SVEUČILIŠTE U ZAGREBU
FAKULTET ORGANIZACIJE I INFORMATIKE
V A R A Ž D I N

HR - 42 000 Varaždin
Pavlinska 2

tel: +385 42 390 800
fax: + 385 42 213 413

ured-dekana@foi.hr
www.foi.unizg.hr

Poziv na promociju knjige „Korporativna informacijska sigurnost“

KORPORATIVNA INFORMACIJSKA SIGURNOST

(INFORMATION SECURITY GOVERNANCE)

Iz tiska je izašla knjiga **Korporativna informacijska sigurnost,** čiji su izdavači Fakultet organizacije i informatike Sveučilišta u Zagrebu i Zavod za informatiku Hrvatske. Nastala je kao rezultat rada skupine autora okupljenih oko prof. dr.sc. Zdravka Krakara, a njeni recenzenti su uvaženi profesori FER-a i FOI-a.

Slikovito rečeno, područje informacijske sigurnosti je meta koja se stalno kreće. Ako se promatra njegov razvoj, do sada su bile 4 faze. Prvu fazu činilo je prepoznavanje potrebe tzv**. IT sigurnosti**, u kojoj su dominirali *tehnički aspekti* zaštite, u to vrijeme, skupe računarske opreme. Nositelji ove sigurnosti bilo je tehničko osoblje IT operative. Za drugu fazu, karakteristično je da se sigurnost fokusirala na podatkovne sadržaje poslovnog sustava, budući su se u njenim bazama podataka nalazili vitalni podaci, pa se ova faza može nazvati **sigurnost podataka.** Nositelji njene odgovornosti bili su stručnjaci koji su radili na tzv. sistemskim poslovima u IT- u. Daljnji razvoj IT sigurnosti postignut je pojavom niza metoda i normizacijom (standardizacijom) pojedinih dijelova sigurnosti. Takve metode osobito su se razvile za područja procjenjivanja IT rizika. Ova faza može se nazvati **sigurnost informacija,** za čiju odgovornost je nadležno vodstvo IT funkcije. U četvrtoj fazi došlo je do prerastanja IT sigurnosti u informacijsku sigurnost i daljnjeg razvoja primjene standarda (normi) u ovom području. Nastao je termin *informacijska imovina* i disciplina *Upravljanje informacijskom sigurnošću* **(ISMS),** za čiju odgovornost je postala nadležna uprava poslovnog sustava. Reprezentant ove faze jesu ISO/IEC 2700x sustavi. Politike informacijske sigurnosti, sigurnosne procedure, organizacija za sigurnost, CISO, auditi sigurnosti, certifikacija sustava sigurnosti, neka su obilježja ove faze. Nastupajuću, petu fazu odnosa prema informacijskoj sigurnosti, čini pojava i primjena koncepta **korporativne informacijske sigurnosti** (eng. Information Security Governance*)*. Potencijalne i stvarne prijetnje informacijama, najvrijednijoj imovini poslovnog sustava, postale su tako velike, osobito u uvjetima globaliziranog i komunikacijski potpuno povezanog poslovanja, da predstavljaju prioritetni poslovni rizik. Zbog toga je nužan novi pristup informacijskoj sigurnosti. Osnovne značajke ove faze jesu: nove doktrine i metode sigurnosti, kao što su ISO/IEC 27014, *COBIT®5* for Information Security, te novi modeli SSE CMM® (System Security Engineering Capability Maturity Model), ISM3® (Information Security Management Maturity Model) i ISO/IEC 38500.

Knjiga se bavi ovom, petom fazom odnosa prema informacijskoj sigurnosti. Na hrvatskom jeziku uopće još nema radova objavljenih na ovu temu. Ima 464 + 15 stranica, raspoređenih u slijedećih 11 poglavlja:

- Uvod u temu
- Korporativno upravljanje
- Modeli korporativnog upravljanja informatikom
- Korporativno upravljanje informacijskom sigurnošću
- Korporativna informacijska sigurnost i norme ISO/IEC 270xx
- Korporativna informacijska sigurnost i COBIT®5
- Korporativna informacijska sigurnost, ITIL i ISO/IEC 20000
- Upravljanje informacijskim i ICT rizicima
- Organizacija i dokumentacija sustava korporativne informacijske sigurnosti
- Kompetencije za informacijsku sigurnost
- Korporativna informacijska sigurnost i nove tehnologije.

Prema ocjeni recenzenata knjiga predstavlja vrlo uravnoteženi prikaz metoda korporativne informacijske sigurnosti i bogate vlastite prakse 5 autora u različitim područjima ovog kompleksa. Vrlo je bogato ilustrirana, trećina slika je u bojama, tako da je postignuta i maksimalna vizualizacija promatrane problematike. Podjednako je namijenjena stručnoj, znanstvenoj i obrazovnoj javnosti. Knjiga se može nabaviti preko ZIH-a (www.zih.hr) ili FOI-a (www.foi.hr)