

BIZTONSÁGTUDATOSSÁGI TRÉNINGEK HATÉKONYSÁGÁNAK VIZSGÁLATA

EVALUATION OF SECURITY AWARENESS TRAINING EFFECTIVENESS

KÁRÁSZ Balázs

(ORCID: 0000-0003-2065-4928)

karaszb@gmail.com

Absztrakt

A közlemény egy sorozat első része, amely egyfelől bemutatja a tréningek hatékonyságát értékelő módszerek tulajdonságait, ezen belül pedig feltárja a befektetés-megtérülési (ROI) módszertan alkalmazásának problémáit a magyarországi vállalati HR menedzsment gyakorlatban. A közlemény másfelől szektorális és egyéb statisztikai elemzések segítségével előkészíti a ROI biztonság-tudatossági tréningek vonatkozásában történő alkalmazásának további vizsgálatát – a sorozat következő részében.

Kulcsszavak: információbiztonság, kulcs mutatószámok, képzés-fejlesztés, ROI

Abstract

This paper is first of a series, which on the one hand presents tools evaluating effectiveness of trainings, and within this unravels the problems of implementing return-on-investment (ROI) methodology in the Hungarian corporate HR management environment. The paper on the one hand also prepares further research on ROI implementation upon security awareness trainings with the help of sectoral and other statistical analysis – to be published in the continuation of the paper series.

Keywords: information security, key indicators, learning&development, ROI

BEVEZETÉS

Az egyik legfontosabb, általános modern felfogásnak tekinthető, hogy az operatív személyzeti osztályból stratégiaivá fejlődő HR menedzsment tevékenységet szükséges beemelni a felső vezetés közvetlenebb irányítása alá. Ez azzal indokolható, hogy a vállalat termelékenység, működésének hatékonysága közvetlenül függ a strukturált és szisztematizált HR menedzsmenttől. Előre mutató tehát annak mentén gondolkodni, hogy az emberi erőforrás gazdálkodás, a munkaerő megtartása, motivációja, értékelése, javadalmazása, képzése és fejlesztése kulcsfontosságú szerepet játszik a munkavégzés hatékonyságában, ami jól nyomon követhető módon kihat a jövedelmezőségre.

A HR menedzsment tevékenységei közül egyre inkább kiemelkedik a képzés-fejlesztés jelentősége, az infokommunikációs technológiák minden gazdasági ágazatban és területen tapasztalható lendületes és meggyőző térnyerésével karöltve. A szakmai és egyéb képzési programok hatékonyságának a vállalat jövedelmi helyzetére gyakorolt hatását felmérve érdemes tehát a források egy meghatározó részét erre a területreallokálni. A tréningek és képzések hatékonyságának vizsgálata Magyarországon olyan aktuális problémakör, amelyre a vezetők és HR szakemberek folyamatosan egyre újabb megoldásokat keresnek, hogy ezzel is biztosíthassák versenyelőnyüket a vetélytársakkal szemben.

Több, hasonló értelmű szakkifejezés közül a közlemény a tréning és a képzés szót – egymás szinonimájaként – elsősorban azon folyamat jelzésére alkalmazza, amely a fejlesztés tevékenységén belül, a továbbképzés által a dolgozókat eredményképpen az aktuálisan végzett munka jobb elvégzésében segíti. Továbbá, a munkavállalók információbiztonságtudatosságának fogalmát a közlemény bármely szervezet működésében olyan kulcsfontosságú tényezőként alkalmazza, amely célképzések, sőt akár tréningek útján növelhető, ezek hatékonysága és célszerűsége pedig mérhető, vizsgálható. Kollár [1] szerint a szervezeti gyakorlatból egyelőre hiányzik az adat-, információ- és informatikai biztonság kulcsmutatószámainak és indexeinek a kidolgozott és egységes módszertana. Jelen közlemény egy új aspektust kíván megvilágítani, hogy e hiányzó módszertan kidolgozása mélyebb merítésen alapulhasson.

A HR menedzsment területén alkalmazott, ún. ROI (befektetés-megtérülési) módszertan egy pénzügyi megtérülés alapú rendszerszemlélet, melynek segítségével bármilyen típusú program, projekt, vállalati folyamat értéke, nyereségtermelő képessége kimutatható. A közlemény célja, hogy ROI metodológia információbiztonsági képzések területén lehetséges alkalmazhatóságának vizsgálatát előkészítendő, részletes eredményeket mutasson be a ROI vállalati alkalmazásának magyarországi gyakorlatát illetően.

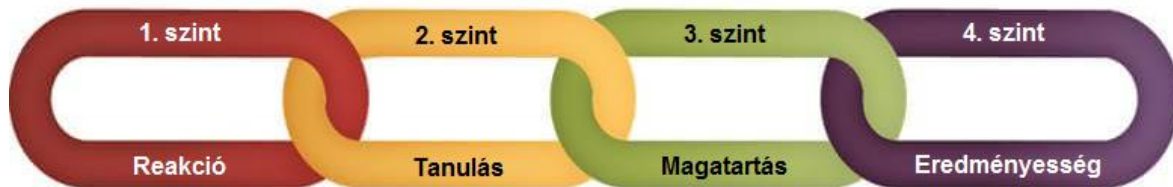
ROI (BEFEKTETÉS-MEGTÉRÜLÉSI) MÓDSZERTAN

A képzések értékelésére számos módszer ismert, amelyeket a következő fejezetben – a hatékonyságmérés kontextusában – röviden ismertetek. A szakirodalom szerint [2] bármely más tevékenységhez hasonlóan egy szervezetben a képzések és tréningek hatékonyságát is értékelni kell. Kirkpatrick 1994-ben kidolgozott modellje alapján (ld. 1. sz. ábra) a következő területek, szintek értékelésére érdemes figyelmet fordítani és erőforrástallokálni:

- **Reakció:** az értékelésnek az egyik legegyszerűbb módja. A tréning elégedett résztvevője valószínűleg eredményesebben tudja alkalmazni a program során hallottakat. A reakciók mérését a program végén azonnal el kell végezni. A kiértékeléskor nem csak általában a programra való reagálást, hanem a program specifikus összetevői által a résztvevőkben kiváltott reakciót, attitűdöt is vizsgálják.
- **Tanulás:** a cél az, hogy megállapítsuk, mennyit tanultak a program résztvevői a tréning ideje alatt. A résztvevők tanulási szintjének ellenőrzéséhez célszerű olyan tesztet alkalmazni, aminek során ellenőrizzük a tudásszintet a program előtt és után.

