„Információvédelem menedzselése” LXXXIII. Szakmai Fórum Budapest, 2018. november 21.

Az információbiztonsági tudatosság érettségi szintjének mérése szervezetekben

Tarján Gábor
Hétpecsét Információbiztonsági Egyesület, al-elnök

www.hetpecset.hu

Áttekintő tartalom

- Miért kell foglalkoznunk az információbiztonsági tudatossággal?
- Egy „tudományos” kutatás kérdései
- Kutatási eredmények
- Egy definíció
- Egy megtalált modell
- Egy továbbfejlesztett modell
- Egy on-line kérdőív
- A vizsgálat (kutatás) logikája

Mert ezt várja tőlünk a világ…

- **PCI DSS** (Payment Card Industry Data Security Standard): A 12.6-os § *„Az alkalmazottak legyenek tisztában a kártyabirtokosok információbiztonságának fontosságával*
  Képezzék az alkalmazottakat (pl. poszterek, levelek, emlékeztetők, találkozók és ösztönző rendezvények által)
  Igényeljék, hogy az alkalmazottak írásban elismerjék, hogy elolvasták és megértették a cég biztonsági szabályzatát és eljárásait."
- Sarbanes-Oxley Act (**SOX**): 404-es § (a).(a).(1) *„Ha a belső kontrollokról szóló jelentést nyilvánosságra kívánja hozni a jövőben, akkor most kezdjen el egy biztonságtudatossági képzési projektet."*
- Health Insurance Portability & Accountability Act (**HIPAA**) releváns pontja: A §164.308.(a).(5).(i) a következő elvárást fogalmazza meg: *„Vezessen be egy biztonságtudatosító és képzési programot a munkaerő mindent tagjára (beleértve a menedzsmentet is)."*
- **ISO/IEC 27001:2013** = MSZ EN ISO 27001:2014 (ISO 27001) szabvány „A" melléklet 7.2.2 pontja így fogalmaz: *„A szervezet minden alkalmazottjának, és ahol ez alkalmazható, a szerződéses munkatársaknak, megfelelő tudatosító képzésben és tréningben illetve a munkakörükhöz tartozó szervezeti szabályzatok és eljárások rendszeres frissítéseiben kell részesülniük."*

A Magyar Nemzeti Bank 26/2018. (VIII.16.) számú ajánlása

a pénzforgalmi szolgáltatások működési és biztonsági kockázataival kapcsolatos biztonsági intézkedésekről („PSD2 megfelelőség")

Képzési és biztonságtudatossági programok

7.4. Az MNB elvárja a pénzforgalmi szolgáltatótól, hogy képzési programot állítson össze a munkavállalók számára, hogy azok fel legyenek készülve a feladataik és felelősségeik vonatkozó biztonsági elvekkel és eljárásokkal összhangban történő ellátására, és ezáltal csökkenjen az emberi hiba, lopás, csalás, visszaélés és veszteség esélye. Elvárt továbbá, hogy a pénzforgalmi szolgáltató gondoskodjon arról, hogy a munkavállalók legalább évente – vagy szükség esetén gyakrabban is – részt vegyenek a képzési programban.

7.5. Az MNB elvárja a pénzforgalmi szolgáltatótól, hogy biztosítsa azt, hogy a 2.1. pontban megnevezett kulcspozíciókat betöltő munkavállalók évente – vagy szükség esetén gyakrabban – célzott információbiztonsági képzésben részesüljenek.

7.6. Az MNB elvárja a pénzforgalmi szolgáltatótól, hogy rendszeres időközönként biztonságtudatossági programokat dolgozzon ki és hajtson végre annak érdekében, hogy oktassa a munkavállalóit, és foglalkozzon az információbiztonsági vonatkozású kockázatokkal. Elvárt, hogy a programok keretében a pénzforgalmi szolgáltató írja elő munkatársai számára, hogy minden szokatlan tevékenységet vagy incidenst jelentsenek.

