HADMÉRNÖK
VÉDELEMINFORMATIKA
19. évfolyam (2024) 4. szám 183–198.
DOI: 10.32567/hm.2024.4.13

Répás József,[1] Berek László,[2] Bak Gerda,[3]
Oláh Norbert,[4] Ujhegyi Péter[5]

HAIS-Q-tól a SAM-ig, a biztonságtudatosság mérésének modernizációja[6]

From HAIS-Q to SAM: Modernising Security Awareness Measurement

Absztrakt

A kiberbiztonság napjaink egyik legkritikusabb kihívása, amely folyamatos fejlődést és alkalmazkodást követel. A technológia exponenciális fejlődésével párhuzamosan a kibertámadások is egyre kifinomultabbá válnak, fokozva ezzel a veszélyt mind az egyénekre, mind a szervezetekre. Ebben a dinamikusan változó környezetben az információbiztonsági tudatosság kulcsfontosságú, amelynek mérése elengedhetetlen a hatékony védekezési stratégiák kialakításához és a fejlesztendő területek azonosításához.
A biztonságtudatosság mérésére számos eszköz áll rendelkezésre, amelyek közül kiemelkedik a HAIS-Q (Human Aspects of Information Security Questionnaire) modell. Jelen kutatásban egy új elméleti modellt, a SAM (Security Awareness Model) modellt mutatjuk be, amely a HAIS-Q modellre építve, de azt kibővítve és modernizálva közelíti meg a biztonságtudatosság mérését. A SAM hét fő dimenziót vizsgál: autentikáció, internetes szolgáltatások használata, információkezelés, eszközhasználat, incidensmenedzsment, szabályozás és tudatosság.

[1] Gábor Dénes Egyetem, e-mail: repas.jozsef@alverad.hu
[2] Óbudai Egyetem Egyetemi Könyvtár; Óbudai Egyetem Innováció Menedzsment Doktori Iskola, e-mail: berek.laszlo@uni-obuda.hu
[3] Óbudai Egyetem Biztonságtudományi Doktori Iskola, e-mail: bak.gerda@uni-obuda.hu
[4] Debreceni Egyetem Informatikai Kar Adattudomány és Vizualizáció Tanszék, e-mail: olah.norbert@inf.unideb.hu
[5] Óbudai Egyetem Biztonságtudományi Doktori Iskola, e-mail: ujhegyi.peter@uni-obuda.hu
[6] A cikk a TKP2021-NVA-05 számú projekt a Kulturális és Innovációs Minisztérium Nemzeti Kutatási Fejlesztési és Innovációs Alapból nyújtott támogatásával, a TKP 2021 pályázati program finanszírozásában valósult meg.

A SAM-modellre épülő kérdőív 120 kérdést tartalmaz, követve a KAB (Knowledge, Attitude, Behaviour) modellt. Ez a komplex mérőeszköz lehetővé teszi a biztonságtudatosság részletes és sokoldalú felmérését, hozzájárulva ezzel a hatékonyabb kiberbiztonsági stratégiák kialakításához.

Kulcsszavak: Security Awareness Model, kiberbiztonság, adatbiztonság, információbiztonsági tudatosság, kvantitatív mérés

Abstract

Cybersecurity is one of the most critical challenges of our time, requiring continuous evolution and adaptation. As technology evolves exponentially, cyberattacks has become more sophisticated, increasing the threat to individuals and organisations. In this dynamically changing environment, security awareness is crucial, and its measurement is essential to developing effective protection strategies and identifying areas for improvement.
Several tools are available to measure security awareness, most notably the HAISQ (Human Aspects of Information Security Questionnaire) model. The present research proposes a new SAM (Security Awareness Model), which builds on the HAISQ model and significantly extends and modernises its approach to measuring security awareness. The SAM examines seven main dimensions: authentication, use of internet services, information management, use of devices, incident management, regulation and human awareness.
The questionnaire based on the SAM model contains 120 questions, following the KAB (Knowledge, Attitude, Behaviour) model. This complex measurement allows a detailed and multifaceted security awareness assessment, contributing to the development of more effective cybersecurity strategies.

Keywords: Security Awareness Model, cybersecurity, security of data, security awareness, quantitative measurement

Bevezetés

Az infokommunikációs technológiák rohamos fejlődése napjainkban nem csupán a digitális jólét megteremtésével jár együtt, hanem egyúttal a polgári lakosság jólétét, kényelmét is elősegítheti. Az információtechnológia fejlődése az egyértelmű előnyei mellett azonban óriási kockázatot is hordoz, amennyiben nem tudatosan használják, így kiemelt figyelmet kell fordítani a lakosság digitális immunitásának erősítésére. Ahogy a digitális eszközök és rendszerek elterjedésével párhuzamosan növekszik a kibertámadások száma és kifinomultsága, új kihívások jelennek meg az egyének és a szervezetek életében. Számos kiberbűncselekmény által okozott kár mértéke, illetve a fejlődő technológia, a szabályozói oldal reaktív természete és a kiberbűnözők által használt újabbnál újabb megoldások is növelik a téma jelentőségét. Kiemelendő, hogy a kiberbűncselekmények okozta negatív hatások a vállalatok esetében az anyagi károkon túl fogyasztói elpártolást, reputációveszteséget és a versenytársak erősödését

