dnevi slovenske informatike

"Ustvarimo nove rešitve!"

Kongresni center Grand hotel Bernardin
Portorož | Slovenija | 16. - 18. april 2012

19. konferenca
Dnevi slovenske informatike

Model kvantitativnega merjenja ocene tveganj informacijske varnosti

dr. Rok Bojanc, ZZI d.o.o.

18. 04. 2012

slovensko društvo informatika

ZZI d.o.o.

Carinska uprava Slovenije
- Carinski IS (Uvoz, izvoz, tranzit,…)
- E-poslovanje s partnerji od 1996 (EDI)
- Brezpapirno poslovanje od 2001
- Carinski portal

Carinska uprava Črne Gore
- Carinski IS od 2003 (uvoz, izvoz, tranzit,…)
- E-poslovanje s partnerji od 2006 (EDI)

Carinska uprava Srbije
- Svetovanje na področju uvedbe SOA in EU zahtev
- TARIS

Statistični urad Slovenije
- E-poročanje Intrastat
- E-poročanje ISIS

Ministrstvo za zunanje zadeve Republike Slovenije
- Programska oprema VIS

Stanovanjski sklad RS
- Storitve e-hrambe dokumentov
- Pilotski projekt upravljanja procesov

Zavod za pokojninsko in invalidsko zavarovanje RS
- Vzpostavitev intranet portala na IBM tehnologiji

Državni zbor RS
- Tehnološka konsolidacija spletnega mesta
- Aplikativna podpora procesom

Storitev elektronske hrambe dokumentov

eHramba.si

Storitev elektronske izmenjave sporočil

zzinet

Brezpaprino poslovanje v oblaku

eStoritve

- **eKatalog**
- **eImenik**
- **eNabiralnik**
- **eHramba**
- **eIzmenjave**

Kakšen je "varen" sistem?

"Lahko stanujete v najbolj varni soseski, vendar ko enkrat priklopite tisti kabel na internet, takrat se znajdete v najhujši možni soseski."

- Michael Howard

"Edini sistem, ki je zares varen, je takšen, ki je izključen in izklopljen iz električnega omrežja, zaklenjen v sefu, narejenem iz titana, zakopan v betonskem bunkerju, ki ga obdaja plast živčnega plina in zelo dobro plačani oboroženi stražarji. Vendar niti takrat ne bi zastavil svojega življenja zanj."

- Gene Spafford

Izhodišča

100% varnosti ni mogoče doseči!

Ključni vprašanji:

- Kako varen je sistem?
- Kakšno stopnjo varnosti želimo imeti?

