, Fábio Bellotti, Rosangela Maria Vanalle és João Alberto Camarotto. "Identification of Ex-Ante and Ex-Post Transaction Costs in Industrial Construction Engineering Projects." *Journal of Civil Engineering and Management* 24, no. 5 (2018): 424–436. https://doi.org/10.3846/jcem.2018.5199

Dalal, Reeshad S., David J. Howard, Rebecca J. Bennett, Clay Posey, Stephan J. Zaccaro és Bradley J. Brummel. "Organizational science and cybersecurity: abundant opportunities for research at the interface." *Journal of Business and Psychology* 37, no. 1 (2022): 1–29. https://doi.org/10.1007/s10869-021-09732-9

D'Arcy, John, Tejaswini Herath és Mindy K. Shoss. "Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective." *Journal of Management Information Systems* 31, no. 2 (2014): 285–318. https://doi.org/10.2753/mis0742-1222310210

Daubert, Jorg, Alexander Wiesmaier és Panayotis Kikiras. "A view on privacy & trust in IoT." In *2015 IEEE International Conference on Communication Workshop (ICCW)*, 2665–2670. London: IEEE, 2015.

Diaz Ismael, Dan S. Chiaburu, Ryan D. Zimmerman és Wendy R. Boswell. "Communication technology: Pros and cons of constant connection to work." *Journal of Vocational Behavior* 80, no. 2 (2012): 500–508. https://doi.org/10.1016/j.jvb.2011.08.007

Ferdousi, Bilquis. "Data Security Concerns and Consumers' Trust in Online Business." In *Proceedings of the 5th NA International Conference on Industrial Engineering and Operations Management*, 2332–2336. USA: IEOM, 2020.

Flowerday, Stephen és Rossouw von Solms. "Trust: An Element of Information Security." In S. Fischer-Hübner, K. Rannenberg, L. Yngström és S. Lindskog (Szerkesztők). *Security and Privacy in Dynamic Environments. SEC 2006*, IFIP International Federation for Information Processing, 201, 87–98. Boston: Springer, 2006.

Forrester Research. "Future of Work." 2019. Utolsó hozzáférés: 2023. január 5. https://www.forrester.com/technology/future-of-work/?utm_source=ciodive&utm_medium=pr&utm_campaign=futureofwork

Fortino, Giancarlo, Lidia Fotia, Fabrizio Messina, Domenico Rosaci és Giuseppe M. L. Sarne. "Trust and Reputation in the Internet of Things: State-of-the-Art and Research Challenges." *IEEE Access* 8 (2020): 60117–60125. https://doi.org/10.1109/access.2020.2982318

Furnell, Steven, Harry Heyburn, Andrew Whitehead és Jayesh Navin Shah. "Understanding the full cost of cyber security breaches." *Computer Fraud & Security* 2020, no. 12 (2020): 6–12. https://doi.org/10.1016/s1361-3723(20)30127-5

Gefen, David, Izak Benbasat és Paula Pavlou. "A Research Agenda for Trust in Online Environments." *Journal of Management Information Systems* 24, no. 4 (2014): 275–286. https://doi.org/10.2753/mis0742-1222240411

Gottschalk, Petter és Hans Solli-Sæther. "Critical success factors from IT outsourcing theories: an empirical study." *Industrial Management & Data Systems* 105, no. 6 (2005): 685–702. https://doi.org/10.1108/02635570510606941

Gratian, Margaret, Sruthi Bandi, Michel Cukier, Josiah Dykstra és Amy Ginther. "Correlating human traits and cyber security behavior intentions." *Computers & Security* 73 (2018): 345–358. https://doi.org/10.1016/j.cose.2017.11.015

Graveling, Richard. *The mental health of workers in the digital era: How recent technical innovation and its pace affects the mental well-being of workers.* European Parliament, Directorate-General for Internal Policies of the Union, 2020. https://doi.org/10.2861/986378

Guo, Yi Maggie és Young K. Ro. "Capturing Flow in the Business Classroom." *Decision Sciences Journal of Innovative Education* 6, no. 2 (2008): 437–462. https://doi.org/10.1111/j.1540-4609.2008.00185.x