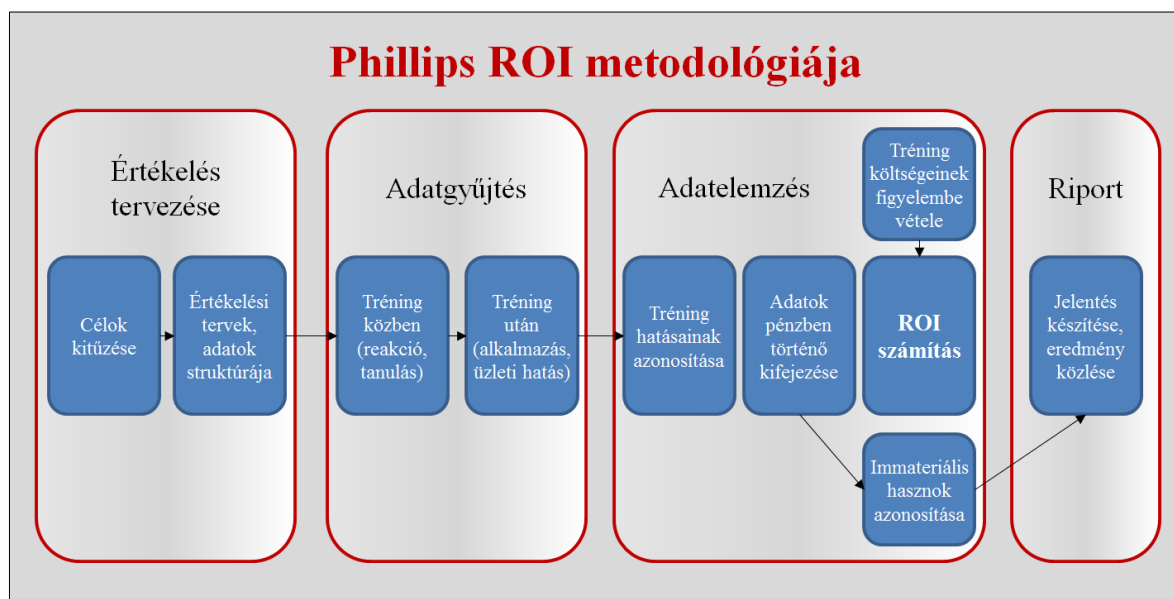
Kontrollcsoportként olyan személyeket kell alkalmazni, akik nem vettek részt a tréningen.

- Magatartás: cél az is, hogy megállapítsuk, hogy a résztvevők a tréning eredményeként változtattak-e a viselkedésükön.
- Eredményesség: a menedzsment részéről állandó a nyomás, hogy a HR-vezetés mutassa ki a tréningprogramokba történt befektetés megtérülési rátáját, eredményességét.



1. ábra: A Kirkpatrick-modell (forrás: [3] alapján saját szerkesztés)

Az eredményesség értékelésének egy kiemelt módszere az USA-ban 1992-ben alapított ROI Institute, Inc. által közzétett, 60 országban (köztük Magyarországon is), több mint 5000 szervezet által alkalmazott módszertan, amely a vállalat vezérigazgató-házaspárjának tudományos munkásságát tükrözi, annak legkiemelkedőbb eredménye. [roiinstitute.net] A ROI módszertan egy pénzügyi megtérülés alapú rendszerszemlélet, melynek segítségével bármilyen típusú program, projekt, vállalati folyamat értéke, nyereségtermelő képessége kimutatható. Az öt különböző, egymásra épülő dimenzióban végzett mérések lehetővé teszik a teljesítmény széles körben történő kiértékelését az elégedettségi mutatóktól a pénzügyi hatásig.



2. ábra: Phillips ROI metodológiája (forrás: [4] alapján saját szerkesztés)

A ROI módszertan egyaránt alkalmas mennyiségi és minőségi adatok kezelésére és előállítására, hiteles megtérülési információkat szolgáltatva a menedzsment tagjai és más érdekelt felek számára. A 2. sz. ábrán vázolt folyamat struktúrát követve lehetőség nyílik az egyéb befolyásoló tényezők teljes leválasztására, a vizsgált projekt hatásainak elkülönítésére a pontos hozzáadott érték kimutatása érdekében. Annak érdekében, hogy az eredmények valósak, megbízhatóak legyenek, a folyamat az alábbi három fő komponensből áll:

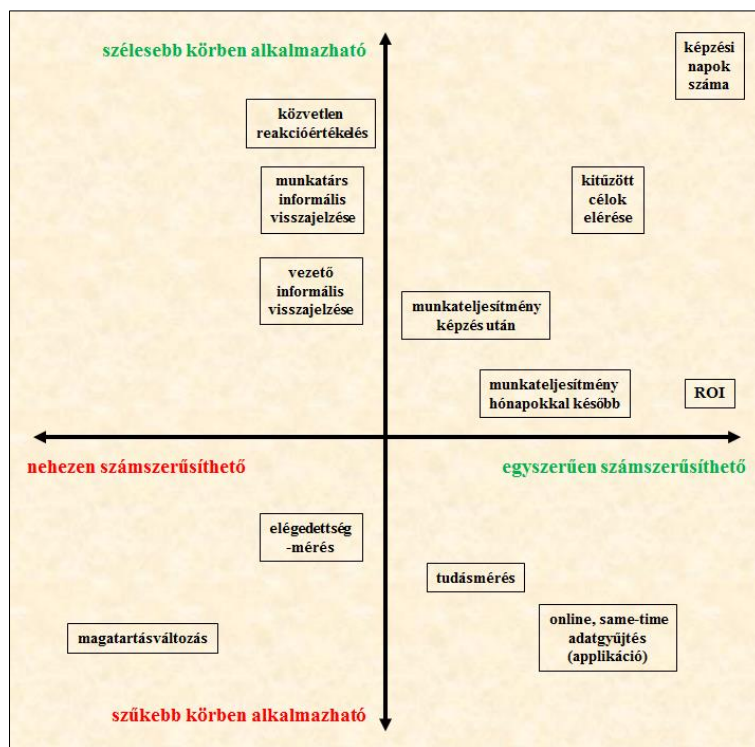
- értékelési keretrendszer, adattípusokat és értékelésük szintjeit definiálja;
- folyamatmodell, amely lépésről lépésre alakítja az aktuális ROI kalkulációt, és részeként a program hatásainak egyéb tényezőit elkülönítve kezeljük;
- konzervatív működési standardok, amelyek a folyamat vezérelveként működnek, biztosítják az eredmények megbízhatóságát, megteremtik a bizalmat a vezetők részéről is.

