HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET
INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

EIVOK-7. Információbiztonsági Szakmai Fórum
2018.11.29.

Az információbiztonsági tudatosság érettségi szintjének mérése szervezetekben (egy kutatás margójára)

Tarján Gábor
Ügyvezető partner
www.magicom.hu

A betöltött munka-szerepeim (ahol hivatalból találkozom az információbiztonsági tudatossággal)

- **Ügyvezető partner** (az ügyvezető igazgató belső tanácsadója)
- **Szolgáltatás menedzser** (néhány futó outsourcing szerződés teljesítésének menedzselése multinacionális környezetben – pl. amerikai ügyfél céggel)
- **Információbiztonsági tanácsadó** és tanácsadási projektek témavezetője (információbiztonsági oktatások, auditok és rendszerépítési tanácsadási projektek vezetője és közreműködő tanácsadója)
- **Információbiztonsági vezető** (az ISO 27001 alapú irányítási alrendszer gazdája és felelőse vagyok)
- **DPO** (Data Protection Officer – Adatvédelmi tisztviselő)
- **Egyetemi oktató, szakvezető**
  - METU – Executive MBA for IT Szak, szakvezető
  - NKE – EIV képzés, „Kockázatmenedzsment” tárgy, tantárgyfelelős
  - BCE – alkalmi előadások BSc, MSc, szakmai továbbképzések előadójaként
- Hétpecsét Információbiztonsági Egyesület - **alelnök**

Miért kell tudatossággal foglalkoznunk az EIVOK-ban? (1.)

- Törvényi előírás: *Az állami és az önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 11. § (1) bekezdésének g) pontja értelmében a szervezet vezetőjének gondoskodnia kell az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai információbiztonsági ismereteinek (biztonságtudatosság) szinten tartásáról.*

Miért kell tudatossággal foglalkoznunk az EIVOK-ban? (2.)

- a 41/2015. (VII.15.) BM rendelet) meghatározza, hogy „*az érintett szervezet annak érdekében, hogy az érintett személyek felkészülhessenek a lehetséges belső fenyegetések felismerésére, az alapvető biztonsági követelményekről tudatossági képzést nyújt az elektronikus információs rendszer felhasználói számára*", mely képzésnek nem csak a belépéskor kell megtörténnie, hanem az ismeretek felfrissítése és aktualizálása érdekében rendszeresen (célszerűen évente) meg kell tartani.