Egy „tudományos” kutatás kérdései

Q1: Hogyan írható le, hogyan értékelhető a szervezetekben az in
Q2: Mérhető-e a változás (javulás, romlás) egy szervezet életébe
Q3: Összehasonlíthatók-e a szervezetek az információbiztonsági
Q4: Támogatható-e a tudatosság szintjének értékelése hagyomá

Mely kontrollok megléte és működése jellemző az egyes érettsé
Milyen audit bizonyítékokat találhatunk egy szervezetben az egy

Kutatási eredmények – egy (saját) definíció

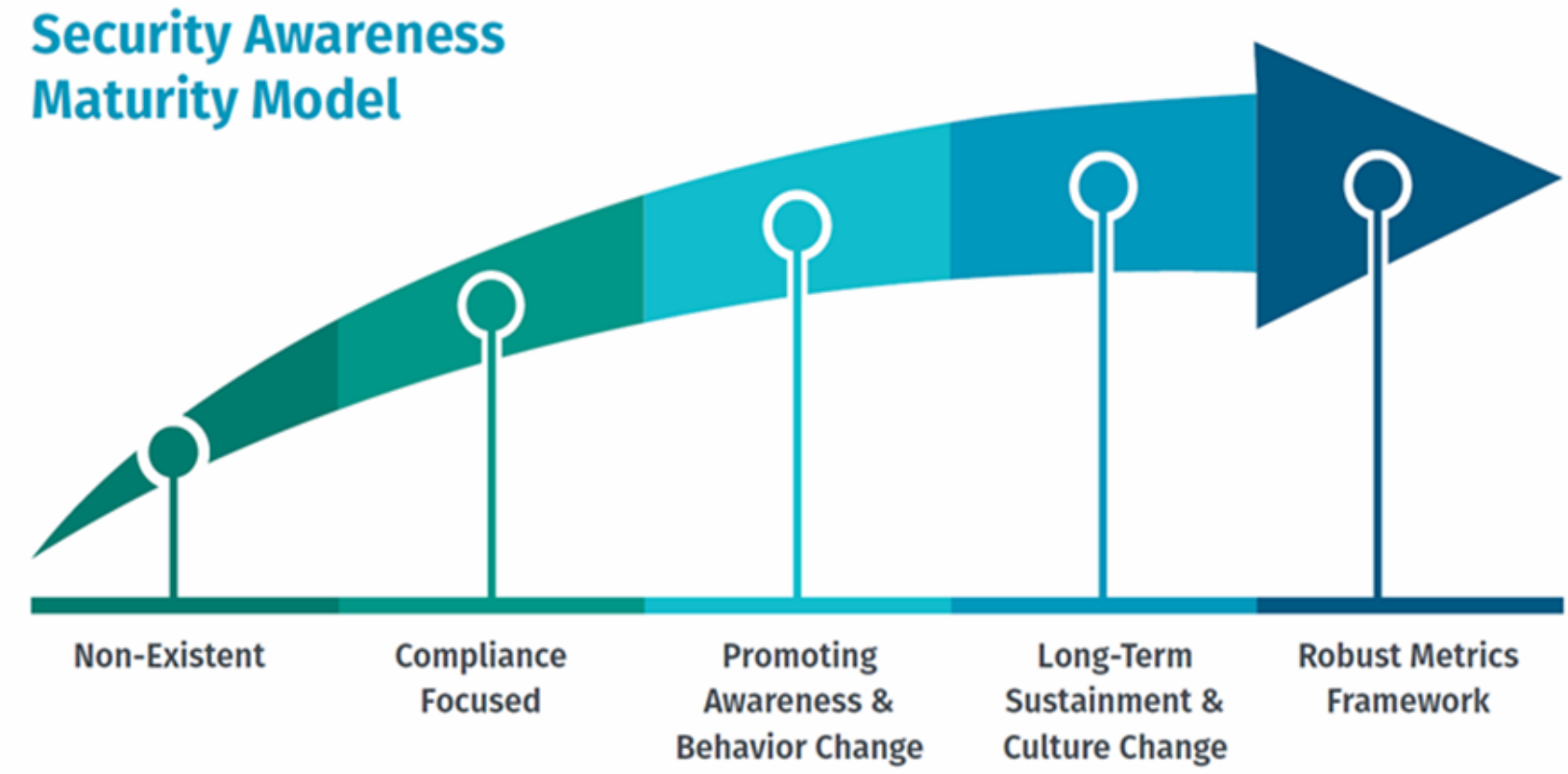
Az információbiztonsági tudatosság a szervezet érdekelt feleinek tudása és attitűdje a szervezet tulajdonában vagy kezelésében lévő információs javak védelmével kapcsolatban.