TRÉNINGHATÉKONYSÁG 2016 KUTATÁS

Aktív és vezető tagja voltam annak a hallgatói kutató teamnek, amely elvégezte a SZIE GTK TTI Menedzsment és HR Kutatóközpontja által 2016-ban lefolytatott országos tréninghatékonyság kutatás elemzését, továbbá az erről kiadott magyar nyelvű kutatási jelentés társszerzője [5]. A jelentés megállapításait az általános statisztikai módszerek (átlag, gyakoriság, eloszlás) alapozták meg. A felmérést 2016 harmadik negyedévében hajtották végre 450 válaszadó magyarországi szervezet részvételével. A kutatást vezetők tervei szerint a kutatás folytatódik, megismételhető, illetve az adatbázis, a résztvevők köre bővíthető.

A vizsgálat leíró jellegű, minden esetben objektív adatokra épít, a jelentés bővebb következtetések levonása nélkül készült. A kérdőív a statisztikai elemzések megkönnyítése érdekében a legtöbb esetben zárt kérdéseket alkalmaz – ez segítségemre volt a későbbi többváltozós elemzés elkészítéséhez is. A vizsgált témaköröket nagymértékben lefedő, előre megfogalmazott válaszok közül a legjellemzőbbek megjelölését kértük a válaszadóktól. Megjegyzendő, az „egyéb” válaszlehetőségek alatt több esetben olyan megfogalmazással szembesültünk, amely alapján az a megadott lehetőségek valamelyikébe besorolható. A felmérésben alkalmazott kérdőív a következő három fő részből áll: személyzetfejlesztés, képzések és tréningek értékelése, válaszadó szervezetek és a válaszadó személyek jellemzői.

Részben a kutatás eredményeinek tükrében, és azok felhasználásával egy összehasonlítást elősegítő portfólió-mátrixot készítettem, mely a mérőeszközöket alkalmazásuk széles körű lehetőségei és számszerűsíthetőségük szempontjából osztályozza: (ld. 3. sz. ábra)



3. ábra: Tréninghatékonyságot mérő eszközök portfóliója (forrás: [5] alapján saját szerkesztés)

A mátrix módszertana alapján elsősorban az egyes eszközök tulajdonságainak egymáshoz viszonyított relációját mutatja, semmiképpen nem értelmezhetők abszolút módon a mátrixban elfoglalt helyük közötti különbségek. Számos kvalitatív és kvantitatív mérőeszköz összehasonlításából (azokon túl is, amelyek a 3. sz. ábrában szerepelnek) eredményképpen azt kaptam, hogy a mátrix azon területein, ahol az egyik ismerv inkább meghatároz egy eszközt, míg a másik kevésbé, összességében kevesebb található, mint azon területeken, ahol mindkét attribútum kevésbé, vagy mindkettő inkább jellemző az adott eszközökre. Így elsősorban azon eszközökre koncentráltam, amelyek egyaránt szélesebb körben alkalmazhatóak, valamint egyszerűbben számszerűsíthetőek, az alábbi megállapítások ezért ezeket a módszereket érintik.

Úgy foglalható össze a portfólió a vizsgálat szempontjából, hogy a ROI mutató a számszerűsíthetőségben élen jár, azonban a vállalati kultúra különösen Magyarországon nem teszi lehetővé azt, hogy igazán széles körben elterjedjen. Ettől függetlenül, tulajdonságai alapján feljebb pozicionálható alkalmazhatóság szerint, hiszen a megfelelő módszertan és kellő ismeretek birtokában szemléletes eredménnyel szolgál a képzések hatékonyságáról. Ezzel szemben a képzési napok számának rögzítése egyszerű adminisztrációs feladatot kíván, ezért azonos a vízszintes tengely szerint elfoglalt helye a ROI mutatóéval. Mivel több nemzetközi kutatás egyik központi témájához szolgáltatott alapot, ezért a HR menedzsment globális fejlődésének is lehet egy fontos alappillére.

A másik három, könnyebben alkalmazható mérőeszköz vonatkozásában elmondható, hogy a munkateljesítmény mérése a képzés után közvetlenül és néhány hónappal később hasonló output-ot szolgáltat napjainkban. A közvetlenül a képzés után megvalósuló értékelés több esetben alkalmazható, mint a sokszor hiányos, nem megfelelő adatrögzítések és az idővel esetleg változó preferenciák által befolyásolt hónapokkal később történő visszamérés. Ettől függetlenül utóbbi épp a finomított értékelési módszertannak köszönhetően számszerűsíthető.

Ami a fejlesztési tervben kitűzött célok elérését illeti, beszélhetünk egyszerű összehasonlításról, sávosan megállapított százalékos teljesülési értékekről, de nem szabad figyelmen kívül hagyni a célkitűzésben szereplő időcél, amelynek vonatkozásában értelmezzük a célokat. Ez az eszköz – ahogyan a képzési napok száma is – a Tréninghatékonyság felmérésnek nem képezte alapját, de megjelenik más, globális vizsgálatokban.