Egy „tudományos” kutatás kérdései

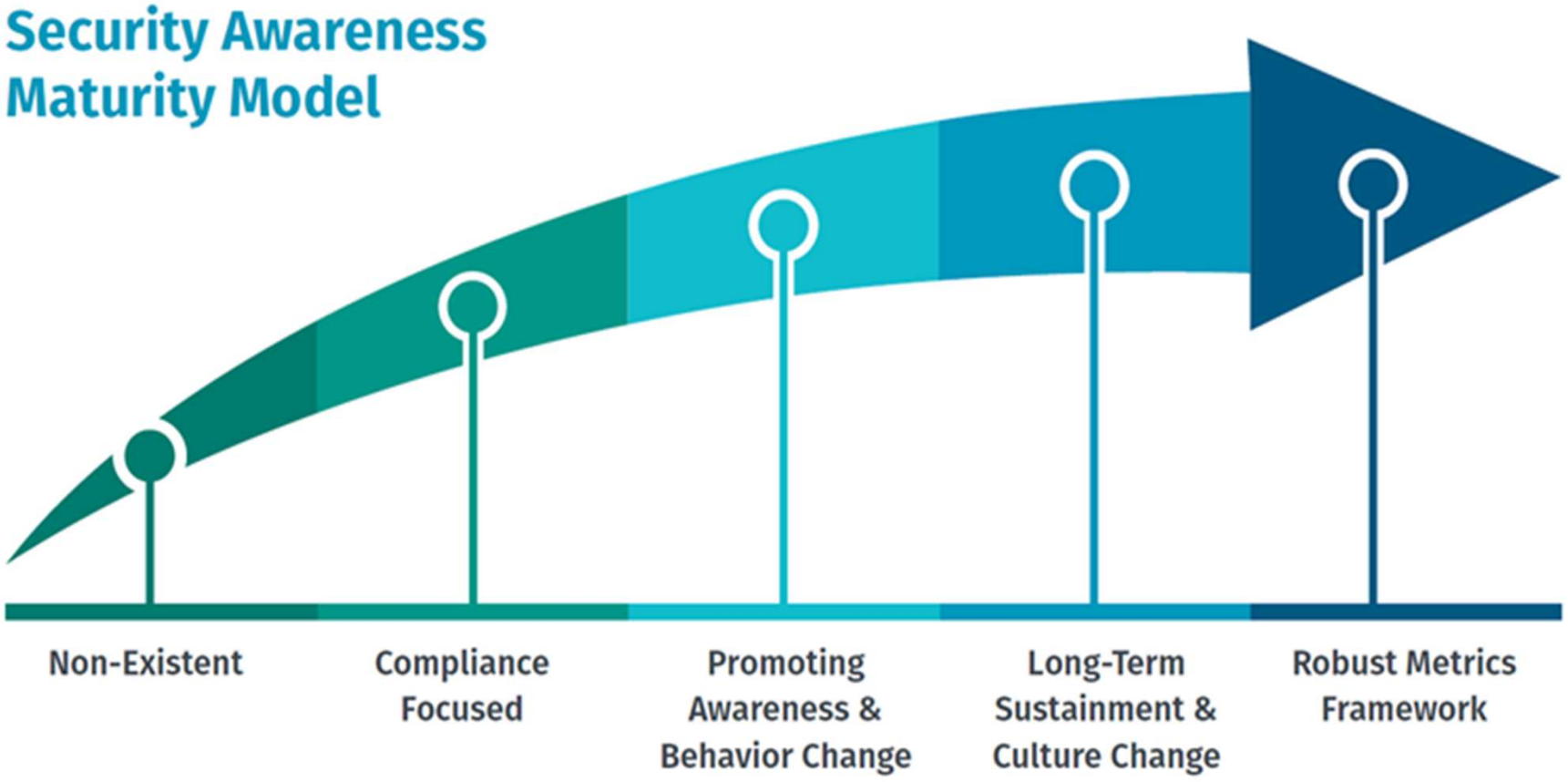
- Q1: Hogyan írható le, hogyan értékelhető a szervezetekben az információbiztonsági tudatosság szintje, minősége a szervezet szintjén?
- Q2: Mérhető-e a változás (javulás, romlás) egy szervezet életében a tudatosság érettségi szintje vonatkozásában?
- Q3: Összehasonlíthatók-e a szervezetek az információbiztonsági tudatosság érettsége szempontjából szervezeti szinten?
- Q4: Támogatható-e a tudatosság szintjének értékelése hagyományos audit eszközökkel (pl. ellenőrző listák)?
- Mely kontrollok megléte és működése jellemző az egyes érettségi szinteken?
- Milyen audit bizonyítékokat találhatunk egy szervezetben az egyes jellemző kontrollok működésére?

Információbiztonsági tudatosság / Information security awareness (ISA)