is eredményezheti.[7] Így többek között az információbiztonsági tudatosítás egyre fontosabb feladattá válik hazai és világszinten,[8] és fokozott aktivitást igényel Magyarország állampolgárai és a társadalom különböző szereplői esetében is, annak érdekében, hogy a mindennapok részévé váló digitális eszközök és szolgáltatások biztonságos használata el legyen sajátítva. Sokszor azonban nem elegendő csupán az egyének információbiztonsági tudatosságát növelni, hanem a tudásukat is erősíteni szükséges a témában, illetve akár az információbiztonsági kultúra kialakítására, formálására is szükség lehet.[9] Bár a kutatók és a gyakorlati szakemberek folyamatos erőfeszítéseket tesznek ezen a területen, munkájukból gyakran hiányzik a „biztonságtudatosság" fogalmának egységes meghatározása,[10] illetve a különböző tanulmányok ellentmondásos megközelítést alkalmaznak abban a kérdésben, hogy szükséges-e különbséget tenni például a biztonságtudatosság és a biztonsági képzés között. Az Egyesült Államok Nemzeti Szabványügyi és Technológiai Intézete (NIST) által meghatározott biztonságtudatossági definíció a következőket mondja ki: „A tudatosság nem képzés. A tudatossági tréningek célja, hogy a figyelmet a biztonsági intézkedésekre és alkalmazásukra irányítsa. Emellett cél még, hogy az egyének felismerjék az informatikai biztonsággal kapcsolatos aggályokat, és ennek megfelelően reagáljanak."[11] A NIST SP 800-16 szerint a tudatosság megteremti a munkavállaló érzékenységét a számítógépes rendszerek fenyegetései és sebezhetőségei iránt, valamint annak felismerését, hogy az adatokat, az információkat és az azok feldolgozására szolgáló eszközöket védeni kell.[12] Az információbiztonsági tudatosság programok alapvető értéke, hogy a szervezeti kultúrát befolyásoló attitűdváltozást előidéző szemléletváltás révén megalapozzák a képzést. Jelen cikkünkben az információbiztonsági tudatosságot egy olyan adaptív folyamatként definiáljuk, amely reagál a környezeti és technológiai változásokra. A cél az, hogy növelje az egyének és szervezetek érzékenységét az információbiztonsági kockázatokkal kapcsolatban, miközben figyelembe veszi a folyamatosan változó környezet kihívásait és lehetőségeit. Az információbiztonsági tudatosság magában foglalja a releváns ismeretek, attitűdök, készségek és viselkedésformák folyamatos fejlesztését, lehetővé téve a résztvevők számára, hogy alkalmazkodjanak az új fenyegetésekhez és technológiai megoldásokhoz. Mivel a hagyományos, tisztán technológiai megközelítések már nem elegendők, valamint az információbiztonsági incidensek jelentős része emberi hibára vezethető vissza, egyre nagyobb hangsúlyt kap az emberi tényező szerepe, és a biztonságtudatosság mérése során kiemelt figyelmet kell fordítani az egyénekre.[13] Az emberi tényezők vizsgálata nemcsak a szervezeti biztonság szempontjából kulcsfontosságú, hanem abban is segít, hogy feltárjuk azokat az ok-okozati összefüggéseket, amelyek hozzájárulnak a biztonsági kockázatok kialakulásához. A biztonsági kockázatok beazonosítása és csökkentése rendszeres formális auditok segítségével minimalizálható, azonban ezek gyakran időigényesek

7 Modi et al. 2014; Jeong et al. 2019.
8 ENISA 2019.
9 Safa et al. 2015.
10 Hänsch et al. 2014.
11 Wilson et al. 1998.
12 Wilson et al. 1998.
13 Sangwan 2024; Rohan et al. 2021.

és drágák.[14] Ezenkívül külön figyelmet igényel az etikai és jogi félreértések elkerülése (például a behatolásvizsgálat során okozott kár).[15]

A cikk második fejezetében áttekintjük az elmúlt évek kutatásait, amelyek foglalkoztak a digitális transzformáció sikerességének feltételeivel és az információbiztonság szervezeti aspektusaival. Ezek a vizsgálatok rámutattak, hogy a technológiai fejlesztések mellett legalább olyan fontos a megfelelő szervezeti kultúra és viselkedési minták kialakítása. A harmadik fejezet a SAM elméleti modell bemutatására fókuszál, ismertetve annak alapvető felépítését és relevanciáját. Ezt követően a negyedik fejezet célja az elméleti modell dimenzióinak alátámasztása, amely szakirodalmi hivatkozások és korábbi kutatások eredményei alapján történik meg. Végül az összegzésben összefoglaljuk a főbb megállapításokat, kiemelve a SAM modell jelentőségét, valamint annak lehetséges alkalmazási területeit és jövőbeli kutatási irányait.

Tudományos megközelítés és a kapcsolódó modell

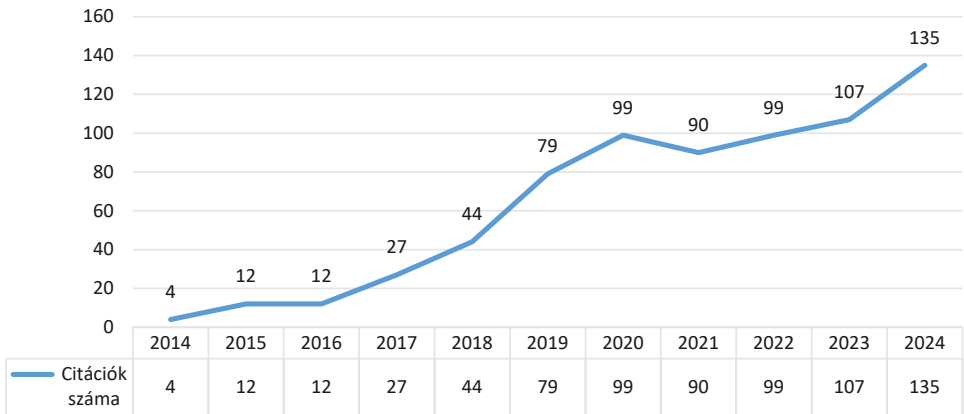
Az információbiztonsági tudatossági szint mérésére kiemelt figyelem irányult mind nemzetközi, mind hazai szinten az elmúlt évtizedekben. A 2010-es évek releváns kutatási eredményeinek szisztematikus áttekintése szerint a kutatócsoport fő iránya a kutatások során alkalmazott felmérések adatgyűjtési és kiértékelési módszerei, a célcsoportok megoszlása, illetve az azonosított biztonságtudatossági paraméterek és a témához kapcsolódó terminológiai változások feltérképezése volt.

A szakirodalmi kutatás során a Web of Science és a Scopus adatbázisokban indexelt, elmúlt 10 évben megjelent releváns publikációk közül a 100 legtöbb citációval rendelkezőt tekintettük át. Ennek során a cím és az absztrakt alapján, majd a teljes szöveg vizsgálatával tudtuk tanulmányozni a korábbi kutatások legfontosabb, témánk szempontjából releváns jellemzőit.[16]

Az adatgyűjtési módszerek vonatkozásában jól látható, hogy a kutatások túlnyomó része kérdőívet használt, a fellelt 37 publikációban mindössze 3 esetben alkalmaztak interjút.[17] Ezek a kutatások mindegyike céges környezetben vizsgálta a biztonságtudatosságot. A mintában szereplő többi, az egyén biztonságtudatosságára vonatkozó felmérés mindegyikében kérdőíves adatgyűjtés szerepelt. A vizsgált publikációkban a legtöbb esetben saját összeállítású, illetve korábbi kutatásokban használt kérdőívek részeiből felépített kérdőíveket alkalmaztak. A publikációk közül 6 esetben találtunk olyan kutatást, amelyben a HAIS-Q (Human Aspects of Information Security Questionnaire) kérdőívet használták.[18] További 4 publikációban hivatkoztak a HAIS-Q-ra. A szakirodalmi mintánkban nevesített kérdőívként egyedül a HAIS-Q szerepelt, és ezekben a kutatásokban egyenlő arányban voltak a kizárólag egyénre vonatkozó, illetve céges környezetben végzett felmérések.

[14] *National Data Guardian for Health and Care: Review of Data Security, Consent and Opt-Outs* 2016.
[15] Yeo 2013.
[16] Bak et al. 2024; Berek et al. 2024.
[17] Ali et al. 2020; Diesch et al. 2020; Kessler et al. 2020.
[18] Parsons et al. 2014; McCormac et al. 2017; Parsons et al. 2017.