ROI ALKALMAZÁSA ÉS PROBLÉMÁI

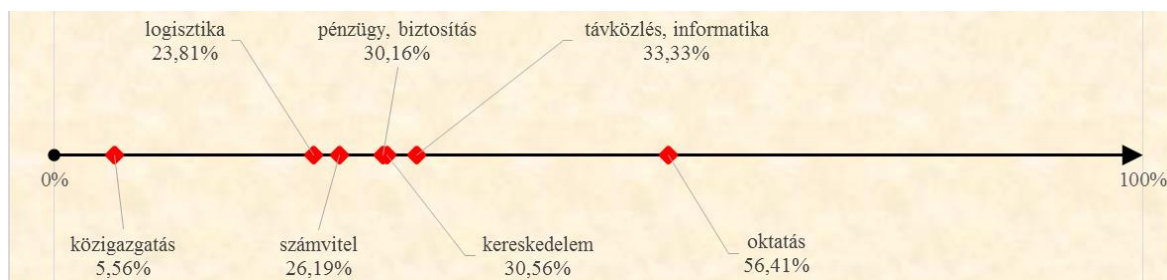
Az adatbázis további vizsgálata során statisztikai összefüggést kerestem a Tréninghatékonyság 2016 kutatás vizsgált adatai között. Az adatbázist leszűkítettem a ROI alkalmazásával kapcsolatban nyilatkozó magyarországi vállalatok körére, és az így kialakult, 167 elemszámú mintán végeztem el az alábbi értékeléseket.

Általános alapelveként a ROI alkalmazásának gyakoriságát az alábbiak szerint számszerűsítettem: százalékos értékeket rendelttem az egyes válaszokhoz („Mindig” = 1,00 / „Gyakran” = 0,67 / „Néha” = 0,33 / „Soha” = 0,00), majd ezek számtani átlagát vettem a különböző szűrések szerint a kategóriához tartozó cégek listájában, így alakultak ki a következő ábrákban látható eredmények. Fontosnak tartottam, hogy amennyiben a minta elemszámának 5%-ánál kevesebb válaszadó tartozik egy kategóriába, annak adatát ne vegyem figyelembe.

A kapott hozzárendelések természete szerint csoportosítom a vizsgált kapcsolatokat, eszerint nominális skálán értelmezhető az iparágak szerinti megosztás, és a tényezők szerinti csoportosítás, amelyek vélt vagy valós hiánya befolyásolja a ROI alkalmazásának gyakoriságát, valamint ordinális skálán a ROI eredményeinek különböző HR menedzsment tevékenységek során történő felhasználása.

ROI alkalmazásának szektorális elemzése

A 4. sz. ábra alapján a válaszok összesítésekor alkalmazott számszerűsítési módszertan magas pontatlanságát figyelembe véve elmondható egyfelől, hogy a közigazgatási profillal rendelkező vállalatok, intézmények esetében legkevésbé gyakori a ROI alkalmazása, tehát a legkevésbé tudatos a tréningek hatékonyságára való törekvés. Az összes többi szegmens (kivéve egyet) az átlag körül szóródik, jelentős eltérés az adatok alapján magyarázó erővel nem mutatható ki. A másik végletet egyedüli kivételként az oktatással foglalkozó szervezetek csoportja képviseli, amelyben a ROI alkalmazásának átlagos gyakorisága meghaladja az 50%-ot.



4. ábra: ROI alkalmazási gyakorisága az egyes iparágakba tartozó vállalatokban (forrás: [5] alapján saját szerkesztés)

A szektorális elemzés legfőbb tanulsága, hogy a vizsgált iparágak közül az oktatással foglalkozó szervezetekben a képzések hatékonyságának értékelésében számottevően gyakrabban kap szerepet a befektetés-megtérülés kalkulációja, mint más szektorokhoz tartozó szervezetekben. Alacsony valószínűség mellett elképzelhető, hogy összességében több más profilú vállalat alkalmazza a szervezett tréningek hatékonyságát mérő befektetés-megtérülési módszertant, de ritkábban. Ez azonban az iparágak sajátosságainak ismerete fényében, valamint tekintettel arra, hogy az elemzés során a metodológia alkalmazásának gyakoriságra került kiemelt hangsúly, nem lenne logikus következtetés.

A vizsgálat alapján megállapítható a közszféra¹ HR menedzsment gyakorlatának meglepő előretörése számos tréning-területen a korábbi átfogó Cranet² felmérések adataihoz képest. A közszférában nagyobb arányban készítenek képzési tervet, mint a versenyszférában. Az ilyen tervek tipikus időintervalluma a 6-12 hónap. A másik olvasata ennek az, hogy jóval kevesebb válaszadónál készítenek személyzetfejlesztési terveket. A kérdőívet kitöltő szervezetek valamivel több mint 50%-a szisztematikus igényfelmérést is alkalmaz a személyzet képzésének és fejlesztésének a megalapozásához, ami inkább a személyzetfejlesztés eszköze.

Míg az állami szféra tréningtervei többnyire a törvényi előírásokhoz való igazodás eszközei, addig a piacon inkább személyzetfejlesztés történik, ehhez kapcsolódó tervvel. A közszférában év elején a Kit.³ hatálya alá tartozó szerveknek le kell adnia a képzési igényt a Nemzeti Közszo szolgálati Egyetem Vezető- és Továbbképzési Intézete felé, ami egy újabb, a törvényességhez való igazodást segítő eszközzé teszi a tréningterveket. Ugyanerre utal a betanítási folyamathoz kapcsolódó képzések gyakorisága az állami szférában.

