ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

**DOKTORI (PHD) ÉRTEKEZÉS**

**TÉZISFÜZETE**

**FEHÉR-POLGÁR PÁL**

# Biztonsági stratégia kialakításának lehetőségei saját tulajdonú mobileszközök munkacélú használatára

Témavezető: Prof. Dr. Michelberger Pál

**BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA**

Budapest, 2026. március 19.

# Tartalomjegyzék

# 1 Summary

The Bring Your Own Device (BYOD) paradigm has become an indispensable element of modern operations, offering significant flexibility and efficiency. However, it fundamentally disrupts traditional network perimeter defenses. The scientific novelty and primary role of this doctoral thesis lie in shifting the cybersecurity focus from purely technological (hard) controls to a comprehensive socio-technical approach. By analyzing human decision-making mechanisms and subjective risk perception, the research addresses the critical vulnerability in IT systems: the user.

Based on an empirical study of a technology-oriented sample, the research established five key scientific theses:

1. Domain-Specific IT Risk-Taking: IT security risk-taking emerges as an independent, measurable construct within the DOSPERT framework, distinct from other everyday risks and influenced by demographics.
2. Perceptional Positioning: Users evaluate cyber threats structurally differently compared to traditional risk domains (e.g., financial or health risks).
3. Perception and Behavior: There is a statistically significant correlation between subjective risk perception and actual security-conscious behavior in a BYOD context.
4. Security Awareness Paradox: Higher technical competence often creates an "illusion of control", which paradoxically increases IT security risk-taking rather than fostering caution.
5. Benefit-Dominant Decision Architecture: In IT security decisions, the perceived benefits (convenience, flexibility) significantly outweigh the deterrent effect of perceived risks, driving user behavior toward pragmatic advantages.

**Corporate and Military Utilization**

The results offer direct strategic applications for both corporate and defense sectors. For corporate Chief Information Security Officers (CISOs), the findings necessitate a shift toward User Experience (UX) focused security (security by default), tailored training programs (Awareness 2.0) to mitigate the awareness paradox, and the integration of Zero Trust Architecture (ZTA). Furthermore, the developed measurement framework provides a crucial foundation for military and defense utilization. Applying this model in strict, hierarchical military environments enables defense organizations to accurately assess cyber risk-taking tendencies, refine strategic protocols, and develop specialized behavioral training that mitigates the illusion of control among personnel managing critical infrastructure.

# 2 A kutatás előzményei

A digitális technológia elmúlt két évtizedben tapasztalható robbanásszerű fejlődése alapvetően átalakította a munkavégzés, az információkezelés és a kommunikáció kereteit. A mobileszközök – különösen az okostelefonok és a táblagépek – mára nem csupán a mindennapi élet kényelmi kiegészítői, hanem a vállalati működés, a civil szféra, sőt, a katonai és kritikus infrastruktúrák meghatározó információs csomópontjaivá is váltak. Az információkhoz való folyamatos hozzáférés, az állandó online jelenlét és a helyfüggetlen munkavégzés (bárhonnan, bármikor) egy olyan új működési modellt hozott létre, amelyben a munka és a magánélet korábban merev határai egyre inkább elmosódnak.

E folyamat egyik legmeghatározóbb, szervezeti szintű jelensége a BYOD (Bring Your Own Device), azaz a saját tulajdonú mobileszközök munkacélú használata. A BYOD keretében a munkavállalók saját okoseszközeiken keresztül férnek hozzá a vállalati erőforrásokhoz, érzékeny adatbázisokhoz és felhőszolgáltatásokhoz. Bár ez a megközelítés soha nem látott rugalmasságot, költséghatékonyságot és produktivitás-növekedést eredményezett a szervezetek számára, ezzel párhuzamosan alapjaiban bontotta meg a hagyományos vállalati hálózatok úgynevezett peremvédelmét (perimeter defense). A vállalati és a magánhasználat egyazon fizikai és szoftveres térben valósul meg, ami az információbiztonsági kontroll szempontjából rendkívül érzékeny, új típusú kockázati struktúrát teremt. Ez a jelenség nem csupán a civil szférát érinti: a civil-katonai technológiai konvergencia révén a BYOD és a mobileszközök metaadat-kitettsége a védelmi és honvédelmi szektorban is kritikus stratégiai kockázattá lépett elő.

A doktori értekezés ebből a problémakörből indul ki, és alapvető kutatási tézise, hogy a BYOD nem kizárólag informatikai vagy technológiai kérdés, hanem döntéselméleti, viselkedéstudományi és rendszerelméleti megközelítést is igényel. A kutatás fókuszpontjában az a felismerés áll, hogy a szervezeti információbiztonsági incidensek túlnyomó többsége napjainkban már nem a technológiai (hard) védelmi vonalak hiányosságaira, hanem a felhasználói döntési mechanizmusokra és a szubjektív kockázatészlelés anomáliáira vezethető vissza. A kutatás célja a technológiai és a humán dimenzió kölcsönhatásának, azaz a BYOD szocio-technikai rendszerének átfogó vizsgálata, különös tekintettel az IT-biztonsági kockázatvállalási hajlandóság mérhetőségére és viselkedésalapú összefüggéseire.

A BYOD jelenség és az információbiztonság szakirodalma az elmúlt években rendkívül kiterjedtté vált, azonban a tudományos megközelítések fókuszpontjai egyenetlenek. A korábbi ku-

tatások és szakmai publikációk túlnyomó része elsősorban a technológiai és szabályozási perspektívát helyezi előtérbe. Számos tanulmány foglalkozik a mobileszközök technikai sérülékenységeivel, a hálózati fenyegetésekkel, a fizikai kitettséggel (pl. eszközök elhagyása), az adatbiztonsági kockázatokkal, valamint a kommunikációs csatornákon keresztül kiszivárgó metaadatok veszélyeivel. A szervezeti válaszok tekintetében a szakirodalom hagyományosan a technikai kontrollok – mint a Mobileszköz-menedzsment (MDM) rendszerek – bevezetését, illetve a merev jogi szabályozások fontosságát hangsúlyozza.