Information Security Awareness (ISA) is a knowledge and attitude of interested parties of an organization on the protection of information assets owned or managed by the organization.

- *Érdekelt felek?*
- *Tudás és attitűd?*
- *Saját vagy kezelt információk védelme?*

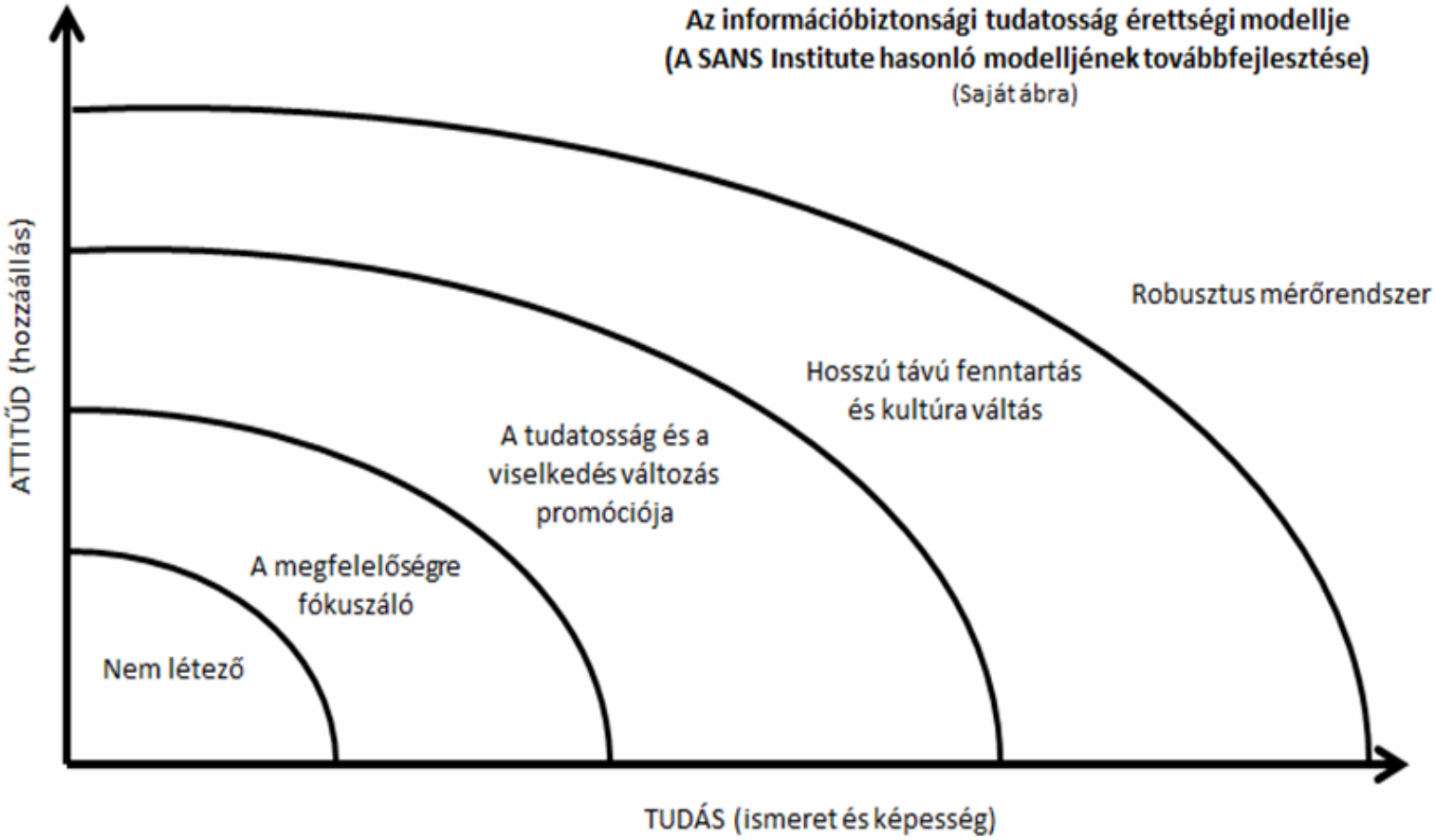
Kutatási eredmények – egy megtalált modell