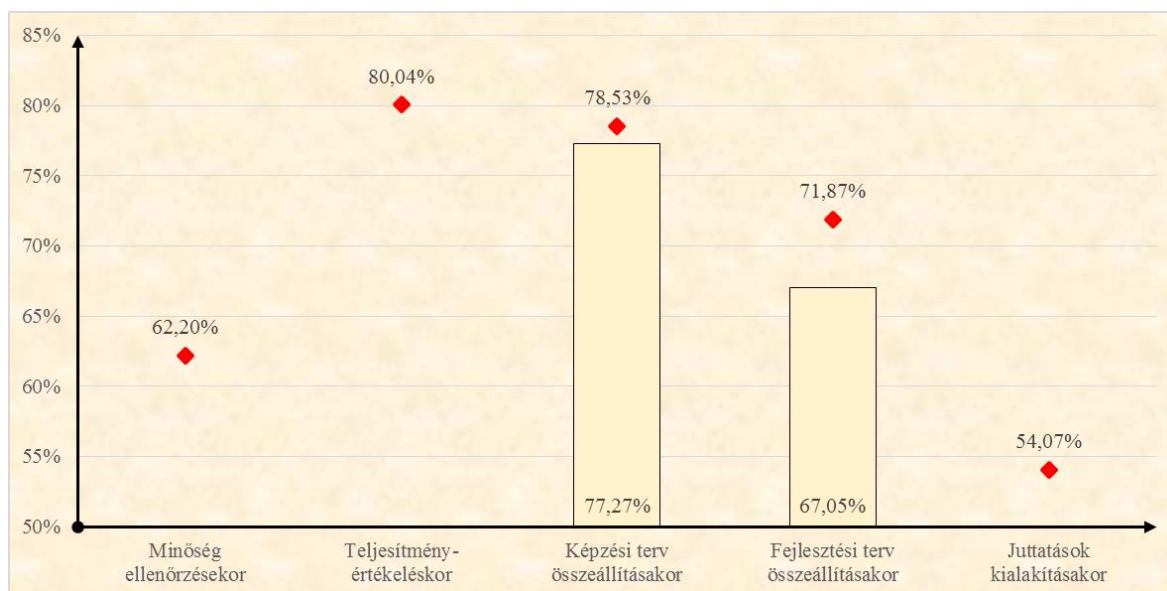
¹ A közszférába a kutatás és jelen közlemény értelmezésében kizárólag költségvetési szervek tartoznak, nem teljes átfedésben a 4. sz ábrán feltüntetett „közigazgatás” profilú válaszadó szervezetek körével. Az állami tulajdonú vállalatok a versenyszférába, ill. a „vegyes” kategóriába kerültek besorolásra.

² Cranfield Network: a Cranfield Business School által működtetett Európai Emberi Erőforrás Kutatási Hálózat. A mintegy hatvan, tényszerű adat közlését váró kérdést tartalmazó kérdőív biztosítja a térbeli összehasonlítást, sőt longitudinális elemzések lehetőségét is. Magyarországon a kutatást először 2004-2005-ben végezték el, amelynek eredménye a rendszerváltás utáni növekedést mutató folyamatokat mutatta be, a 2008-2009-ben folytatott vizsgálat tükrözte a válság hatását, a legfrissebb, 2014-2015-ös pedig a válságból való kilábalás fázisában értékelte az országok HR menedzsment gyakorlatát.

³ 2018. évi CXXV. törvény a kormányzati igazgatásról

Mindez összecseng a honvédelem és a rendvédelem képzési folyamatainak alapgondolataival, amely területeken szintén elsősorban a törvényi és egyéb jogszabályi megfelelés áll a fizikai és szellemi jellegű képzések középpontjában egyaránt. Jelen közlemény nem foglalkozik hosszabban a honvédelmi és rendvédelmi szervek képzés-fejlesztési tevékenységének jellemzésével, de kitekintést kíván adni a későbbi rész kutatások számára néhány összefüggés megfogalmazásával.

ROI alkalmazása a képzési folyamat során



5. ábra: ROI alkalmazási gyakorisága az eredmények felhasználásának helye szerint (forrás: [5] alapján saját szerkesztés)

Az 5. sz. ábra értelmezéséhez és relevanciájának megértéséhez távolabbról kell vizsgálni a problémakört. Meglátásom szerint az ábrázolt értékhalmoz azért értelmezhető egyfajta függvényként, mert a hozzárendelés alapjául szolgáló tevékenységek bizonyos szempontból egymásból következő, egymással kölcsönhatásban lévő lépésekként jelennek meg a szervezetfejlesztési folyamat során. A minőség-ellenőrzés egy egyszerű visszamérést jelent, amely számos iparágban a termelés hatékonyságát értékeli. A teljesítményértékelés ugyanakkor a munkavállaló számára is visszacsatolást nyújt, alapot teremtve a képzési tervhez, amennyiben készül ilyen. Mindezt a fejlesztési terv már komplex szemlélettel kezeli, és amennyiben a HR menedzsment gyakorlata tartalmazza ezt a többletet, egyes juttatások megállapításának fő befolyásoló tényezője lehet a ROI.

Ennek értelmében hasznos, ha a válaszadó szervezetek gyakorlatát olyan szempontból is látjuk, hogy készül-e teljesítményértékelés, képzési, fejlesztési terv, valamint van-e szerepe a juttatások kialakításában a teljesítménynek. Sajnos a kérdőív és az elkészült adatbázis nem tette lehetővé minden tényező vizsgálatát, így csupán az ábrában is látható képzési terv és fejlesztési terv alkalmazásának gyakoriságát tudjuk elemezni. A fent látható adatok azon vállalatok esetében érvényesek, amelyek legalább „néha” alkalmazzák a ROI-t. Az összefüggés tehát ebben a statisztikai kapcsolatban beigazolódik: kevesebb olyan válaszadó szervezet készít fejlesztési, mint képzési tervet, amelynek HR gyakorlatában szerepet kap a befektetés-megtérülés számítása.