Hansen, Lene és Helen Nissenbaum. “Digital Disaster, Cyber Security, and the Copenhagen School.” *International Studies Quarterly* 53, no. 4 (2009): 1155–1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x

Hauk, Nathalie, Anja S. Göritz és Stefan Krumm. “The mediating role of coping behavior on the age-technostress relationship: A longitudinal multilevel mediation model.” *PLoS One* 14, no. 3 (2019): e0213349. https://doi.org/10.1371/journal.pone.0213349

Hill, Charles W.L. “Cooperation, Opportunism, and the Invisible Hand: Implications for Transaction Cost Theory.” *The Academy of Management Review* 15, no. 3 (1990): 500. https://doi.org/10.2307/258020

Hooper, Val és Chris Blunt. “Factors influencing the information security behaviour of IT employees.” *Behaviour & Information Technology* 39, no. 8 (2019): 862–874. https://doi.org/10.1080/0144929x.2019.1623322

Hosking, Ian Michael és Kate Livingstone. “Meta-usability: Understanding the Relationship Between Information Technology and Well-Being.” In Marcelo M. Soares, Elisabeth Rosenzweig és Aaron Marcus (Szerkesztők). *Design, User Experience, and Usability: Design Thinking and Practice in Contemporary and Emerging Technologies. HCII 2022*. Lecture Notes in Computer Science, 14–32. Cham: Springer, 2022.

Hwang, Inho, Sanghyun Kim és Carl Rebman. “Impact of regulatory focus on security technostress and organizational outcomes: the moderating effect of security technostress inhibitors.” *Information Technology & People* 35, no. 7 (2021): 2043–2074. https://doi.org/10.1108/itp-05-2019-0239

Im, Ghi Paul és Richard L. Baskerville. “A longitudinal study of information system threat categories.” *ACM SIGMIS Database: the DATABASE for Advances in Information Systems* 36, no. 4 (2005): 68–79. https://doi.org/10.1145/1104004.1104010

Jenei, Szonja és Módosné Szalai Szilvia. “A digitális átalakulás és a koronavírus járvány hatásai a munkaerőpiacon.” Új Munkaügyi Szemle 3, 2. szám (2022): 2–12.

Johnson, Devon S., Fleura Bardhi és Dan T. Dunn. “Understanding how technology paradoxes affect customer satisfaction with self-service technology: The role of performance ambiguity and trust in technology.” *Psychology and Marketing* 25, no. 5 (2008): 416–443. https://doi.org/10.1002/mar.20218

Kamal, Nida, Sajeela Rabbani, Hina Samdani, Sobia Shujaat és Mubashir Ahmad. “Social Media Usage, Overload and Exhaustion: A Performance Perspective.” *International Review of Management and Marketing* 10, no. 5 (2020): 19–26. https://doi.org/10.32479/irmm.10190

Kaplan, Andreas és Michael Haenlein. “Rulers of the world, unite! The challenges and opportunities of artificial intelligence.” *Business Horizons* 63, no. 1 (2020): 37–50. https://doi.org/10.1016/j.bushor.2019.09.003

Karimikia, Hadi, Harminder Singh és Damien Joseph. “Negative outcomes of ICT use at work: meta-analytic evidence and the role of job autonomy.” *Internet Research* 31, no. 1 (2020): 159–190. https://doi.org/10.1108/intr-09-2019-0385

Kováts Gergely. “A bizalom szerepe egy felsőoktatási reform megvalósulásában: a fenntartói megállapodások esete.” *Vezetéstudomány* 50, 6. szám (2019): 2–13. https://doi.org/10.14267/veztud.2019.06.01.

Lankton, Nancy, D. Harrison McKnight és John Tripp. “Technology, Humanness, and Trust: Rethinking Trust in Technology.” *Journal of the Association for Information Systems* 16, no. 10 (2015): 880–918. https://doi.org/10.17705/1jais.00411

La Torre, Giuseppe, Alessia Esposito, Iliana Sciarra és Marta Chiappetta. “Definition, symptoms and risk of techno-stress: a systematic review.” *Int Arch Occup Environ Health* 92, no. 1 (2019): 13–35. https://doi.org/10.1007/s00420-018-1352-1.