Ezt követően a HAIS-Q három „alap" publikációja[19] idézettségének vizsgálata történt meg. A három publikáció citációinak száma a Scopus adatbázisban 734. Természetesen ez csak a Scopus által indexált tartalmakban található idézettséget mutatja, de ebből a kimutatásból jól látható, hogy a publikációk „minőségi szegmensében" a mai napig meghatározó felmérési módszerről beszélünk (1. ábra).



1. ábra: HAIS-Q citációk a Scopus adatbázisban, 2014–2024
Forrás: a szerzők szerkesztése

A három publikáció idézettségének időbeli megoszlásából jól látható, hogy szinte folyamatosan nő a hivatkozások száma. Az is beszédes adat, hogy az összes 734 idézőből 2024 során 135 publikációban hivatkoztak a három folyóiratcikk valamelyikére.

A Web of Science és a Scopus adatai mellett természetesen egy tágabb, nem feltétlen a legmagasabban jegyzett kiadványokban megjelenő publikációkat tartalmazó adatbázisban is lefolytattuk a keresést. A GoogleScholarban bár – adatszinten – szerepelnek azok a publikációk is, amelyeket a két nagy tudományos adatbázis indexel, de ezek mellett alacsonyabban rangsorolt folyóiratok, konferenciaközlemények is megtalálhatók. A GoogleScholar adatai alapján a három HAIS-Q cikk hivatkozásainak száma: 1489. Ezt követően HAIS-Q-ra vonatkozó keresést indítottunk a GoogleScholar felületén, amelynek eredménye 974 olyan publikáció volt, amelyben a „HAIS-Q" kifejezés szerepelt.

Látható, hogy a HAIS-Q széles körben hivatkozott eszköz, amely 7 területen, 63 elemmel vizsgálja a biztonságtudatosság kapcsán a felhasználói viselkedést, tudást és attitűdöt. A HAIS-Q áttekintését követően elmondható, hogy annak kérdései, témái nem feltétlen felelnek meg napjaink kiberbiztonsági kihívásainak, több hiányosságot azonosítottunk.

Ilyen hiányosság például az autentikáció területén az, hogy csak a jelszófaktoron alapuló hitelesítést vizsgálja, amely napjaink biometrikus és kétfaktoros megoldásaiban már kisebb súlyt reprezentál. Ezzel a témával az elmúlt években egyre több kutató

[19] Parsons et al. 2014; McCormac et al. 2017; Parsons et al. 2017.

foglalkozik különböző szempontból vizsgálva a kérdést.[20] Emellett a mesterséges intelligencia dinamikus fejlődése miatt egyre inkább részévé válik mindennapi életünknek, amely területtel értelemszerűen a HAIS-Q 2014-ben még nem foglalkozott. A mesterséges intelligencia az elmúlt években egyértelműen az egyik legforróbb téma volt, természetesen a technológia elfogadottságával, humán vonatkozásaival is sok kutatás foglalkozott.[21] A HAIS-Q kérdőív hiányosságai közé tartozik még a felhőbiztonság az IoT-eszközök szintjén, ami a biztonságtudatosság egyre fontosabb területe.

A kérdőív mindenképpen aktualizálásra, frissítésre szorult, azonban az alkalmazott modell nagyon jól használható a biztonságtudatossággal kapcsolatos felmérés során. A HAIS-Q kérdőív továbbfejlesztése során érdemes figyelembe venni a viselkedésváltozás elméleti megközelítéseit is, hiszen a biztonságtudatosság nem csupán a tudás meglététől, hanem az attitűdök és a viselkedésformák alakulásától is függ. Ebben nyújt hasznos keretet a KAB (Tudás, Attitűd, Viselkedés) modell, amely széles körben alkalmazott elméleti alap a viselkedésváltozás megértésére és előmozdítására. A modell azt hangsúlyozza, hogy a viselkedés megváltoztatásához szükség van a kapcsolódó tudás, attitűdök és készségek együttes fejlesztésére. A tudás magában foglalja a megfelelő információk és készségek elsajátítását, az attitűd a hozzáállás és meggyőződések módosítását, míg a viselkedés a kívánt cselekvések végrehajtására való képességet jelenti. A modell szerint e három tényező összehangolt fejlesztése kulcsfontosságú ahhoz, hogy a célzott viselkedésváltozás hosszú távon fenntartható legyen. A KAB modellt széles körben alkalmazzák az egészségügyi felvilágosítástól a szervezeti fejlesztésekig, mivel átfogó keretet nyújt a komplex emberi viselkedés megértéséhez és befolyásolásához.

A KAB modell szakirodalmi vizsgálata azt mutatja, hogy a modell alkalmazhatósága, megfelelősége szempontjából a kutatók eltérően értékelik: Hermawan et al. (2022) és An et al. (2022) szerint a tudás és viselkedés erősen kapcsolódik egymáshoz.[22] Egyes kutatások élesen bírálták a modellt, mert az az érzelmi és szituációs tényezőket nem veszi figyelembe: Kollmuss és Agyeman (2002) és Baranowski et al. (2003) kutatása szerint több olyan viselkedést befolyásoló tényező van, amelyet a KAB modell figyelmen kívül hagy.[23] A modell hatékonyságát csak akkor lehet megbízhatóan értékelni, ha a vizsgált változókat világosan meghatározzák, és azok kapcsolata a viselkedésváltozás folyamatával összefüggésbe állítható. A releváns eredmények elérése érdekében a modell használatakor figyelembe kell venni a viselkedést befolyásoló összetett tényezőket.

Modell

Az előző fejezetben áttekintett szakirodalom és az általa bemutatott empirikus kutatások feltárt összefüggései alkotják annak az elméleti modellnek az alapját, amely

[20] Srinivasan 2023; Mujeye 2021; Gokulkumari 2020; Buckley et al. 2019.
[21] Kaya et al. 2024; Stein et al. 2024; Kelly et al. 2023.
[22] Hermawan et al. 2022.
[23] Kollmuss–Agyeman 2002; Baranowski et al. 2003.

lehetővé teszi az információbiztonsági tudatosság komplex vizsgálatát, hidat teremtve a tudományos megállapítások és az aktuális gyakorlati alkalmazások között.

A modell célkitűzése az információbiztonsági tudatosság felmérése, amelynek alapját a KAB modell és a HAIS-Q modernizált dimenziói képezik. Az elméleti modellhez javasolt kérdőív a tudás, attitűd és viselkedés dimenzióinak felmérését valósítja meg, ahol az új állítások figyelembe veszik a legújabb információbiztonsági kihívásokat, például a kibertámadások egyre kifinomultabb fenyegetéseit és a hozzájuk kapcsolódó védelmi kontrollokat. Mivel a korszerűsített kérdőív nemcsak az egyén elméleti tudására fókuszál, hanem részletesen feltárja az attitűdöket, a kockázatészlelést és a tényleges biztonsági magatartásmintákat is, így lehetővé válik egy többdimenziós értékelés, amelynek segítségével azonosíthatók a kitöltő információbiztonsági tudatosságának erősségei és fejlesztendő területei.