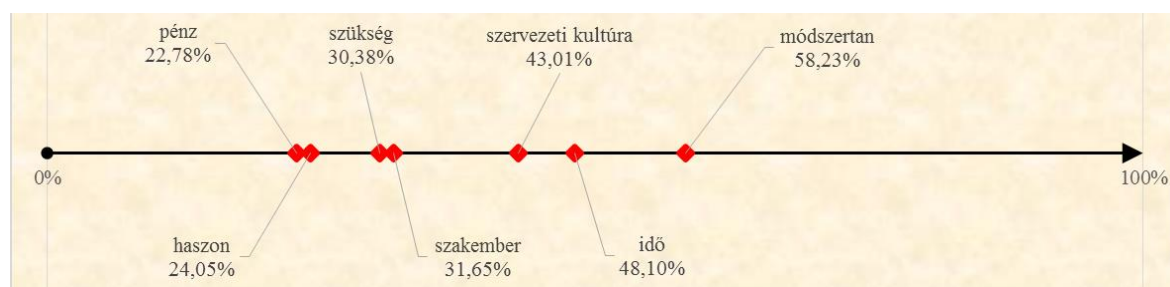
A válaszadók tehát, akik legalább „néha” alkalmazzák a ROI módszertant, akár egyszerű mutató formájában, relatíve nagy gyakorisággal használják a kalkuláció eredményét az egyes fázisok során. Összefüggés fedezhető fel azonban természetesen a képzési és fejlesztési tervek

ritkább előfordulása, illetve az e lépésekhez rendelhető egyre alacsonyabb értékek között. Legkevésbé jellemző a magyar vállalatokra a ROI juttatások kialakításakor történő figyelembe vétele, ugyanakkor meglepő, hogy sok szervezet már a legegyszerűbbnek tekinthető minőség-ellenőrzés során sem fordít figyelmet a befektetések megtérülésére.

Fejlesztendő terület lehet ezek alapján tehát a minőség-ellenőrzés során történő ROI kalkuláció módszertanának szélesebb körben való megismertetése, kidolgozása. Mindenképpen megfontolandó a teljesítményértékelés szempontrendszerének magasabb szintű kidolgozása a vállalatok jelentős részében, kiegészítve azt a tréningek hatásaival, amely nem csupán a ROI alkalmazását jelentheti. Fontos megállapítani mindezek alapján, hogy a képzés-fejlesztés folyamata közvetlenül befolyásolja a termelékenységet és a hatékony, minőségi munkavégzést.

ROI alkalmazását lehetővé tévő tényezők hiánya

A 6. sz. ábra azt mutatja, hogy a ROI alkalmazásának elutasításában milyen tényezők játszanak szerepet, mely tényezők vélt vagy valós hiánya milyen mértékben határozza meg, hogy az adott szervezet elzárkózik a mérőeszköz bevezetésétől. Leginkább a megfelelő módszertani ismeretek hiánya veti vissza a tréningek hatékonyságának visszamérésére való hajlandóságot, majd a sorban a nem elegendő erre szánt idő és a szervezeti kultúra hiányosságai következnek.



6. ábra: Tényezők hiányának szerepe a ROI alkalmazásának elutasításában (forrás: [5] alapján saját szerkesztés)

A ROI alkalmazásának gyakoriságára szűkítve a kutatási kérdőívből kiemelt, az összes mérőeszközhöz vonatkoztatott kérdéshez képest azt találtam, hogy a kevés rendelkezésre álló anyagi forrás és a tréninghatékonyság mérését előnyben nem részesítő szervezeti kultúra kevésbé indokolja a válaszadó szervezeteknél az alacsonyabb elterjedtséget. Érdekes ugyanakkor megfigyelni, hogy a válaszok alapján viszonylag alacsony azon esetek száma, amelyekben a szakemberek hiánya okozza az alacsonyabb színvonalú visszamérést, mint ahogy azzal az alapvetéssel is egyetértenek a menedzserek, hogy a hatékonyságmérés haszonnal jár, nem csupán a költségvonzata merül fel.

A megfelelő ROI elemzéshez elengedhetetlen *adatgyűjtésnek* Bartel [6] szerint az alábbi feltételeknek kell maradéktalanul megfelelnie:

- átfogó, széles körű és minden részletre kiterjedő,
- lehetőség szerint minél több munkavállalóra kiterjedő,
- többszörösen ismételhető, valamint ad-hoc időpontokban végrehajtott,
- lehetőség szerint minden folyamaton belül minél több pontot érintő.

Ezzel összhangban fejlesztendő a vállalatok módszertani ismerete, amelyben a Magyarországon is működő nemzetközi HR kutatóközpontoknak és szervezeteknek kell egyre nagyobb szerepet vállalnia. Áttételesen megoldást jelent a megfelelő képzés nyújtása a későbbiekben HR menedzsmenttel foglalkozó szakemberek számára, akik felvértézve a módszertani ismeretekkel, egyszerre formálják a szervezeti kultúrát, valamint nyújtanak a szakemberhiány problémájára is megoldást, csapatuk szakirányú továbbképzésével.

BIZTONSÁGTUDATOSSÁGI TRÉNING

A biztonságtudatossági tréning célja, hogy a munkatársak értesüljenek a rájuk vonatkozó mindenkor jogszabályokról, a szervezetben érvényes biztonsági előírásokról, tisztában legyenek azok betartásának szükségességével, tudomást szerezzenek az őket fenyegető lehetséges veszélyekről, támadási technikákról, sőt tudatosan tegyenek lépéseket ezek hatékony észleléseért és elhárításáért. [7] Mindez – összhangban a Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program által megfogalmazott kibervédelmi törekvésekkel – a honvédelmi és rendvédelmi szervek törvényi előírásoknak történő megfelelésének is alapjául szolgál. A közlemény elsődlegesen az olyan szervezetekben megvalósuló biztonságtudatossági képzéseket tárgyalja, amelyek önállóan vagy dedikáltan működő információbiztonsági szakterülettel rendelkeznek.

Oroszi [8] az általa a *social engineering* támadások⁴ elleni védekezések lehetséges útjai között említett biztonságtudatossági képzések szintjei azonosításához az alábbi terminológiát alkalmazza: biztonságtudatossági oktatás – figyelemfelkeltés, alapismeretek elsajátítása, tréning – specializált, ismeretek bővítése, különböző felhasználói csoportok, továbbképzés – szakirányú képzés, tanfolyam, célja a szakemberek képzése. Ezzel szemben a közlemény a biztonságtudatossági képzést/tréninget (a bevezetőben említett módon ugyancsak egymás szinonimájaként) átfogó folyamatként definiálja, amelynek elemei az oktatás, célzott és általános tájékoztatás stb., továbbá a biztonságtudatossági szint fenntartása, mérése, ill. a tréning hatékonyságának vizsgálata.