Lazarus, Richard S. és Susan Folkman. *Stress, appraisal, and coping*. New York: Springer, 1984.

Lee, Chunghun, Choong C. Lee és Suhyun Kim. “Understanding information security stress: Focusing on the type of information security compliance activity.” *Computers & Security* 59 (2016): 60–70. https://doi.org/10.1016/j.cose.2016.02.004

Lehota Zsuzsanna, Lehota József, Komáromi Nándor és Illés Bálint Csaba. “Az élelmiszerfogyasztói információ-ellátottság, a bizalom és a fogyasztói magatartás kapcsolatrendszere.” In Lencsés Enikő és Pataki László (Szerkesztők). *Menedzsment válaszok a XXI. század gazdasági és társadalmi kihívásaira*, 201–211. Budapest: Inform Kiadó és Nyomda Kft, 2020.

Levitt, Ted. *Internet of Things - IoT Governance, Privacy and Security Issues*. European Commission. 2015. Utolsó hozzáférés: 2023. január 5. http://www.internet-of-things-research.eu/pdf/IERC_Position_Paper_IoT_Governance_Privacy_Security_Final.pdf

Li, Ling, Li Xu, Wu He, Yong Chen és Hong Chen. „Cyber Security Awareness and Its Impact on Li, Ling, Li Xu, Wu He, Yong Chen és Hong Chen. “Cyber Security Awareness and Its Impact on Employee’s Behavior.” In A. Tjoa, L. Xu, M. Raffai és N. Novak (Szerkesztők). *Research and Practical Issues of Enterprise Information Systems. CONFENIS 2016. Lecture Notes in Business Information Processing*, 103–111. Cham: Springer, 2016.

Lieli, Suharti és Susanto Agung. “The Impact of Workload and Technology Competence on Technostress and Performance of Employees.” *Indian Journal of Commerce & Management Studies* 5, no. 2 (2014): 1–7.

Lowry, Paul Benjamin, Jun Zhang, Gregory D. Moody, Sutirtha Chatterjee, Chuang Wang és Tailai Wu. “An Integrative Theory Addressing Cyberharassment in the Light of Technology-Based Opportunism.” *Journal of Management Information Systems* 36, no. 4 (2019): 1142–1178. https://doi.org/10.1080/07421222.2019.1661090

McKnight, D. Harrison, Michelle Carter, Jason Bennett Thatcher és Paul F. Clay. “Trust in a specific technology.” *ACM Transactions on Management Information Systems* 2, no. 2 (2011): 1–25. https://doi.org/10.1145/1985347.1985353

McKnight, D. Harrison, Peng Liu és Brian T. Pentland. “Trust Change in Information Technology Products.” *Journal of Management Information Systems* 37, no. 4 (2020): 1015–1046. https://doi.org/10.1080/07421222.2020.1831772

Mészáros Alexandra Ágnes és Tick Andrea. “Az ipari kémkedéssel szembeni felkészültség vizsgálata a magyar szervezetek körében.” *Biztonságtudományi Szemle* 3, no. 4 (2021): 57–72.

Muha Lajos és Krasznay Csaba. *Az elektronikus információs rendszerek biztonságának menedzselése*. Budapest: NKE, 2018.

Ninaus, Katharina, Sandra Diehl és Ralf Terlutter. “Employee perceptions of information and communication technologies in work life, perceived burnout, job satisfaction and the role of work-family balance.” *Journal of Business Research* 136, no. 9 (2021): 652–666. https://doi.org/10.1016/j.jbusres.2021.08.007

Ninaus, Katharina, Sandra Diehl, Ralf Terlutter, Kara Chan és Anqi Huang. “Benefits and stressors – Perceived effects of ICT use on employee health and work stress: An exploratory study from Austria and Hong Kong.” *International Journal of Qualitative Studies on Health and Well-being* 10, no. 1 (2015): 28838. https://doi.org/10.3402/qhw.v10.28838