Ezzel szemben lényegesen kevesebb figyelem irányult arra, hogy a felhasználói döntések, a kognitív torzítások és az egyéni kockázatvállalási attitűdök miként befolyásolják a biztonsági fenyegetettséget. A biztonságtudományi szakirodalomban ugyan közhelynek számít a Michelberger [3], Keszthelyi [1] és más szerzők által is megfogalmazott tétel, miszerint „a leggyengébb láncszem az ember”, azonban e humán tényező strukturált, empirikus mérése sokáig hiányos volt az IT-kockázatok terén.

A kockázat fogalmának tudományos értelmezéséhez a dolgozat Renn [4] kockázatklasszifikációs modelljére támaszkodik, amely a bizonytalanság és az érték kapcsolatát, valamint a technológiai, adatvédelmi, szervezeti és humán kockázati dimenziók integrált kezelését teszi lehetővé. A humán tényező és az egyéni kockázatvállalás mélyebb vizsgálatához a kutatás a pszichológiai szakirodalomból ismert, Weber, Blais és Betz által megalkotott DOSPERT (Domén-Specific Risk-Taking) [1][5] skálát emeli be. A DOSPERT modell alapvetése, hogy a kockázatvállalás nem egy univerzális személyiségvonás, hanem doménspecifikus: az emberek másként kockáztatnak az öt eredeti területen (pénzügyi, egészségügyi/biztonsági, etikai, szociális és rekreációs domének).

A szakirodalmi áttekintés külön kitér az Y és Z generáció, avagy a „digitális bennszülöttek” sajátosságaira is. E generációk számára a technológia használata természetes és rutinszerű, gyors és kényelmes megoldásokat várnak el. Elemzések mutatják, hogy a kényelmi funkciók előtérbe helyezése gyakran vezet az árnyékinformatika (Shadow IT) erősödéséhez, amikor is a munkavállalók megkerülik a hivatalos, de kényelmetlen vállalati biztonsági csatornákat.

A disszertáció a felvázolt szakirodalmi hiányosságokra (kutatási résekre) reagálva, jellemzően műszaki és informatikai egyetemi hallgatókból álló, mintán végzett empirikus kutatással több ponton is továbbfejleszti a korábbi tudományos modelleket.

A kutatás elsődleges és legfontosabb kapcsolódási pontja a DOSPERT modellhez kötődik. Míg a korábbi pszichológiai kutatások nem tartalmaztak dedikált informatikai területet, a jelen kutatás sikeresen kiterjesztette a modellt, és statisztikailag validálta az IT-biztonsági kockázatvállalást mint önálló, a korábbiaktól jól elkülöníthető domént. Az eredmények kimutatták, hogy az eredeti öt domén nem képes megbízhatóan előre jelezni az informatikai kockázatvállalást, azaz a felhasználók a kibertérből érkező veszélyeket másként értékelik és pozicionálják, mint a mindennapi élet (például egészségügyi vagy pénzügyi) fenyegetettségeit.

A korábbi információbiztonsági kutatások gyakran egy leegyszerűsített, racionális modellt (Homo Economicus) feltételeztek, amely szerint a magasabb észlelt fenyegetettség automatikusan elrettentő erővel bír, és óvatosabb magatartást eredményez. Ezzel szemben a dolgozat többváltozós regressziós modellekkel igazolta a „Haszon-domináns döntési architektúra" meglétét. Az eredmények bizonyítják, hogy a BYOD-döntésekben súlyos aszimmetria áll fenn: az észlelt pragmatikus haszon (kényelem, rugalmasság, gyorsaság) standardizált regressziós súlya ($\beta = 0{,}679$) többszörösen felülmúlja az észlelt kockázat visszatartó erejét ($\beta = -0{,}125$). Ez empirikus magyarázatot ad a Shadow IT terjedésére, hiszen igazolja, hogy a döntéseket nem a fenyegetettség elkerülése, hanem az előnyök maximalizálása vezérli.

Végezetül a disszertáció radikálisan újraértelmezi a hagyományos biztonságtudatossági (awareness) oktatások hatékonyságáról szóló korábbi nézeteket. A klasszikus megközelítés szerint a magasabb technikai tudás egyenlő a nagyobb biztonsággal. Az értekezés ezzel szemben azonosította és igazolta a „Biztonságtudatossági paradoxont". Az adatok rámutattak, hogy a magasabb technikai kompetenciával rendelkező (például folyamatosan frissítéseket telepítő) felhasználók körében fellép a kontroll illúziója, aminek következtében paradox módon hajlamosabbak nagyobb IT-biztonsági (szervezeti) kockázatot vállalni, mint a laikusok.

Ezen tudományos eredmények összessége rámutat arra, hogy a korábbi, tisztán tiltásra és technológiai peremvédelemre épülő stratégiák fenntarthatatlanok. A kutatás a szakirodalom eddigi fókuszát áthelyezve arra a következtetésre jut, hogy mind a civil vállalatok, mind a katonai és kritikus infrastruktúrák számára olyan új keretrendszerekre – például Zero Trust Architecture (ZTA) integrációjára és felhasználói élményre (UX) fókuszáló, „láthatatlan" biztonsági kontrollokra – van szükség, amelyek alkalmazkodnak a felhasználók kognitív, haszon-domináns pszichológiai valóságához.