Biztonságtudatossági képzést érdemes (és szükséges) rendszeresen, minimum évente szervezni, hogy a munkatársak az előírásokat ismétlő jelleggel elsajátítsák, jelentősebb jogszabályi, külső veszélyekkel kapcsolatos változás esetén pedig ennél sűrűbben, a tanulás és mielőbbi alkalmazás elősegítése céljából. Eseti jelleggel ugyancsak megfontolandó képzés szervezése, amennyiben incidens következik be, annak kivizsgálását követően az érintettek részére, továbbá új munkavállaló részére, belépését követően a többi szakterületi tájékoztatóval együtt. A tréning megvalósítási módját tekintve lehet tantermi, e-learning oktatás vagy ezek kombinációja is. A tantermi oktatásokon való részvételt a társaság által szabadon meghatározott jelenléti ív kitöltésével kell igazolni. A rendszeres oktatás esetében célszerű külön oktatási célcsoportok, valamint tematika meghatározása (pl. felső vezetés, adminisztrációs terület, üzemeltetés stb.). A célcsoportok kialakításakor figyelembe kell venni a célcsoportra jellemző speciális fenyegetéseket, valamint a célcsoport által használt adatok biztonsági besorolását.

A munkavállalók biztonságtudatossági szintjének folyamatos fenntartása és javítása érdekében igény szerint változó rendszerességű biztonságtudatossági program megvalósítása válhat szükségessé, mely a következőképpen valósítható meg:

- biztonságtudatossági program: egész évet átölelő program, mely mindennapos, heti, kétheti, havi vagy negyedéves gyakoriságú, jellemzően általános, de célzott jellegű programelemekkel is rendelkezhet;
- biztonságtudatossági kampány: rendszeresen, de csak időszakosan pár hét vagy hónap időtartamban jelenik meg, elemei lehetnek általánosak, de jellemzőbb inkább a célzott, adott probléma megvitatására vonatkozó figyelemfelkeltés (pl. szabályzatok módosítása, új rendszerek bevezetése, eszközök használata, korábbi incidensek bemutatása és megelőzése).

⁴ „Mivel a *social engineering* a felhasználók figyelmetlenségét és tudatlanságát használja ki a támadás során, ezért megelőzésére a legjobb módszer az alkalmazottak megfelelő képzésének biztosítása.” [8] „Az ember *social engineering* típusú sebezhetősége a következő tulajdonságokban érhető tetten: befolyásolhatóság, bosszúállás, emberi hanyagság és figyelmetlenség, félelem, hiszékenységek és naivság, kényelmesség, konfliktuskerülés, segítőkészség, szexuális vágy/vonzalom, tekintélyelvűség, tudatlanság és szakképzetlenség.” [9]

Az oktatási és tájékoztatási célú tréningelemek magukba kell, hogy foglalják a munkavállaló felelősségét arra nézve, ha az előírások hiányos alkalmazása, figyelmen kívül hagyása következtében káresemény keletkezik, illetve ezek szankcionálását⁵ a szervezet belső szabályzata, ezen túlmenően pedig a Munka Törvénykönyve, indokolt esetben a Polgári törvénykönyv, illetve a Büntető törvénykönyv alapján.

A felhasználók biztonságtudatossági szintjét, illetve a tréningelemek hatékonyságát rendszeres időközönként mérni szükséges, erre szolgálhatnak az alábbi módszerek:

- a biztonságtudatossági szint mérésére, a sebezhetőség felderítésére alkalmas lehet:
 - kérdőív – a kérdések fókuszában pl. a tréningelemekhez visszacsatoló reakciók,
 - helyszíni bejárások – tiszta asztal, tiszta képernyő politika ellenőrzése, hulladék átvizsgálás, egyéb szimulált támadást mellőző (passzív) módszerek,
 - social engineering audit során végrehajtott szimulált támadások, aktív módszerek,
 - automatizált (folyamatosan alkalmazható) tesztek;
- a tréning hatékonyságának mérésére alkalmas lehet:
 - kérdőív a tréningfolyamat több pontján – longitudinális elemzés segítségével,
 - informális visszajelzés munkatárstól, ill. közvetlen vezetőjétől,
 - KPI, KRI, KRA, KPSI stb. mutatószámok [1]
 - ROI módszertan.

A biztonságtudatossági tréning elemeit jellegük és céljuk alapján tehát az 1. sz. táblázatban foglaltak szerint csoportosíthatjuk:

TRÉNINGELEM		JELLEGE	
		célzott	általános
CÉLJA	oktatás (új ismeretek)	tantermi képzés	tantermi képzés
	tájékoztatás (változásról)	e-learning tananyagok	kombinált (tantermi és e-learning)
	biztonságtudatosság fenntartása és javítása	biztonságtudatossági kampány	biztonságtudatossági program
	biztonságtudatossági szint felmérése	szimulált támadás, helyszíni bejárás	kérdőív, automatizált teszt
	hatékonysági visszamérés	KPI, KRI, KRA, KPSI stb. mutatószámok	<u>ROI módszertan</u>

1. táblázat Az információbiztonsági tréningelemek csoportosítása (saját szerkesztés)

A tréning célja tehát elsősorban az információbiztonsági kockázatok lehető legteljesebb méréséklése és megfelelő kezelése. Az informatikai folyamatszervezés során a kockázatmenedzsment és más vállalatirányítási szakterületektől kölcsönzött indikátorok kombinált alkalmazása révén újszerű módon azonosíthatók az információbiztonsági törekvések gyenge pontjai, számszerűsíthetővé válik a hiányosságok gazdasági hatása. [1]

⁵ Információbiztonsági szempontból pl. a következő biztonsági események szankcionálhatók:

- infokommunikációs, ill. informatikai eszköz elvesztése, rongálása,
- munkavégzéshez a munkáltató által biztosított eszköz nem rendeltetésszerű használata (pl. illegális szoftverhasználat, fájlok letöltése, nem megfelelő biztonsági beállítások alkalmazása),
- fenti eszközökön tárolt adatok kompromittálódása;
- incidensek, működési rendellenességek jelentésének elmulasztása;
- információ nem rendeltetésszerű felhasználása.