SANS Institute - Az Információbiztonsági Tudatossági Érettségi Modell (2012.05.22. Lance Spitzner blogbejegyzése – 2017 – 2018…)



Kutatási eredmények – egy saját (továbbfejlesztett) modell

Az információbiztonsági tudatosság érettségi modellje
(A SANS Institute hasonló modelljének továbbfejlesztése)
(Saját ábra)

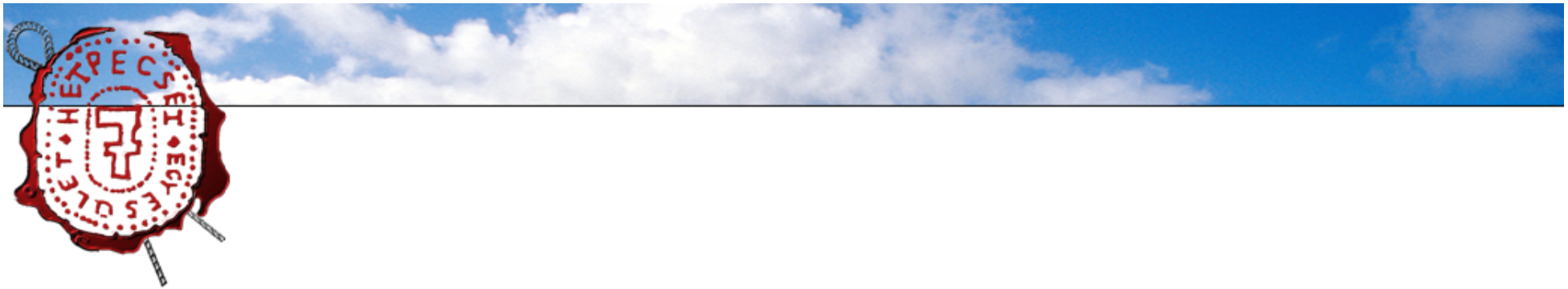


On-line kérdőívezés (kvantitatív kutatás)

- A Hétpecsét Információbiztonsági Egyesület levelező listájának tagjai (kb. 2200 személy, akik jelentős része gyakorló információbiztonsági szakember, szakauditor, tanácsadó)
- Az ISACA Budapest Chapter tagsága (kb. 550 személy, gyakorló auditorok, tanácsadók, kockázatmenedzserek az IT területén)
- Az EIVOK tagsága (kb. 150 személy, gyakorló információbiztonsági vezetők jellemzően a közigazgatási, államigazgatási szférából)

A vizsgálat (kutatás) logikája

1. Válaszadói (demográfiai) jellemzők begyűjtése
2. A válaszadó besorolja szervezetét a modell alapján
3. A válaszadó egy előre megadott listában megjelöli azokat a kontrollokat, melyek léte jellemző a szervezetére…
4. A válaszadó egy előre megadott listában megadja azokat az audit bizonyítékokat, melyeket fel tud a szervezete mutatni egy audit során…
5. *A (remélhetően) statisztikai méretű mintán vizsgáljuk az érettségi szint besorolás és a jellemző kontrollok és az audit bizonyítékok kapcsolatát (kapcsolati erősségét)!*



Köszönöm a figyelmet!

Tarján Gábor

Gabor.Tarjan@magicom.com