# 3 Célkitűzések

A jelen doktori kutatás átfogó célja a saját tulajdonú mobileszközök munkacélú használatából (BYOD) fakadó információbiztonsági kihívások újszerű, szocio-technikai megközelítésű vizsgálata. Bár a technológiai védelmi vonalak elengedhetetlenek, a rendszer legkritikusabb pontja maga a felhasználó és az ő döntési mechanizmusa. Ennek megértése és a vállalati stratégiába történő integrálása érdekében az alábbi öt, egymásra épülő kutatási célt fogalmaztam meg:

### C1: Az IT-biztonsági kockázatvállalás mint önálló, doménspecifikus konstrukció azonosítása és mérési kereteinek validálása

Az általános kockázatvállalási hajlandóságot vizsgáló modellek (mint például a DOSPERT) hagyományosan pénzügyi, egészségügyi, etikai, szociális és rekreációs doméneket különítenek el. Kutatásom elsődleges célja annak tudományos igazolása, hogy az infokommunikációs technológiák térnyerésével az IT-biztonsági kockázatvállalás egy ezektől jól elkülöníthető, önálló doménként jelenik meg az egyének kognitív térképén. Célom továbbá feltárni, hogy ez a specifikus IT-kockázatvállalási hajlandóság milyen mértékben magyarázható olyan alapvető demográfiai és egyéni változókkal, mint az életkor vagy a nem, ezáltal megteremtve a felhasználói viselkedés mérésének és előrejelzésének alapjait.

### C2: Az IT-biztonsági kockázatok percepciós helyzetének meghatározása és rendszerezése a BYOD-környezetben

Nem elegendő pusztán azonosítani az IT-biztonságot, mint önálló területet; vizsgálni kell annak szubjektív súlyát is a felhasználók értékrendjében. Második célkitűzésem a BYOD modell alkalmazása során felmerülő specifikus kockázatok (adatvesztés, jogosulatlan hozzáférés, eszközök kompromittálódása stb.) strukturált rendszerezése, valamint annak feltárása, hogy a felhasználók a mindennapi életük során megélt egyéb (pl. pénzügyi vagy egészségügyi) fenyegetettségekhez képest hová pozicionálják a kibertérből érkező veszélyeket. Ennek megértése elengedhetetlen a megfelelő fókuszú vállalati figyelemfelhívó és oktatási programok, biztonságtudatosság kialakításához.

### C3: A szubjektív kockázatpercepció és a biztonságtudatos felhasználói viselkedés közötti összefüggések feltárása

A szakirodalom gyakran feltételezi, hogy a magasabb fenyegetettség-érzet automatikusan óvatosabb magatartást eredményez. Harmadik kutatási célom ennek az összefüggésnek az empirikus vizsgálata a mobil okoseszközök vállalati környezetben történő használata során. Meg kívánom vizsgálni, hogy a felismert és észlelt kockázatok (szubjektív percepció) milyen irányban és mértékben alakíthatóak tényleges, mérhető biztonságtudatos viselkedéssé (például képernyőzár használata, nyilvános hálózatok kerülése). Célom azonosítani azokat a tényezőket, amelyek erősítik, vagy éppen gátolják ezt az átmenetet.

### C4: A technikai biztonságtudatosság és a szervezeti kockázatvállalás ellentmondásainak (biztonságtudatossági paradoxon) elemzése

A szervezeti IT-biztonsági incidensek jelentős része nem az ismeretek hiányából, hanem a túlzott magabiztosságból fakad. Negyedik célom a "biztonságtudatossági paradoxon" jelenségének mélyreható elemzése a BYOD kontextusában. Ennek során azt vizsgálom, hogy a magasabb szintű technikai kompetenciák és a fejlett biztonsági ismeretek hogyan és miért vezethetnek – a kontroll illúzióján keresztül – magasabb szervezeti kockázatvállaláshoz. E jelenség feltárása rávilágít arra, hogy a puszta technikai oktatás önmagában miért nem elégséges a biztonsági incidensek elkerüléséhez.

### C5: A haszon-domináns döntési mechanizmusok feltárása és a BYOD döntéstámogató stratégiai alapjainak kidolgozása

A BYOD modell terjedésének alapvető motorja a felhasználói és szervezeti előnyök maximalizálása. Ötödik célkitűzésem annak bizonyítása, hogy az IT-biztonsági és eszközhasználati döntések során a felhasználók kognitív mérlegelésében súlyos aszimmetria figyelhető meg: az észlelt haszon (pl. kényelem, rugalmasság, produktivitás) sokkal erősebben dominálja a viselkedést, mint az észlelt kockázat. Eredményeimre támaszkodva egy olyan döntéstámogató és stratégiai keretrendszer alapjainak kidolgozását tűztem ki célul, amely a tiltáson alapuló, tisztán technológiai (hard) megközelítés helyett a viselkedésalapú, a haszon-kockázat aszimmetriát menedzselni képes (soft) elemeket is integrálja a vállalati biztonsági szabályozásba.

# 4 Vizsgálati módszerek

A kutatás módszertani alapvetései és megközelítése

A doktori értekezés primer kutatásának célja a BYOD (Bring Your Own Device) környezetben megjelenő felhasználói döntési mechanizmusok, a szubjektív kockázatészlelés és a tényleges biztonságtudatos viselkedés közötti összefüggések feltárása volt. A megfogalmazott öt kutatási cél és a kilenc hipotézis (H1–H9) empirikus tesztelése érdekében a kutatás egy deduktív, többváltozós, kvantitatív statisztikai elemzésekre épülő módszertani keretrendszert alkalmazott. A témakör szocio-technikai jellege miatt a kutató nem csupán a technológiai paramétereket, hanem a felhasználók pszichológiai és kognitív döntési térképét kívánta mérhetővé tenni, amihez egy robusztus, nemzetközileg validált pszichometriai mérőeszköz adaptálására volt szükség.