Az általunk javasolt Security Awareness Measurement (SAM) az információbiztonsági tudatosság holisztikus mérési módszerére kifejlesztett 120 tételből álló eszköz, amelyet a 2. ábra mutat be. A SAM hét fókuszterületet értékel, nevezetesen a hitelesítési módszereket, az internetes alkalmazásokat és szolgáltatásokat, az információkezelést, az eszközöket, az incidensmenedzsmentet, a szabályozást és a tudatosságot. Egyes fókuszterületek további aldimenziókra oszthatók, amelyek tartalmazzák az új szempontokat (például az új autentikációs megoldásokat). Minden egyes fókuszterület esetén meg vannak adva állítások, ahol egy ilyen állítás a tudás, attitűd és viselkedés hármasát kérdezi le. A kérdőív összesen 40 állítást tartalmaz, így a tudás-, az attitűd- és viselkedéselemek 120 tételt adnak vissza. A SAM kérdőív elérhető az alábbi GitHub-linken.[24]

Az alábbi szakaszban áttekintést nyújtunk először az információbiztonsági kérdőívek evolúciójáról, majd a SAM fejlesztéséről, finomításáról és használatáról, amelyet az 1. és a 2. táblázatban foglalunk össze.

Az információbiztonsági tudatosság mérésére az évek során számos kérdőív készült, amelyek folyamatos fejlődésen mentek keresztül. A korai modellek még az egyéni biztonsági szokásokra fókuszáltak, míg az újabb kérdőívek egyre átfogóbb, strukturáltabb megközelítést alkalmaznak. A kontingenciaelmélet alapelvei a SAM esetében jelennek meg, amely figyelembe veszi a környezeti és technológiai változásokhoz való alkalmazkodás szükségességét.

A táblázatban felsorolt kérdőíveket azért választottuk ki, mert jelentős mérföldköveket jelentenek az információbiztonsági tudatosság kutatásában. A Kruger & Kearney által kidolgozott első modell megteremtette az alapokat, míg a HAIS-Q egy strukturáltabb, tudás–attitűd–viselkedés megközelítést alkalmazott. Az ISCA a szervezeti szintű biztonsági kultúra elemzésére fókuszált, a SeBIS pedig az egyéni biztonsági szokások mérése felé tett fontos lépést. A legújabb SAM modell a kontingenciaelmélet alkalmazásával biztosít egy adaptívabb és szélesebb körű mérési keretet.

[24] Lásd: https://github.com/ONorbert1991/SAM-kerdoiv

1. táblázat: Információbiztonsági tudatosság kérdőívek fejlődése

Kérdőív	Fejlesztés éve	Kulcsterületek	Felépítés	Újítások
Information Security Awareness Questionnaire (Kruger & Kearney)	2006	Politikai megfelelés, jelszókezelés, adathozzáférés, fenyegetések ismerete	Tudás, attitűd és viselkedés szerinti bontás	A biztonságtudatosság háromdimenziós megközelítése
Information Security Culture Assessment (ISCA) (Da Veiga & Eloff)	2010	Szervezeti információbiztonsági kultúra, munkavállalói viselkedés, szabályzatok betartása	Többdimenziós elemzés, szervezeti szintű megközelítés	Az információbiztonság kultúrájának átfogó vizsgálata szervezeti kontextusban
Human Aspects of Information Security Questionnaire (HAIS-Q) (Parsons et al.)	2014	Jelszóhasználat, e-mailek és adathalászat, internetes viselkedés, munkahelyi biztonság, mobilbiztonság	Tudás, attitűd és viselkedés alapú értékelés	Átfogó, strukturált mérési eszköz az egyéni biztonságtudatosságra
Security Behavior Intentions Scale (SeBIS) (Egelman & Peer)	2016	Jelszóbiztonság, szoftverfrissítések, eszközvédelem, biztonságtudatos viselkedés	Önbeszámolós kérdések skálázott válaszokkal	Magánszemélyek biztonsági viselkedési hajlandóságának mérése
Security Awareness Measurement (SAM)	2025	Hitelesítési módszerek, internetes alkalmazások és szolgáltatások, információkezelés, eszközök, incidensmenedzsment, szabályozás, tudatosság	40 állítás, mindegyik tudás, attitűd és viselkedés szerint bontva (összesen 120 tétel)	A kontingenciaelmélet alapján fejlesztett kérdőív, amely figyelembe veszi a technológiai és környezeti változásokat

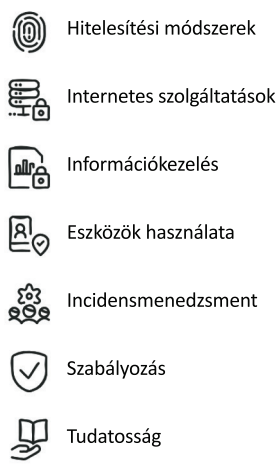
Forrás: a szerzők szerkesztése

2. táblázat: SAM modell fejlesztési lépései

Lépés	Leírás	Eredmény
Tudományos szakirodalom feldolgozása	Átfogó irodalomkutatás az információbiztonsági tudatosság mérésére alkalmazott módszerekről. A meglévő modellek, például a KAB (Knowledge, Attitude, Behaviour) vizsgálata	A mérési keretek, dimenziók és megközelítések azonosítása; a HAIS-Q alapjainak megértése
HAIS-Q modell beazonosítása	A HAIS-Q (Human Aspects of Information Security Questionnaire) vizsgálata és a KAB modellhez való illeszkedésének elemzése	A HAIS-Q hiányosságainak feltárása, például az új technológiákra való korlátozott alkalmazhatóság
HAIS-Q továbbfejlesztése	Az eredeti modell új dimenziókkal és kérdésekkel való kiegészítése. Az új területek közé tartozik a felhőalapú adattárolás biztonsága, a modern autentikációs megoldások és a szabályozási megfelelés	Az új SAM modell létrehozása, amely a HAIS-Q modernizált és bővített változata

Lépés	Leírás	Eredmény
Modernizálás keretének meghatározása	Az információbiztonsági kihívásokra való adaptáció főbb alapelveinek kialakítása, például a dinamikus technológiai változásokra való reagálás szükségessége	Az új kérdőív strukturális alapjai, amelyek igazodnak a mai környezet követelményeihez
Kontingenciaelmélet alkalmazása	A kérdőív alkalmazhatósága a kontingenciaelmélet alapján, amely hangsúlyozza a környezeti és technológiai változásokhoz való alkalmazkodás fontosságát	A kérdőív elméleti alapjainak megerősítése, amely rugalmas keretet biztosít a különböző szervezeti helyzetekhez való igazodáshoz

Forrás: a szerzők szerkesztése



2. ábra: A SAM fő dimenziói
Forrás: a szerzők szerkesztése

Az új területek adaptálását (például modern autentikációs megoldások, webes alkalmazásokkal kapcsolatos biztonsági elemek, tudatosság fejlesztése és kiterjesztése, illetve a napjaink szabályozási kérdésköre) az alábbi szempontok alapján alakítottuk ki.