ÖSSZEGZÉS, KITEKINTÉS

A közlemény bemutatta a képzések értékelése során alkalmazott eszközök és módszerek közül a befektetés-megtérülési (ROI) módszertan tulajdonságait, alkalmazásának problémáit a magyarországi vállalati gyakorlatban. A szervezetek egyre inkább jövedelmi csomagként kezdenek a munkavállalókra tekinteni, akiknek a bérek és juttatások mellett a ráfordított képzési költségét is hozzáveszik a juttatásaikhoz – ez befektetés-megtérülési szemléletet, annak vizsgálatát, sőt nyomon követését fontosnak tartó attitűdöt feltételez a szervezetekben.

A közleményben megállapításra került, hogy a ROI módszertanilag is indokolható, megfelelő visszacsatolást nyújt a menedzsment számára a tréningek eredményességét illetően, ami elengedhetetlen az információbiztonság-tudatosság fejlesztésében szerepet játszó tréningek vonatkozásában. A közlemény meghatározta a ROI módszertan lehetséges helyét az információbiztonsági tréningek elemei között, részutatási eredményeket mutatott be a ROI vállalati alkalmazásának magyarországi gyakorlatát illetően, ezek által pedig előkészítette az információbiztonsági képzések területén lehetséges alkalmazhatóságának további részletes vizsgálatát.

A szerző szándéka a kutatás folytatása és publikálása olyan közleményben, amelynek főkulcsában az áll, hogy rendelkezésre álló mutatószámok, mutatószámrendszerek implementálása és testre szabása milyen mértékben, arányban és milyen módon segítheti a vezető és beosztottai erőfeszítéseinek hatékonyságát az információbiztonsági kockázatok kezelésének területén, és hogyan érdemes az indikátorok mérőpontjait helyesen megválasztani és kialakítani. A szerző célja a folytatással, hogy az információbiztonsági mutatószámok és -indexek jelenleg hiányzó módszertana kidolgozásra, egységesítésre kerülhessen.

A szerző szándéka még a kutatás eredményeinek további felhasználása olyan kontextusban, hogy a vizsgált ROI módszertan mennyiben alkalmazható a honvédelmi és rendvédelmi szervek speciális képzési igényei vonatkozásában, illetve hogyan illeszthető bele a hatékonyságmérés tevékenysége a Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program elsődlegesen haderőfejlesztési folyamataiba.

FELHASZNÁLT IRODALOM

- [1.] KOLLÁR Cs.: *Mutatószámok a szervezetek életében, különösen az információbiztonság területén* 111-125. o. In: BENCSIK, B., SÁBJANICS, I. (szerk.): *Digitális környezetünk fenyegetettsége a mindennapokban*, Dialóg Campus 2018. 152. o. ISBN: 9786155920899 <https://drkollar.hu/wp-content/uploads/2019/02/digitalis-kornyezetunk-fenyegetettsége.pdf> (letöltve: 2019. február 20.)
- [2.] POÓR J., BENCSIK A., SZRETYKÓ Gy., TERNOVSZKY F.: *Személyzetfejlesztési rendszer* 365-400. o. In: KAROLINY M., POÓR J. (szerk.): *Emberi erőforrás menedzsment kézikönyv: rendszerek és alkalmazások*. Wolters Kluwer, Budapest, 2010, 644 oldal, ISBN: 9789632951089
- [3.] The Kirkpatrick Model, <https://www.kirkpatrickpartners.com/Our-Philosophy/The-Kirkpatrick-Model>, (letöltve: 2019. március 3.)
- [4.] PHILLIPS, J., PHILLIPS, P.: *The Elusive ROI for Learning Through Technology*, 2014, <https://www.learningsolutionsmag.com/articles/1343/the-elusive-roi-for-learning-through-technology> (letöltve: 2019. március 6.)
- [5.] POÓR J. (szerk.): *Tréningek és képzések hatékonysága – Magyarország 2016. Kutatási zárójelentés*. SZIE GTK Menedzsment és HR Kutató Központ 2016. ISBN: 9789632696065 http://www.hsosz.hu/sites/default/files/aktualis/treninghatekonysag_magyarorszag_2016.pdf (letöltve: 2019. március 18.)

- [6.] BARTEL, A. P.: *Measuring the employer's return on investments in training: evidence from the literature*. Industrial Relations 39/3., 2000, pp. 502-524 <https://pdfs.semanticscholar.org/bf58/5b0bf389bb9a7bfbb90b7a3933d76e6b4c8d.pdf> (letöltve: 2019. március 18.)
- [7.] WILSON, M., HASH, J.: *Building an Information Technology Security Awareness and Training Program*, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology Gaithersburg, MD 20899-8933 October 2003, U.S Government Printing Office, Washington, 2003, <https://nvlpubs.nist.gov/nist-pubs/Legacy/SP/nistspecialpublication800-50.pdf> (letöltve: 2019. március 3.)
- [8.] OROSZI E. D.: *Social Engineering. Az emberi erőforrás, mint az információbiztonság kritikus tényezője*; Budapesti Corvinus Egyetem Gazdálkodástudományi Kar, Számítástudományi Tanszék 2008. 89. o. <http://docplayer.hu/3827943-Social-engineering-az-emberi-eroforras-mint-az-informaciobiztonsag-kritikus-tenyezoje.html> (letöltve: 2019. március 18.)
- [9.] KOLLÁR Cs.: *Social engineering a gyakorlatban - Manipulációk értelmezése a SPEAKING modellben*; Jel-Kép 2017/3. 62-77. o. https://communicatio.hu/jel-kep/2017/3/JelKep_2017_3_Kollar_Csaba.pdf (letöltve: 2019. február 20.)