Az adatfelvétel eszköze: A DOSPERT skála kiterjesztése

A kutatás legfontosabb módszertani innovációja a kérdőíves adatfelvétel eszközének megválasztása és továbbfejlesztése volt. A szubjektív kockázatvállalás mérésére az eredetileg Weber, Blais és Betz által megalkotott DOSPERT (Domain-Specific Risk-Taking) [1][5] skála szolgált alapul. Az eredeti DOSPERT modell alaptézise, hogy a kockázatvállalás nem egy univerzális személyiségvonás, hanem területspecifikus (doménspecifikus): az emberek eltérő módon értékelik a kockázatokat öt alapvető domén – a pénzügyi, az egészségügyi/biztonsági, az etikai, a szociális és a rekreációs – területein.

Mivel az eredeti mérőeszköz nem tartalmazott az IT-biztonságra vonatkozó kérdéseket. Kutatásomban az eredeti struktúrát egy hatodik, specifikusan az IT-biztonsági kockázatvállalást mérő doménnel egészítettem ki. A kérdőív egyidejűleg mérte a válaszadók esetében:

Az észlelt kockázatot (milyen veszélyesnek tartanak egy adott cselekvést, pl. nyílt Wi-Fi hálózatra való csatlakozást vagy céges adatok saját, privát emailcímre való továbbítását).

Az észlelt hasznot (milyen előnyöket remélnek az adott cselekvéstől, pl. kényelem, időmegtakarítás, gyorsabb munkavégzés).

A cselekvési valószínűséget vagy kockázatvállalási hajlandóságot (milyen eséllyel tennék meg az adott cselekvést a valóságban).

A kérdőív ezen felül kitért a tényleges, mindennapi biztonságtudatos viselkedés elemeire (például a képernyőzár használati szokásaira, a jelszókezelésre), valamint a válaszadók technikai affinitására és demográfiai adataira is. A válaszok számszerűsítése hagyományos, többpontos

Likert-skálák segítségével történt, amely lehetővé tette a parametrikus és nem-parametrikus statisztikai próbák későbbi alkalmazását.

A mintavételi eljárás és a minta jellemzői

A primer adatfelvétel kényelmi mintavételi eljárással készített, célzott megkérdezés keretében zajlott két időszakban (2019, 2025). A kutatás végleges mintái 357, illetve 772 főből álltak. A válaszadók felsőoktatásban részt vevő hallgatók voltak, döntően műszaki és informatikai (például villamosmérnök, gépészmérnök, gazdaságinformatikus) tanulmányokat folytató fiatal felnőttek.

Bár a minta demográfiai és iskolai végzettség tekintetében homogénabb, és a teljes magyar aktív korú lakosságra nézve statisztikailag nem reprezentatív, a vizsgált célcsoport kiválasztása tudatos kutatói döntés eredménye volt. A minta a társadalom azon szegmensét, az úgynevezett „Y és Z generációt" vagy digitális bennszülötteket fedi le, akik a BYOD megoldások legaktívabb jelenlegi és jövőbeni felhasználói. Számukra a technológia integrációja a mindennapi életbe rutinszerű. A mérnöki és IT-affinis hallgatók bevonása különösen fontossá vált a módszertan szempontjából, hiszen ezen a csoporton keresztül lehetett a leghatékonyabban tesztelni a kutatás egyik legfontosabb felvetését: a magasabb technológiai tudás és a túlzott kockázatvállalás (biztonságtudatossági paradoxon) kapcsolatát. A kutatás érvelése szerint, ha az IT-biztonsági anomáliák, a kognitív torzítások és a szabálykerülési hajlandóság (Shadow IT) egy technológiában jártas rétegnél is markánsan kimutatható, akkor az a kevésbé képzett vállalati munkavállalók körében még fokozottabban jelen lehet.

Alkalmazott statisztikai elemzések

A begyűjtött kvantitatív adatok rögzítése, tisztítása és mélyreható statisztikai elemzése az IBM SPSS szoftvercsomag segítségével történt. A módszertan egymásra épülő, komplex statisztikai eljárások sorozatát foglalta magában:

- Leíró statisztikák és skálamegbízhatóság: Az alapsokaság jellemzésére átlagok, szórások és gyakoriságok kiszámítására került sor. A kiterjesztett DOSPERT skála megbízhatóságának és belső konzisztenciájának ellenőrzésére a kutató Cronbach-alfa mutatókat alkalmazott, igazolva a kérdőív validitását a hazai és a specifikus IT környezetben.
- Faktoranalízis (Főkomponens-elemzés): Az 1. tézis (az IT-biztonság önálló konstrukcióként való azonosítása) igazolása érdekében faktorelemzést hajtottam végre. A változók faktorálhatóságát a KMO (Kaiser-Meyer-Olkin) kritérium és a Bartlett-féle szfericitási teszt

támasztotta alá. Az elemzés statisztikailag is bizonyította, hogy az IT-kockázatok nem olvadnak be a pénzügyi vagy egészségügyi doménekbe, hanem egy önálló látens változóként, külön faktorként jelennek meg a felhasználók kognitív térképén.