Jelenleg az emberi tényezőkre jelentős nyomás helyeződik, ugyanis a hatékony információbiztonság nem csupán a technikai eszközökön múlik, hanem a felhasználók tudatosságán, szokásain és viselkedésén is, ami a KAB modellel továbbra is jól leképezhető.

Az autentikációs megoldások között a jelszavak relevanciája és szerepe továbbra is központi jelentőségű, bár a digitális világ egyre fejlettebb hitelesítési módszerei mellett gyakran vitatják hatékonyságukat.[25] A jelszavak napjainkban még mindig a rendszereink alapvető védelmi vonalát képezik, ugyanakkor a kizárólag jelszavakra támaszkodó védelem már nem elegendő a korszerű kiberfenyegetésekkel szemben. A HAIS-Q elsősorban az egyszerű jelszókezelési elvekre összpontosít, de nem veszi figyelembe a napjainkban egyre szélesebb körben alkalmazott többfaktoros hitelesítés (MFA) vagy jelszó nélküli autentikációs megoldások (például biometrikus azonosítás, hardveres

[25] Weber et al. 2008; Taneski et al. 2014; Wang et al. 2023.

tokenek) összetettségét.[26] A modern rendszerek esetében az autentikáció már nem csupán a jelszavak biztonságos megválasztásáról szól, hanem a hitelesítési folyamatok holisztikus megértéséről, valamint a felhasználók képességéről, hogy helyesen alkalmazzák az új technológiákat. Ezért az új megoldások, különösen a többfaktoros hitelesítés (MFA) alkalmazása, a biztonság új alappillérévé vált. Egyes elemzések azt mutatják, hogy a többfaktoros hitelesítés a fiókfeltörési támadások több mint 99,9%-át képes blokkolni.[27] Az MFA nemcsak technikai előnyt kínál, hanem rávilágít a felhasználók és a rendszerek közötti interakciók komplexitására is. Az ilyen megoldások hatékonysága azonban nagyban múlik azon, hogy a felhasználók megértik-e ezek működését, és elkötelezettek-e azok alkalmazása iránt (technológiai elfogadottság).[28]

A HAIS-Q internethasználatának dimenziója mér bizonyos böngészés közben felmerülő fenyegetéseket, azonban ezen a területen elkerülhetetlen, hogy a nyilvánvaló veszélyeken túl (mint az adathalász e-mailek) a preventív és a proaktív védekezési intézkedések is bekerüljenek az információbiztonsági tudatosság mérésébe. Ilyen intézkedések lehetnek a TLS- (Transport Layer Security) protokollt nem használó oldalakkal kapcsolatos óvatos felhasználói magatartás, a rosszindulatú bővítmények vagy a drive-by download támadások kockázatainak minimalizálása, a böngésző naprakészen tartása, a cookie-kezelési szabályok betartása vagy a privát böngészési lehetőségek alkalmazása. A webes biztonság aldimenzió hozzáadása a modellhez és külön vizsgálata kulcsfontosságú, mivel az internetes böngészés és a hozzá kapcsolódó kockázatok alapvető részei manapság a munkahelyi tevékenységeknek. A munkavállalók gyakran látogatnak külső weboldalakat információkeresés vagy üzleti kommunikáció céljából, és ezek az interakciók számos biztonsági fenyegetést hordozhatnak.[29] A kérdőív kapcsolódó állításaival megvizsgáljuk, az egyének képesek-e felismerni a nem biztonságos webhelyeket, tudják-e, milyen lépéseket kell tenniük, ha webes sérülékenységet látnak, és miért fontos a titkosítás az online vásárlások során.

Az internetes alkalmazások, különösen a felhőalapú szolgáltatások és kollaborációs platformok (Google Drive, Microsoft Teams, Slack stb.) használata napjaink egyik releváns kihívása. A digitalizáció rohamos térnyerése és a külső események (például Covid-járvány) tovább erősítették e platformok elterjedését és használatát. A HAIS-Q nem veszi figyelembe azokat a dinamikus és összetett adatmegosztási, jogosultságkezelési vagy incidenskezelési gyakorlatokat, amelyek ezeknél az alkalmazásoknál kiemelkedően fontosak. A felhő után a felhasználók mesterséges intelligencián alapuló alkalmazásokkal és rendszerekkel való kapcsolatát vizsgáljuk, kitérve arra, hogy tudatában vannak-e a potenciális biztonsági kockázatoknak, például az adatfeldolgozási torzításoknak vagy az automatizált döntések manipulálhatóságának. E hiányosságok különösen relevánsak a mai információbiztonsági környezetben, ahol a mesterséges intelligencia és a felhőalapú technológiák széles körben alkalmazott megoldásokká váltak. Az ezekhez kapcsolódó tudatosság hiánya jelentős kockázatok forrása lehet, ezért az új kérdőívbe feltétlenül integrálni kellett ezeket a területeket az elméleti modellben.

[26] Otta et al. 2023; Almadani et al. 2023.
[27] Hess et al. 2021.
[28] Ometov et al. 2018.
[29] Kashevnik et al. 2020.

A szabályozás dimenziójának integrálása az elméleti modellbe a GDPR, NIS2 és más globális adatvédelmi szabályozások megjelenésével áll összefüggésben.[30] Ezek az előírások nemcsak a személyes adatok felelős kezelését, hanem a szervezeti szinten alkalmazott biztonsági gyakorlatok harmonizálását is megkövetelik. Egy információbiztonsági tudatossági kérdőív számára a szabályozások értékelése azért kritikus, mert lehetővé teszi annak vizsgálatát, hogy az egyének és szervezetek mennyire értik és tartják be a vonatkozó jogi előírásokat, például az adattárolási vagy adatfeldolgozási folyamatokra vonatkozó szabályokat. E dimenzió figyelembevétele elősegíti a megfelelési kockázatok csökkentését, miközben megteremti a szabályozás és a gyakorlat közötti harmóniát.[31] A szabályozási ismeretek felmérésével a cél, hogy az elméleti modell a későbbi empirikus vizsgálatokkor megmutassa, hogy a felhasználók mennyire ismerik ezeket az előírásokat, illetve hogyan alkalmazzák őket a mindennapi munkafolyamatok során. Ez nemcsak a jogi megfelelőség biztosítása szempontjából fontos, hanem hozzájárul a szervezet reputációjának és biztonsági színvonalának fenntartásához is. A változó technológiai és a szabályozási környezethez való alkalmazkodás létfontosságú a versenyképesség és a hatékonyság érdekében, amely indokolja az aktuális jogi és üzleti követelményeken túl az általános megfelelőség és harmadik felek menedzselésének szabályozásait is.