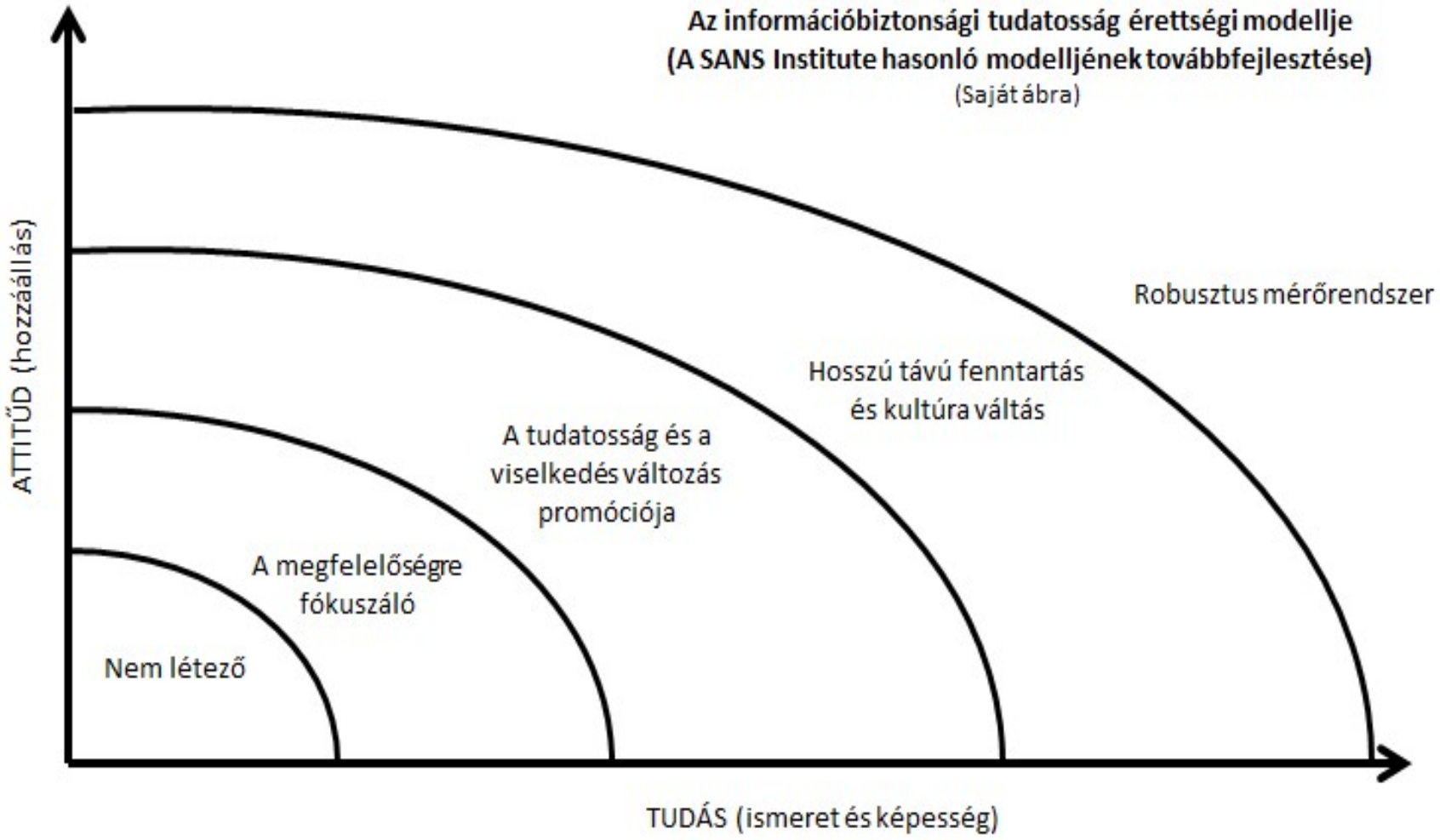
Az információbiztonsági tudatosság a szervezet érdekelt feleinek tudása és attitűdje a szervezet tulajdonában vagy kezelésében lévő információs javak védelmével kapcsolatban. / *ISA is a knowledge and attitude of interested parties of an organization on the protection of information assets owned or managed by the organization.*

- Érdekelt felek?
- Tudás?
- Attitűd?
- Saját tulajdonú vagy kezelt információk?

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



A SANS Institute modelljének továbbfejlesztése (TG - 2018)



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
(06-20-502-7775)
gabor.tarjan@magicom.com