- Korrelációelemzés: A szubjektív kockázatpercepció és a tényleges biztonságtudatos magatartás (pl. képernyőzár aktiválása) közötti irányok és erősségek feltárására Pearson- és Spearman-féle korrelációanalízisek szolgáltak.
- Többváltozós regresszióanalízis: A módszertan talán legkritikusabb eleme a regressziós modellek építése volt, amely a „Haszon-domináns döntési architektúra" és a „Biztonságtudatossági paradoxon" igazolását tette lehetővé. A cselekvési valószínűséget (mint függő változót) vizsgáltam az észlelt kockázat és az észlelt haszon (mint független változók) függvényében. A regressziós együtthatók (standardizált β értékek) pontos matematikai összehasonlítása mutatta ki azt a markáns aszimmetriát, mely szerint a haszon ($\beta = 0{,}679$) befolyásoló ereje többszörösen felülmúlja a kockázatét ($\beta = -0{,}125$).
- Varianciaanalízis (ANOVA) és t-próbák: A demográfiai változók, különösen az életkor és a nem (gender) hatásának vizsgálatára a különböző csoportok átlagai közötti statisztikailag szignifikáns különbségeket parametrikus próbákkal elemezte a kutató.

A módszertan korlátai és az eredmények általánosíthatósága

A disszertáció módszertani fejezete reflektál a saját korlátaira is. Egyértelműen elkülönítem a statisztikai és az elméleti általánosíthatóság (external validity) fogalmát. Míg az egyetemi minta statisztikailag nem reprezentálja a teljes társadalmat, a feltárt pszichológiai-döntési mechanizmusok – mint amilyen a kontroll illúziója vagy a haszon-kockázat mérlegelésének strukturális aszimmetriája – alapvető, egyetemes emberi sajátosságok.

Ennek megfelelően a kutatás módszertana nem csupán egy zárt, befejezett rendszert alkot, hanem egy olyan validált, robusztus mérési keretrendszert ad a biztonságtudomány kezébe, amely a jövőben közvetlenül és változatlan formában alkalmazható kiterjesztett vállalati (Kkv és nagyvállalati szektor), valamint rendvédelmi és honvédelmi/katonai populációk kockázatvállalási profiljának feltérképezésére is. Ezzel a disszertáció módszertana hidat képez a pszichometria és az információbiztonsági stratégiaalkotás között.

# 5 Új tudományos eredmények

**T1: Az IT-biztonsági kockázatvállalás mint önálló konstrukció**

Empirikusan kimutattam, hogy az IT-biztonsági kockázatvállalás nem írható le megfelelően a DOSPERT eredeti doménstruktúrájával, és a technikai képzés, valamint az általános kockázatvállalási dimenziók kontrollálása mellett is szignifikáns szerepet játszanak demográfiai tényezők (életkor, nem). Eredményeim alapján az IT-biztonsági kockázatvállalás részben autonóm, kontextus-specifikus konstrukcióként értelmezhető. [P4][P12][P14][P24][P25]

**T2: Az IT-biztonsági kockázatok percepciós pozíciója**

Igazoltam, hogy az IT-biztonsági kockázatok észlelt szintje nem a legmagasabb a vizsgált kockázati területek között, hanem inkább a középmezőnyben vagy annak alsó szegmensében helyezkedik el, ami a digitális kockázatok relatív percepciós alulsúlyozottságára utal. [P2][P5][P6][P8][P16][P17]

**T3: Kockázatpercepció és biztonságtudatos viselkedés kapcsolata**

Empirikusan alátámasztottam, hogy az IT-biztonsági kockázatok magasabb észlelése több esetben szignifikáns, irányhelyes kapcsolatban áll a biztonságtudatos viselkedési gyakorlatok alkalmazásával, ugyanakkor az összefüggések erőssége mérsékelt, ami az attitűd és viselkedés közötti kapcsolat részleges jellegét jelzi. [P3][P13][P15][P18][P19]

**T4: A technikai kompetencia és a szervezeti kockázat viszonya**

Kimutattam, hogy a technikai biztonságtudatosság bizonyos formái BYOD-kontextusban együtt járhatnak szervezeti szempontból kockázatos magatartással, ami a technikai kompetencia és a szervezeti szabálykövetés közötti potenciális strukturális feszültségre utal. [P20][P21][P22][P23]

**T5: Haszon-domináns döntési architektúra az IT-biztonsági döntésekben**

Igazoltam, hogy az IT-biztonsági döntésekben az észlelt haszon hatása szignifikánsan meghaladja az észlelt kockázat hatását, és ez a súlyozási aszimmetria nem kizárólag az IT-biztonsági domén sajátossága, hanem más kockázati területeken is strukturálisan megjelenik. [P1][P7][P9][P10][P11]

# 6 Az eredmények hasznosítási lehetősége

A saját tulajdonú okoseszközök munkacélú használatából eredő biztonsági kihívások kezelése nem maradhat meg a tisztán technológiai megközelítések szintjén. A hagyományos, kizárólag a peremvédelemre és a technikai hard kontrollokra (tűzfalak, titkosítási protokollok, merev szoftveres tiltások, stb.) épülő informatikai stratégiák elégtelennek bizonyultak. A védekezés fókuszpontját át kell helyezni a szocio-technikai rendszer egészére, azon belül is a legkritikusabb és legváltozékonyabb elemre: magára a felhasználóra és a szubjektív döntési mechanizmusaira.

A szervezetek számára komoly nehézséget okoz a humán kockázatok egzakt, számszerűsíthető felmérése. A kutatás által az IT-biztonságra kiterjesztett mérési struktúra lehetővé teszi a vállalatok számára, hogy objektíven feltérképezzék a munkavállalói állomány doménspecifikus kockázatvállalási profilját.