A tudatosság dimenzió kiemelt szerepe abban rejlik, hogy a felhasználók biztonsági attitűdje és viselkedése alapvetően befolyásolja a szervezetek kockázatának alakulását.[32] A digitális világ gyors fejlődése megköveteli, hogy az alkalmazottak tisztában legyenek az információbiztonság alapelveivel és azzal, hogyan védekezhetnek a legújabb fenyegetések ellen. A humán faktornak ez a szerepe továbbra is meghatározó az információbiztonság területén, így elengedhetetlen a mérése, valamint a beépítése.[33] A biztonságtudatosságot holisztikus megközelítésben vizsgálva az emberi tűzfal *(human firewall)* fogalma kerül előtérbe. Az Awareness Continuum Management Model (ACM2) alkalmazásával látható, hogyan lehet az alkalmazottak viselkedését proaktívabbá és tudatosabbá tenni, ezzel minimalizálva az emberi hibából eredő kockázatokat.[34] Az elméleti modell kialakítása során ez a dimenzió szolgál arra, hogy a felhasználók mennyire értik a biztonságtudatos magatartás jelentőségét, és milyen mértékben képesek ezt a mindennapi helyzetekben alkalmazni. Az egyének és a szervezetek akkor működnek hatékonyan és megbízhatóan, ha képességeik és erőforrásaik alkalmazkodnak a környezet által támasztott igényekhez. Ennek megfelelően a tudatosság dimenziójának vizsgálata hozzájárul a szervezeti kiberreziliencia növeléséhez, miközben biztosítja, hogy a mérési eszköz a változó fenyegetési környezethez igazodva maradjon releváns.

Az új elméleti modellt lefedő kérdőívstruktúra tehát nemcsak az új technológiákhoz és kihívásokhoz igazodik, hanem figyelembe veszi a modern szervezeti környezetek dinamikáját és a humán tényezők folyamatos változását is. Ez a megközelítés lehetőséget nyújt arra, hogy az információbiztonságot átfogóbb módon mérjük és értékeljük.

[30] Bakare et al. 2024; Reis et al. 2024.
[31] Bamberger et al. 2010.
[32] Rohan et al. 2021.
[33] Sangwan 2024.
[34] Koza 2022.

Eredmények

Szakirodalmi áttekintésünk a mérésre használt módszerek feltérképezésén túl kiterjedt a kapcsolódó kutatások számának alakulására, tudományterületi és országok szerinti megoszlására, valamint a kulcsszavak változására és fejlődésére. Az eredmények alapján egyértelmű, hogy a biztonságtudatosság kutatása egyre fontosabbá válik, a kutatások specializálódnak, és a terület egyértelműen bővülni fog. A vizsgált kutatásokban foglalkoztak az emberi információbiztonsági tudatosság, viselkedés és szabálykövetési hajlandóság közötti összefüggésekkel, valamint a befolyásoló tényezőkkel. A kutatásokban megjelenő tényezőket emberi (ismeretek, tapasztalatok, attitűd, motivációk), környezeti (munkahelyi kultúra, normák, technológia, társadalmi elvárások), technológiai (biztonsági megoldások és eszközök) és oktatási/képzési (képzés, tréning) tényezőkre lehet csoportosítani. A HAIS-Q felmérésén alapuló, kibővített kérdőívünk ezeket a tényezőket figyelembe véve készült el.

A kérdőív bevezetése után a kontingenciaelmélet vált az eszköz működésének és relevanciájának elméleti magyarázatává, amely keretet biztosított a kérdőív alapelveinek és alkalmazkodási képességeinek értelmezéséhez. A kontingenciaelmélet segít megvilágítani, hogy ezek az új dimenziók és változtatások hogyan reflektálnak környezeti feltételekre és az aktuális technológiai elvárásokra.

A kontingenciaelmélet tehát keretet adott az új kérdőív indoklásához, és megmagyarázza, hogy miért van szükség a mérési eszköz folyamatos fejlesztésére és adaptálására. Az elmélet hangsúlyozza, hogy a hatékony mérési eszközöknek illeszkedniük kell a dinamikusan változó technológiai környezethez, és tükrözniük kell a releváns fenyegetéseket és alkalmazási területeket. Az új kérdőív ezen elvárások szerint lett kialakítva, amit a kontingenciaelmélet rendszerbe foglalva megmagyaráz.

Jövőbeli tervek

A SAM kérdőív fejlesztésének következő lépése az elméleti modell empirikus alátámasztása, amely jelenleg a meglévő kulcsszóelemzésre és a szakirodalomban elérhető empirikus adatok statisztikai vizsgálatára épül. A jelenlegi adatelemzés betekintést nyújt az információbiztonsági tudatosság dimenzióiba, azonban ezek megerősítéséhez további nagymintás vizsgálatok szükségesek. Ennek érdekében online kérdőíves felmérést tervezünk, amelyet egy közvélemény-kutató cég bevonásával szeretnénk megvalósítani, biztosítva a reprezentatív minta elérését. Az így gyűjtött adatok lehetővé teszik a SAM modell statisztikai validációját, különös tekintettel a dimenziók közötti összefüggésekre és azok prediktív erejére, megerősítve a kérdőív gyakorlati alkalmazhatóságát.

Összegzés

A kiberbiztonság napjainkban kiemelkedő fontosságú, hiszen nélkülözhetetlen a személyes adatok, üzleti információk és kritikus infrastruktúrák védelméhez, miközben a kibertámadások

egyre gyakoribbá és kifinomultabbá válnak. Ebben a környezetben a biztonságtudatosság segít az embereknek felismerni a potenciális fenyegetéseket és hatékony lépéseket tenni azok megelőzésére. Az egyre digitalizáltabb világban a felhasználók viselkedése és döntései alapvetően befolyásolják a rendszerek és adatok védelmét, ezért elengedhetetlen a tudatosság szintjének mérése. Ezáltal azonosíthatók azok a területek, ahol további képzésre vagy szabályozásra van szükség a kiberbiztonsági kultúra erősítése érdekében. Egy felkészült és tudatos társadalom pedig jelentősen csökkentheti a kibertámadások sikerességét, hozzájárulva a digitális biztonság fenntartásához.