Nissenbaum, Helen. “Where Computer Security Meets National Security1.” *Ethics and Information Technology* 7, no. 2 (2005): 61–73. https://doi.org/10.1007/s10676-005-4582-3

Pathak, Buddhi, Mona Ashok és Yin Leng Tan. “Value co-destruction: Exploring the role of actors’ opportunism in the B2B context.” *International Journal of Information Management* 52 (2020): 102093. https://doi.org/10.1016/j.ijinfomgt.2020.102093

Pham, Hiep-Cong, Jamal El-Den és Joan Richardson. “Stress-based security compliance model – an exploratory study.” *Information & Computer Security* 24, no. 4 (2016): 326–347. https://doi.org/10.1108/ics-10-2014-0067

Pirkkalainen, Henri, Markus Salo, Monideepa Tarafdar és Markus Makkonen. “Deliberate or Instinctive? Proactive and Reactive Coping for Technostress.” *Journal of Management Information Systems* 36, no. 4 (2019): 1179–1212. https://doi.org/10.1080/07421222.2019.1661092

Qi, Cong. “A double-edged sword? Exploring the impact of students’ academic usage of mobile devices on technostress and academic performance.” *Behaviour & Information Technology* 38, no. 12 (2019): 1337–1354. http://doi.org/10.1080/0144929x.2019.1585476

Rab Árpád és Török Bernát. “Online bizalom a magyar társadalomban.” *Információs Társadalom* 20, 3. szám (2020): 92–98. http://doi.org/10.22503/inftars.XX.2020.3.6

Reicher Regina. “Hungarian Millennials’ attitudes on being online.” *Forum Scientiae Oeconomia* 6, no. 1 (2018): 5–18. http://doi.org/10.23762/FSO_VOL6NO1_18_1

Reinke, Kathrin és Sandra Ohly. “Double-edged effects of work-related technology use after hours on employee well-being and recovery: The role of appraisal and its determinants.” *German Journal of Human Resource Management: Zeitschrift Für Personalforschung* 35, no. 2 (2021): 224–248. http://doi.org/10.1177/2397002221995797

Rindfleisch, Aric. “Transaction cost theory: past, present and future.” *AMS Review* 10, no. 1–2 (2019): 85–97. https://doi.org/10.1007/s13162-019-00151-x.

Rousseau, Denise M., Sim B. Sitkin, Ronald S. Burt és Colin Camerer. “Not So Different After All: A Cross-Discipline View Of Trust.” *Academy of Management Review* 23, no. 3 (1998): 393–404. https://doi.org/10.5465/amr.1998.926617

Schmidt, Christoph G. és Stephan M. Wagner. "Blockchain and supply chain relations: A transaction cost theory perspective." *Journal of Purchasing and Supply Management* 25, no. 4 (2019): 100552.
https://doi.org/10.1016/j.pursup.2019.100552

Schmidt, Marco, Lukas Frank és Henner Gimpel. "How Adolescents Cope with Technostress: A Mixed-Methods Approach." *International Journal of Electronic Commerce* 25, no. 2 (2021): 154–180.
https://doi.org/10.1080/10864415.2021.1887696

Sharma, Avani, Emmanuel S. Pilli, Arka P. Mazumdar és Poonam Gera. "Towards trustworthy Internet of Things: A survey on Trust Management applications and schemes." *Computer Communications* 160 (2020): 475–493.
https://doi.org/10.1016/j.comcom.2020.06.030

Sicari, Sabrina, Alessandra Rizzardi, Luigi Alfredo Grieco és Alberto Coen-Porisini. "Security, privacy and trust in Internet of Things: The road ahead." *Computer Networks* 76 (2015): 146–164.
https://doi.org/10.1016/j.comnet.2014.11.008

Siham, El-Kafafi. "Providing Constructive Feedback: Emotional Intelligence Perspective." In Karadal, Himmet, Erdogan Ekiz, Muhammet Saygin, Evren Dinçer és Menekşe Şahin Karadal (Szerkesztők). *7th International EMI Entrepreneurship & Social Sciences Congress Proceedings E-Book*, Tashkent, Üzbegisztán, Dilkur Academy, Jun 20-22. (2022): 376–387.