A gyakorlati hasznosítás egyik legfontosabb sarokköve annak elismerése és beépítése a szervezeti folyamatokba, hogy a felhasználók egy markáns, "haszon-domináns döntési architektúra" mentén cselekednek az IT-biztonsági szituációkban. A munkavállalók a kényelmet, a feladatok minél gyorsabb elvégzését, a rugalmasságot és a megszokott digitális felhasználói élményt szinte minden esetben magasabbra értékelik, mint a potenciális adatvesztésből, jogosulatlan hozzáférésből vagy a szervezeti szabályzatok megszegéséből fakadó, gyakran elvontnak tűnő kockázatokat.

Ennek a súlyozási aszimmetriának az egyik legsúlyosabb gyakorlati következménye a szervezeti szabálykerülés, a "Shadow IT" (árnyékinformatika) kiterjedt és rejtett használata. Amennyiben a felhasználók a hivatalos vállalati csatornákat és védelmi megoldásokat túl bürokratikusnak, lassúnak vagy a mindennapi munkát akadályozónak találják, saját, nem engedélyezett és felügyelet nélküli alkalmazásokat, kommunikációs platformokat és felhőtárhelyeket fognak bevonni a vállalati adatok kezelésébe. A hasznosítás elsődleges és legfontosabb lépése tehát ezen alapvető emberi viselkedési mintázatok elfogadása, és az informatikai rendszerek ehhez történő adaptálása a puszta tiltás helyett.

A kutatás korlátai és azok értelmezése. A legfőbb korlátozó tényező a mintavételi eljárásból és a vizsgált populáció összetételéből fakad. A minta gerincét a felsőoktatásban részt vevő, döntően műszaki, mérnöki és informatikai tanulmányokat folytató, technológiailag magasan képzett (az „Y és Z generációhoz” tartozó) fiatalok alkották. Ennek következtében az adatok de-

mográfiai szempontból – életkor, szakmai tapasztalat, iskolai végzettség tekintetében – homogénabb képet mutatnak, és statisztikai értelemben nem tekinthetők reprezentatívnak a teljes hazai aktív munkavállalói rétegre.

Ugyanakkor, a döntéselméleti alapmechanizmusok kontextustól független, egyetemes emberi jellemzők. Továbbá a vizsgált minta tagjai úgynevezett "digitális bennszülöttek", akik magas szintű digitális írástudással rendelkeznek. Ha a biztonságtudatossági paradoxon (a jelenség, amikor a magasabb technikai ismeret nem feltétlenül eredményez óvatosabb magatartást, hanem a "kontroll illúzióján" keresztül a kockázatvállalás növekedéséhez vezet) egy ilyen felkészült rétegnél is dominánsan jelen van, akkor joggal feltételezhető, hogy ez a probléma az átlagos, technológiailag kevésbé képzett felhasználók körében még fokozottabban jelentkezik. A minta specifikuma tehát egyenesen felerősíti a kutatás vezetői relevanciáját, hiszen pontosan a BYOD megoldások legaktívabb jelenlegi és jövőbeni felhasználói bázisának viselkedését modellezi.

A haszon-domináns döntési logika elismeréséből az következik, hogy a szervezeteknek el kell kerülniük a munkavégzést lassító, frusztrációt okozó biztonsági akadályokat. A stratégiai válasz az "alapértelmezett biztonság" (security by default) elvének meghonosítása. A kontrollokat "láthatatlanná", súrlódásmentessé kell tenni a felhasználók számára: a rendszereknek a háttérben kell automatizálniuk a védelmet. Ide tartoznak a folyamatos, felhasználói beavatkozást nem igénylő VPN kapcsolatok, a passzív biometrikus azonosítás, a kontextus-alapú hozzáférés-vezérlés (amely a hálózat és a lokáció alapján dinamikusan, észrevétlenül állítja be a jogosultságokat), valamint a háttérben futó automatikus adattitkosítás. Ha a biztonságos folyamat egyben a legegyszerűbb is, az árnyékinformatika használatának motivációja drasztikusan lecsökken.

A vállalati biztonságtudatossági (awareness) programok hagyományosan uniformizáltak, és a puszta technikai ismeretek átadására (jelszószabályok, adathalász levelek felismerése) koncentrálnak. A biztonságtudatossági paradoxon azonban rávilágít arra, hogy a technikai tréning önmagában kontraproduktív lehet, ha csak növeli a munkavállalók indokolatlan magabiztosságát. A fejezet javaslata az „Awareness 2.0” keretrendszer bevezetése, amely pszichológiai alapokon nyugszik és differenciált. A képzéseket a munkavállaló valós technikai szintjéhez és kockázati profiljához kell igazítani. A technológiailag képzett, IT-affinis "kockázati bajnokokat" nem az alapvető fenyegetésekre, hanem a saját túlzott magabiztosságukból fakadó kognitív torzításokra és a rendszerszintű felelősségre kell oktatni. A tréningeknek interaktívnak és szituációsnak kell lenniük, céljuk a tényleges attitűdformálás és a vállalati biztonsági kultúra elmélyítése.

A vezetőknek stratégiai szinten kell reagálniuk arra a tényre, hogy a BYOD eszközök kikerülnek a vállalati peremvédelem (perimeter defense) alól. Javaslatom a Zero Trust ("Soha ne bízz, mindig ellenőrizz") elvének maradéktalan alkalmazása. A magas egyéni kockázatvállalási hajlandóság miatt a szervezet hálózata nem tekintheti megbízhatónak a felhasználó saját okostelefonját pusztán egy korábbi sikeres hitelesítés okán.