A biztonságtudatosság mérésére számos eszköz létezik, amelyek közül kiválasztottuk a HAIS-Q modellt. Manapság azonban a HAIS-Q-nak számos hiányossága van, ami abból ered, hogy a dimenziói részben elavultak, ideértve az autentikációs megoldásokat, a webes biztonságot és az új internetes alkalmazások kihívásait. Emiatt egy rugalmasabb, környezetérzékeny kérdőívre van szükség, amely az információbiztonsági tudatosságot a jelenlegi technológiai és üzleti realitásokhoz igazítva méri.

Jelen kutatás egy új megközelítést, a SAM elméleti modellt javasolja. Ez a modell a HAIS-Q alapjaira épül, ugyanakkor jelentősen kibővített és modernizált dimenziókat kínál a biztonságtudatosság átfogó értékelésére. A SAM hét fő dimenzióra összpontosít: autentikáció, internetes szolgáltatások használata, információkezelés, eszközhasználat, incidensmenedzsment, szabályozás és tudatosság. A SAM modellhez kapcsolódó kérdőív 120 kérdést tartalmaz, amelyek a KAB (Knowledge, Attitude, Behavior) modellt követik. Ezzel a célunk egy komplex és sokoldalú mérőeszközt javasolni, amely az empirikus adatok beérkezése után lehetővé teszi a biztonságtudatosság mélyreható elemzését, ezzel hozzájárulva hatékonyabb kiberbiztonsági stratégiák kidolgozásához és megvalósításához.

A cikk a 2024. október 15-i II. Alverad-Bánki Nemzetközi Kiberbiztonsági Konferencián elhangzott előadás kivonata.

Felhasznált irodalom

Ali, Omar – Shrestha, Anup – Chatfield, Akemi – Murray, Peter (2020): Assessing Information Security Risks in the Cloud: A Case Study of Australian Local Government Authorities. *Government Information Quarterly,* 37(1). Online: https://doi.org/10.1016/j.giq.2019.101419

Almadani, Mwaheb S. – Alotaibi, Suhair – Alsobhi, Hada – Hussain, Omar K. – Hussain, Farookh K. (2023): Blockchain-Based Multi-Factor Authentication: A Systematic Literature Review. *Internet of Things,* 23. Online: https://doi.org/10.1016/j.iot.2023.100844

Bak, Gerda – Berek, László – Som, Zoltán – Ujhegyi, Péter – Répás, József (2024): On the Way to Updating the Measurement of Information Security Awareness: a Literature Analysis. *Interdisciplinary Description Of Complex Systems,* 22(3), 305–316. Online: https://doi.org/10.7906/indecs.22.3.6

Bakare, Seun S. – Adeniyi, Adekunle O. – Akpuokwe, Chidiogo U. – Eneh, Nkechi E. (2024): Data Privacy Laws and Compliance: A Comparative Review of the

EU GDPR and USA Regulations. *Computer Science & IT Research Journal,* 5(3), 528–543. Online: https://doi.org/10.51594/csitrj.v5i3.859

Bamberger, Kenneth A. (2010): Technologies of Compliance: Risk and Regulation in a Digital Age. *Texas Law Review,* 88(4), 669–739.

Baranowski, Tom – Cullen, Karen W. – Nicklas, Theresa – Thompson, Deborah – Baranowski, Janice (2003): Are Current Health Behavioral Change Models Helpful in Guiding Prevention of Weight Gain Efforts? *Obesity Research,* 11(S10), 23S–43S. Online: https://doi.org/10.1038/oby.2003.222

Berek László – Som Zoltán – Bak Gerda – Ujhegyi Péter – Répás József – Pető Richárd (2024): Az egyén információbiztonsági tudatossági szintjének megállapítására elterjedt mérési módszerek összefoglaló elemzése nemzetközi kutatások alapján. In Molnár György – Temesvári Zsolt – Wührl Tibor (szerk.): *XXXIX. Kandó Konferencia 2023.* Budapest: Óbudai Egyetem, 265–277.

Buckley, Gerard – Caulfield, Tristan – Becker, Ingolf (2024): GDPR and the Indefinable Effectiveness of Privacy Regulators: Can Performance Assessment be Improved? *Journal of Cybersecurity,* 10(1). Online: https://doi.org/10.1093/cybsec/tyae017

Buckley, Oliver – Nurse, Jason R. C. (2019): The Language of Biometrics: Analysing Public Perceptions. *Journal of Information Security and Applications,* 47, 112–119. Online: https://doi.org/10.1016/j.jisa.2019.05.001

Diesch, Rainer – Pfaff, Matthias – Krcmar, Helmut (2020): A Comprehensive Model of Information Security Factors for Decision-Makers. *Computers and Security,* 92. Online: https://doi.org/10.1016/j.cose.2020.101747

Egelman, Serge – Harbach, Marian – Peer, Eyal (2016): *Behavior Ever Follows Intention? A Validation of the Security Behavior Intentions Scale (SeBIS).* Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, 5257–5261. Online: https://doi.org/10.1145/2858036.2858265

ENISA (2018): Cyberhead – Cybersecurity Higher Education Database. Online: www.enisa.europa.eu/topics/education/cyberhead#/

Gokulkumari, G. (2020): Analytical Outlook on Customer Awareness Towards Biometrics Mechanism of Unimodal and Multimodal in Online Transactions. *Multimedia Tools and Applications,* 79(41–42), 31691–31714. Online: https://doi.org/10.1007/s11042-020-09526-w

Hänsch, Norman – Benenson, Zinaida (2014): *Specifying IT Security Awareness.* 2014 25th International Workshop on Database and Expert Systems Applications (DEXA), 326–330. Online: https://doi.org/10.1109/DEXA.2014.71

Hermawan, Deni S. – Setiadi, Farisya – Oktaria, Dita (2022): *Measurement Level of Information Security Awareness for Employees Using KAB Model with Study Case at XYZ Agency.* 1st International Conference on Software Engineering and Information Technology (ICoSEIT) Bandung, Indonesia, 2022, 174–179. Online: https://doi.org/10.1109/ICoSEIT55604.2022.10029989

Hess, Elie – Tolbert, Matthew – Nascimento, Mattheus (2021): *Vulnerabilities of Multi-factor Authentication in Modern Computer Networks.* Worcester, UK: Worcester Polytechnic Institute.