Siponen, Mikko, M. Adam Mahmood és Seppo Pahnila. "Employees' adherence to information security policies: An exploratory field study." *Information & Management* 51, no. 2 (2014): 217–224.
https://doi.org/10.1016/j.im.2013.08.006

Spiess, Teresa, Christian Ploder, Reinhard Bernsteiner és Thomas Dilger. "Techno-stress in the workplace: triggers, outcomes, and coping strategies with a special focus on generational differences." *International Journal of Web Engineering and Technology* 16, no. 3 (2021): 217.
https://doi.org/10.1504/ijwet.2021.119875

Tarafdar, Monideepa, Cary L. Cooper és Jean-François Stich. "The technostress trifecta - techno eustress, techno distress and design: Theoretical directions and an agenda for research." *Information Systems Journal* 29, no. 1 (2017): 6–42.
https://doi.org/10.1111/isj.12169

Tarafdar, Monideepa, Ellen Bolman Pullins és T. S. Ragu-Nathan. "Technostress: negative effect on performance and possible mitigations." *Information Systems Journal* 25, no. 2 (2015): 103–132.
https://doi.org/10.1111/isj.12042

Tarafdar, Monideepa, Qiang Tu, Bhanu S. Ragu-Nathan és T. S. Ragu-Nathan. "The Impact of Technostress on Role Stress and Productivity." *Journal of Management Information Systems* 24, no. 1 (2014): 301–328.
https://doi.org/10.2753/mis0742-1222240109

Tourinho, Ana és Bruna de Oliveira. "Time flies when you are having fun: Cognitive Absorption and Beliefs about Social Media Usage." *AIS Transactions on Replication Research* no. 5 (2019): 1–14.
https://doi.org/10.17705/1atrr.00036

Trang, Simon és Ilja Nastjuk. “Examining the role of stress and information security policy design in information security compliance behaviour: An experimental study of in-task behaviour.” *Computers & Security* 104 (2021): 102222. https://doi.org/10.1016/j.cose.2021.102222

Valociková Cintia. “A bizalom a játékelméletek vizsgálatán keresztül.” *Biztonságtudományi Szemle* 4, 2. szám (2022): 15–24.

Vasilomanolakis, Emmanouil, Jorg Daubert, Manisha Luthra, Vangelis Gazis, Alex Wiesmaier és Panayotis Kikiras. “On the Security and Privacy of Internet of Things Architectures and Systems.” In *2015 International Workshop on Secure Internet of Things (SIoT)*, 49–57. IEEE, 2015.

Venz, Laura és Hadar Nesher Shoshan. “Be smart, play dumb? A transactional perspective on day-specific knowledge hiding, interpersonal conflict, and psychological strain.” *Human Relations* 75, no. 1 (2021): 113–138. https://doi.org/10.1177/0018726721990438

Vigren, Olli, Anna Kadefors és Kent Eriksson. “Digitalization, innovation capabilities and absorptive capacity in the Swedish real estate ecosystem.” *Facilities* 40, no. 15/16 (2022): 89–106. https://doi.org/10.1108/F-07-2020-0083

Webster, Jane és Hayes Ho. “Audience engagement in multimedia presentations.” *ACM SIGMIS Database: the DATABASE for Advances in Information Systems* 28, no. 2 (1997): 63–77. https://doi.org/10.1145/264701.264706

Weil, Michelle M. és Larry D. Rosen. *TechnoStress: Coping with Technology @Work @Home @ Play.* New York: Wiley, 1997.

Williamson, Oliver E. *Markets and hierarchies: analysis and antitrust implications: a study in the economics of internal organization.* New York: Free Press, 1975.

World Economic Forum. “The Future of Jobs Report 2018: Centre for the New Economy and Society.” 2018 Utolsó hozzáférés: 2023. február 1. https://www3.weforum.org/docs/WEF_Future_of_Jobs_2018.pdf