A BYOD technológiai implementációjának fókuszát az eszközök teljes menedzseléséről (MDM - Mobile Device Management) az adatok és az alkalmazások mikroszintű, izolált kezelésére (MAM - Mobile Application Management) kell áthelyezni. A hozzáférés-kezelésnek folyamatosnak és viselkedésalapúnak kell lennie (például UEBA technológiák alkalmazásával). A munkavállaló kizárólag az adott munkafolyamathoz elengedhetetlenül szükséges jogosultságokat kaphatja meg (Least Privilege elv), és a vállalati adatoknak az eszközön belül egy szigorúan elszeparált, titkosított virtuális konténerben kell maradniuk. Ez a mikroszegmentációs megközelítés garantálja, hogy a személyes használat során bekövetkező kompromittálódás (például egy kártékony magánalkalmazás letöltése) ne juthasson át a szervezeti adatterekbe.

# 7 Irodalmi hivatkozások listája/ Irodalomjegyzék

[1] BLAIS Ann-Renée, WEBER U. Elke, A Domén-Specific Risk-Taking (DOSPERT) Scale for Adult Populations, vol. 1, pp. 33-47, 2006. ISSN:1930-2975

[2] KESZTHELYI András, Paradigmaváltás - biztonság - emberi tényező, Taylor : gazdálkodás- és szervezéstudományi folyóirat , vol. 7, no. 1-2, pp. 406-412, 2015. ISSN:2062-1396

[3] MICHELBEGER Pál: Információ-, folyamat- és vállalatbiztonság;. Budapest, Magyarország Óbudai Egyetem, Keleti Károly Gazdasági Kar, 2022. ISBN 978-963-449-289-4

[4] RENN Ortwin: Risk Governance, Coping with Uncertainty in a Complex World;. London Routledge, 2017. ISBN: 978-1-84407-291-0

[5] WEBER U. Elke, BLAIS Renée Ann, BETZ E. Nancy, A Domén-Specific Risk-Attitude Scale: Measuring Risk Perceptions and Risk Behaviors, Journal of Behavioral Decision Making Volume , vol. 15, no. 4, pp. 263-290, 2002. ISSN:1099-0771 DOI:10.1002/BDM.414

# 8 A tézispontokhoz kapcsolódó tudományos közlemények


[P1] FEHÉR-POLGÁR, P., & MICHELBERGER, P. (2018). A sajáttulajdonú mobil eszközök információbiztonsági kockázatai: The information security risks of the BYOD. International Journal of Engineering and Management Sciences, 3(4), 176–185. ISSN: 2498-700X. https://doi.org/10.21791/IJEMS.2018.4.16

[P2] FEHÉR-POLGÁR, P. (2018). BYOD, hozd magaddal a saját biztonsági kockázataid. In P. FEHÉR-POLGÁR (Szerk.), Kutatók éjszakája – Fiatal kutatók előadásai 2018 (p. 9). Óbudai Egyetem Keleti Károly Gazdasági Kar. ISBN: 978-963-449-102-6.

[P3] FEHÉR-POLGÁR, P., & NÉMETH, Z. (2016). Safety consciousness of the mobile phone users. In A. SZAKÁL (Szerk.), Proceedings of the 11th IEEE International Symposium on Applied Computational Intelligence and Informatics (SACI 2016) (pp. 345–348). IEEE. ISBN: 978-1-5090-2380-6. https://doi.org/10.1109/SACI.2016.7507399

[P4] FEHÉR-POLGÁR, P. (2015). Felsőoktatásban tanuló hallgatók biztonságtudatossága. Taylor: Gazdálkodás- és Szervezéstudományi Folyóirat, 7(3-4), 15–21. ISSN: 2676-8917.

[P5] FEHÉR-POLGÁR, P. (2015). A biztonságot veszélyeztető tényezőkkel kapcsolatos attitűdök vizsgálata egyetemi hallgatókon. Taylor: Gazdálkodás- és Szervezéstudományi Folyóirat, 7(1-2), 413–419. ISSN: 2676-8917.

[P6] FEHÉR-POLGÁR, P. (2015). Safety conscious of the students in higher education. In G. KRISTÓVÁ, P. SCHMIDT, J. BRIXOVÁ, & M. SZIVOSOVÁ (Szerk.), Trends and innovations in e-business, education and security: Proceedings of the Fourth International Scientific Videoconference of Scientists and PhD. students or candidates (pp. 8–16). Ekonomická Univerzita v Bratislave. ISBN: 978-80-225-3987-6.

[P7] FEHÉR-POLGÁR, P. (2014). Saját tulajdonú mobilinformatikai eszközök vállalati használatának jogi kérdései. In P. RÁCZ (Szerk.), IESB 2014: Nemzetközi Gépész és Biztonságtechnikai Szimpózium. Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar. ISBN: 978-615-5460-08-1.

[P8] FEHÉR-POLGÁR, P. (2014). Data security of mobile phones, from the aspect of university students. In P. MICHELBERGER (Szerk.), MEB 2014: Management, Enterprise and Benchmarking in the 21st Century (pp. 393–400). Óbudai Egyetem Keleti Károly Gazdasági Kar. ISBN: 978-615-5460-06-7.

[P9] MICHELBERGER, P., & FEHÉR-POLGÁR, P. (2020). BYOD security strategy (Aspects of a managerial decision). Journal of Security and Sustainability Issues, 9(4), 1135–1143. ISSN: 2029-7025. https://doi.org/10.9770/jssi.2020.9.4(1)

[P10] FEHÉR-POLGÁR, P., & MICHELBERGER, P. (2019). The information security risks of the BYOD, from theoretical point of view. In 2019 IEEE 17th International Symposium on Intelligent Systems and Informatics (SISY) (pp. 83–88). IEEE. https://doi.org/10.1109/SISY47553.2019.9111514

[P11] FEHÉR-POLGÁR, P. (2019). Managerial decision options about BYOD with the consideration of shadow IT. In P. SZIKORA & P. FEHÉR-POLGÁR (Szerk.), 17th International Conference on Management, Enterprise, Benchmarking. Proceedings (MEB 2019) (pp. 28–34). Óbuda University Keleti Károly Faculty of Business and Management. ISBN: 978-963-449-127-9.