Kashevnik, Alexey – Lashkov, Igor – Ponomarev, Andrew – Teslya, Nikolay – Gurtov, Andrei (2020): Cloud-Based Driver Monitoring System Using a Smart-

phone. *IEEE Sensors Journal,* 20(12), 6701–6715. Online: https://doi.org/10.1109/JSEN.2020.2975382

Kaya, Feridun – Aydin, Fatih – Schepman, Astrid – Rodway, Paul – Yetişensoy, Okan – Demir Kaya, Meva (2024): The Roles of Personality Traits, AI Anxiety, and Demographic Factors in Attitudes toward Artificial Intelligence. *International Journal of Human-Computer Interaction,* 40(2), 497–514. Online: https://doi.org/10.1080/10447318.2022.2151730

Kelly, Sage – Kaye, Sherrie-Anne – Oviedo-Trespalacios, Oscar (2023): What Factors Contribute to the Acceptance of Artificial Intelligence? A Systematic Review. *Telematics and Informatics,* 77. Online: https://doi.org/10.1016/j.tele.2022.101925

Kessler, Stacey R. – Pindek, Shani – Kleinman, Gary – Andel, Stephanie A. – Spector, Paul E. (2020): Information Security Climate and the Assessment of Information Security Risk Among Healthcare Employees. *Health Informatics Journal,* 26(1), 461–473. Online: https://doi.org/10.1177/1460458219832048

Kollmuss, Anja – Agyeman, Julian (2002): Mind the Gap: Why Do People Act Environmentally and What Are the Barriers to Pro-Environmental Behavior? *Environmental Education Research,* 8(3), 239–260. Online: https://doi.org/10.1080/13504620220145401

Koza, Erfan (2022): Information Security Awareness and Training as a Holistic Key Factor – How Can a Human Firewall Take on a Complementary Role in Information Security? In Ahram, Tareq – Karwowski, Waldemar (szerk.): *Human Factors in Cybersecurity.* New York: AHFE International, 49–57. Online: https://doi.org/10.54941/ahfe1002201

Kruger, H. A. – Kearney, W. D. (2006): A Prototype for Assessing Information Security Awareness. *Computers & Security,* 25(4), 289–296. Online: https://doi.org/10.1016/j.cose.2006.02.008

McCormac, Agata – Zwaans, Tara – Parsons, Kathryn – Calic, Dragana – Butavicius, Marcus – Pattinson, Malcolm (2017): Individual Differences and Information Security Awareness. *Computers in Human Behavior,* 69, 151–156. Online: https://doi.org/10.1016/j.chb.2016.11.065

Mujeye, Stephen (2021): *A Survey on Multi-Factor Authentication Methods for Mobile Devices.* Proceedings of the 2021 4th International Conference on Software Engineering and Information Management, 199–205. Online: https://doi.org/10.1145/3451471.3451503

National Data Guardian (2016): *National Data Guardian for Health and Care: Review of Data Security, Consent and Opt-Outs.* Online: www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs

Ometov, Aleksandr – Bezzateev, Sergey – Mäkitalo, Niko – Andreev, Sergey – Mikkonen, Tommi – Koucheryavy, Yevgeni (2018): Multi-Factor Authentication: A Survey. *Cryptography,* 2(1), 1. Online: https://doi.org/10.3390/cryptography2010001

Otta, Souma P. – Panda, Subhrakanta – Gupta, Maanak – Hota, Chittaranjan (2023): A Systematic Survey of Multi-Factor Authentication for Cloud Infrastructure. *Future Internet,* 15(4). Online: https://doi.org/10.3390/fi15040146

Parsons, Kathryn – McCormac, Agata – Butavicius, Marcus – Pattinson, Malcolm – Jerram, Cate (2014): Determining Employee Awareness Using the Human

Aspects of Information Security Questionnaire (HAIS-Q). *Computers and Security,* 42, 165–176. Online: https://doi.org/10.1016/j.cose.2013.12.003

Parsons, Kathryn – Calic, Dragana – Pattinson, Malcolm – Butavicius, Marcus – McCormac, Agata – Zwaans, Tara (2017): The Human Aspects of Information Security Questionnaire (HAIS-Q): Two Further Validation Studies. *Computers and Security,* 66, 40–51. Online: https://doi.org/10.1016/j.cose.2017.01.004

Reis, Oluwatosin – Eneh, Nkechi E. – Ehimuan, Benedicta – Anyanwu, Anthony – Olorunsogo, Temidayo – Abrahams, Temitayo O. (2024): Privacy Law Challenges in the Digital Age: A Global Review of Legislation and Enforcement. *International Journal of Applied Research in Social Sciences,* 6(1), 73–88. Online: https://doi.org/10.51594/ijarss.v6i1.733

Rohan, Rohani – Funilkul, Suree – Pal, Debajyoti – Chutimaskul, Wichian (2021): *Understanding of Human Factors in Cybersecurity: A Systematic Literature Review.* 2021 International Conference on Computational Performance Evaluation (ComPE), Shillong, India, 133–140. Online: https://doi.org/10.1109/ComPE53109.2021.9752358

Safa, Nader S. – Sookhak, Mehdi – Von Solms, Rossouw – Furnell, Steven – Ghani, Norjihan A. – Herawan, Tutut (2015): Information Security Conscious Care Behaviour Formation in Organizations. *Computers & Security,* 53, 65–78. Online: https://doi.org/10.1016/j.cose.2015.05.012

Sangwan, Aarti (2024): *Human Factors in Cybersecurity Awareness.* 2024 International Conference on Intelligent Systems for Cybersecurity (ISCS), Gurugram, India, 1–7. Online: https://doi.org/10.1109/ISCS61804.2024.10581139

Srinivasan, Srihari (2023): *Understanding User Perception of Biometric Privacy in the Era of Generative AI.* 4th International Conference on Communication, Computing and Industry 6.0 (C216) 2023, Bangalore, India, 01–06. Online: https://doi.org/10.1109/C2I659362.2023.10430931

Stein, Jan-Philipp – Messingschlager, Tanja – Gnambs, Timo – Hutmacher, Fabian – Appel, Markus (2024): Attitudes Towards AI: Measurement and Associations with Personality. *Scientific Reports,* 14(1). Online: https://doi.org/10.1038/s41598-024-53335-2

Taneski, Viktor – Heričko, Marjan – Brumen, Boštjan (2014): *Password Security – No Change in 35 Years?* 2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 1360–1365. Online: https://doi.org/10.1109/MIPRO.2014.6859779

Wang, Ding – Shan, Xuan – Dong, Qiying – Shen, Yaosheng – Jia, Chunfu (2023): *No Single Silver Bullet: Measuring the Accuracy of Password Strength Meters.* 32nd USENIX Security Symposium (USENIX Security 23), 947–964.

Weber, James E. – Guster, Dennis – Safonov, Paul – Schmidt, Mark B. (2008): Weak Password Security: An Empirical Study. *Information Security Journal: A Global Perspective,* 17(1), 45–54. Online: https://doi.org/10.1080/10658980701824432

Wilson, Mark – Pitcher, S. I. – Tressler, J. D. – Ippolito, J. B. – de Zafra, D. E. (1998): *Information Technology Security Training Requirements: A Role- and Performance-Based Model.* National Institute of Standards and Technology Special Publication, 800–816. Online: https://doi.org/10.6028/NIST.SP.800-16

Yeo, John (2013): Using Penetration Testing to Enhance Your Company's Security. *Computer Fraud & Security,* (4), 17–20. Online: https://doi.org/10.1016/S1361-3723(13)70039-3