[P12] FEHÉR-POLGÁR, P. (2020). Examination of IT risk-taking with modified DOSPERT questionnaire among university students. In A. KESZTHELYI, P. SZIKORA, & P. FEHÉR-POLGÁR (Szerk.), 18th International Conference on Management, Enterprise, Benchmarking. Proceedings (MEB 2020) (pp. 48–56). Óbudai Egyetem Keleti Károly Gazdasági Kar. ISBN: 978-963-449-223-8.

[P13] EISEMANN, G., & FEHÉR-POLGÁR, P. (2020). Safety consciousness in future employees. Macrotheme Review: A Multidisciplinary Journal of Global Macro Trends, 9(1), 74–84. ISSN: 2379-9765.

[P14] FEHÉR-POLGÁR, P. (2021). Measuring safetyconsciousness. In A. KELEMEN-ERDŐS, P. FEHÉR-POLGÁR, & A. POPOVICS (Szerk.), FIKUSZ 2021 XVI. International Conference Proceedings (pp. 22–27). Óbudai Egyetem, Keleti Károly Gazdasági Kar. ISBN: 978-963-449-274-0.

[P15] FEHÉR-POLGÁR, P. (2022). Can be the DOSPERT questioner used for measuring IT risk taking. In Á. CSISZÁRIK-KOCSIR, A. POPOVICS, & P. FEHÉR-POLGÁR (Szerk.), FIKUSZ 2022 XVII. International Conference Proceedings (pp. 637–645). Óbudai Egyetem. ISBN: 978-963-449-305-1.

[P16] FEHÉR-POLGÁR, P. (2022). Results upon two samples of university students on safety consciousness in smartphone usage. In Á. CSISZÁRIK-KOCSIR, A. POPOVICS, & P. FEHÉR-POLGÁR (Szerk.), FIKUSZ 2022 XVII. International Conference Proceedings (pp. 123–128). Óbudai Egyetem. ISBN: 978-963-449-305-1.

[P17] FEHÉR-POLGÁR, P. (2023). Testing ICT security risk attitude questions on a small scale level for future use. In M. GARAI-FODOR, Á. CSISZÁRIK-KOCSIR, A. POPOVICS, & T. EDŐCS (Szerk.), XVII. FIKUSZ 2023 International Conference: Proceedings (pp. 362–368). Óbuda University Keleti Károly Faculty of Business and Management. ISBN: 978-963-449-341-9.

[P18] FEHÉR-POLGÁR, P. (2023). Usage of self-assessment questionnaires in safety and security sciences - a literature review. In M. GARAI-FODOR, Á. CSISZÁRIK-KOCSIR, A. POPOVICS, & T. EDŐCS (Szerk.), XVII. FIKUSZ 2023 International Conference: Proceedings (pp. 268–272). Óbuda University Keleti Károly Faculty of Business and Management. ISBN: 978-963-449-341-9.

[P19] FEHÉR-POLGÁR, P. (2023). Alkalmazható-e a DOSPERT kérdőív informatikai kockázatvállalási hajlandóság mérésére? In P. SZIKORA (Szerk.), Társadalom, Informatika és Gazdaság Kutatócsoport Konferencia kiadvány: TIGKONF 2023 (pp. 132–141). Óbudai Egyetem, Keleti Károly Gazdasági Kar. ISBN: 978-963-449-342-6.

[P20] FEHÉR-POLGÁR, P. (2024). IT biztonságtudatosság fontossága. In P. SZIKORA (Szerk.), Társadalom, Informatika és Gazdaság Kutatócsoport Konferencia kiadvány: TIGKONF 2024 (pp. 106–111). Óbudai Egyetem, Keleti Károly Gazdasági Kar. ISBN: 978-963-449-370-9.

[P21] SZIKORA, P., & FEHÉR-POLGÁR, P. (2025). Kiberbiztonsági és felhasználói kihívások a digitális korban: párhuzamok a BYOD és az önvezető autók között. In P. SZIKORA (Szerk.), Társadalom, Informatika és Gazdaság Kutatócsoport Konferencia kiadvány: TIGKONF 2025 (pp. 69–76). Óbudai Egyetem, Keleti Károly Gazdasági Kar. ISBN: 978-963-449-407-2.

[P22] SZIKORA, P., & FEHÉR-POLGÁR, P. (2025). Cybersecurity and user challenges in the digital age: parallels between BYOD and self-driving cars. In P. SZIKORA & A. KESZTHELYI (Szerk.), 23rd International Conference on Management, Enterprise, Benchmarking. Proceedings III. (MEB 2025) (pp. 173–179). Óbuda University Keleti Károly Faculty of Business and Management. ISBN: 978-963-449-386-0.

[P23] FEHÉR-POLGÁR, P., & SZIKORA, P. Domain-Specific Risk Perception in IT Security Decisions: Empirical Examination of the Modified Domain-Specific Risk-Taking (DOSPERT) Framework. (2026). The Eurasia Proceedings of Educational and Social Sciences, 48, 1-7. https://doi.org/10.55549/epess.1006

[P24] FEHÉR-POLGÁR, P., & SZIKORA, P. (in press). Demographic differences in IT security risk-taking: Implications for targeted training and prevention.

[P25] FEHÉR-POLGÁR, P. & SZIKORA, P. (in press). Cross-domain asymmetry in risk–benefit weighting: Evidence for benefit-dominant decision architecture in IT security contexts.