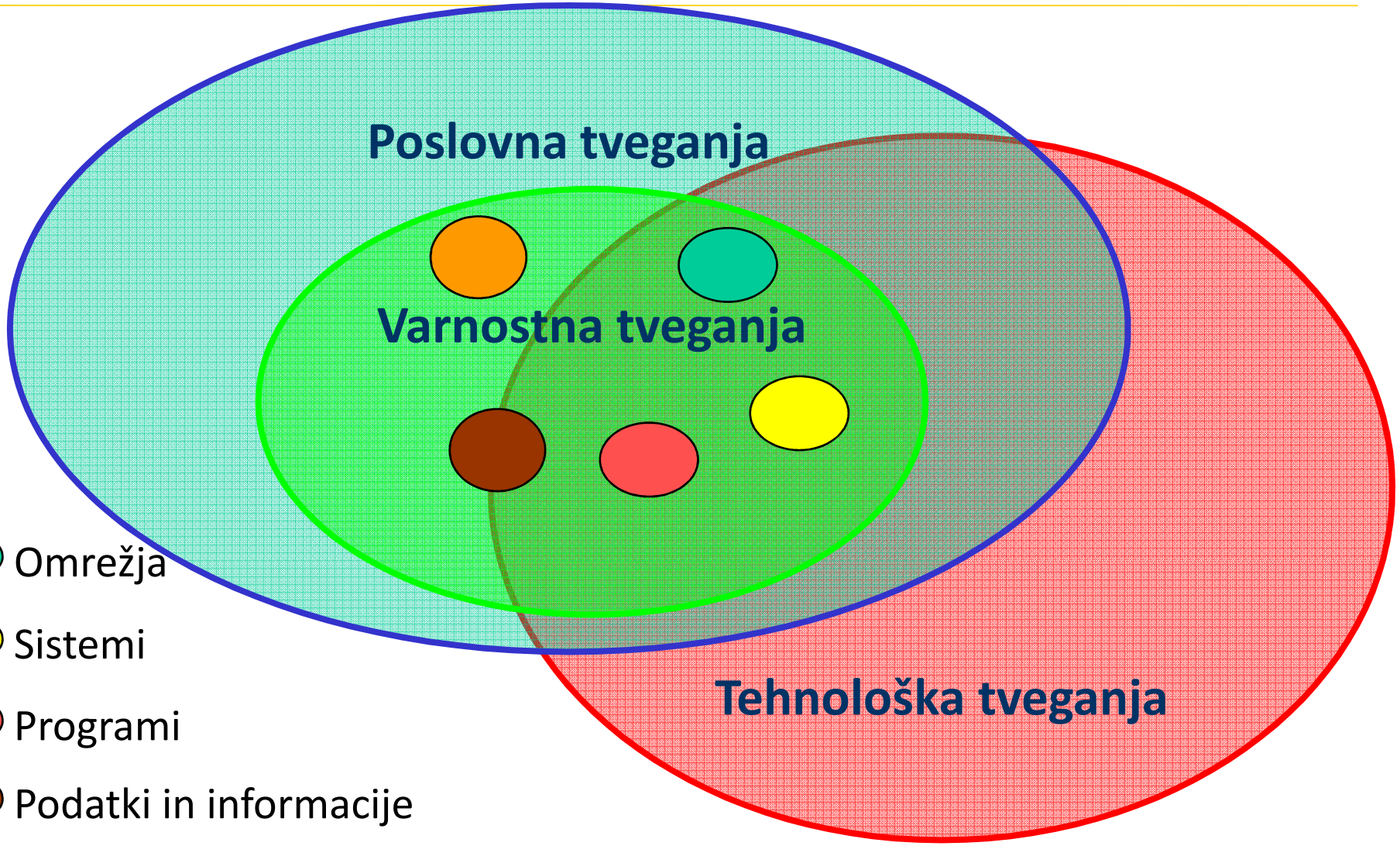
Odgovor (by Dan Geer):

- Dovolj dobro varnost :)
- Zelo težko je določiti, kaj je dovolj dobro

Popolna varnost = stopnja varnosti, ki je za podjetje sprejemljiva

- Upoštevati kompromis varnost – uporabnost

Varnostna tveganja



Vprašanja povezana s tveganji

- Kako lahko podjetje postane varno?
- Katera stopnja varnosti je ustrezna?
- Koliko denarja naj podjetje investira v varnost?
- Ali podjetje zapravi dovolj denarja, da hekerjem prepreči vdor v sistem?
- Ali podjetje zapravi preveč?
- Ali podjetje zapravi varnostni proračun za ustrezne stvari?
- Ali je za podjetje bolj ekonomično, da izbere varnostni ukrep A ali B?

Iščemo odgovor na vprašanja

- Predstavljena metodologija za kvantitativno merjenje ocene tveganj
- Omogoča izbiro optimalnega varnostnega ukrepa
- Omogoča medsebojno ekonomsko vrednotenje investicij v varnostne ukrepe

Izbira ustrezne metode

Kvantitativne metode

(numerične vrednosti)

+ omogoča cost-benefit analizo
+ rezultati so taki, da jih razume vodstvo

- pomanjkanje standardnih metod
- težko je vse izraziti v denarnih enotah
- izračuni so kompleksni in zahtevajo čas
- potrebuje dobre zgodovinske podatke
- lahko nas zavede numerična vrednost

Kvalitativne metode

(opisne ocene)

+ enostavni izračuni
+ manj človeških virov
+ primernejši za manjša podjetja

- splošnost rezultatov
- subjektivne ocene

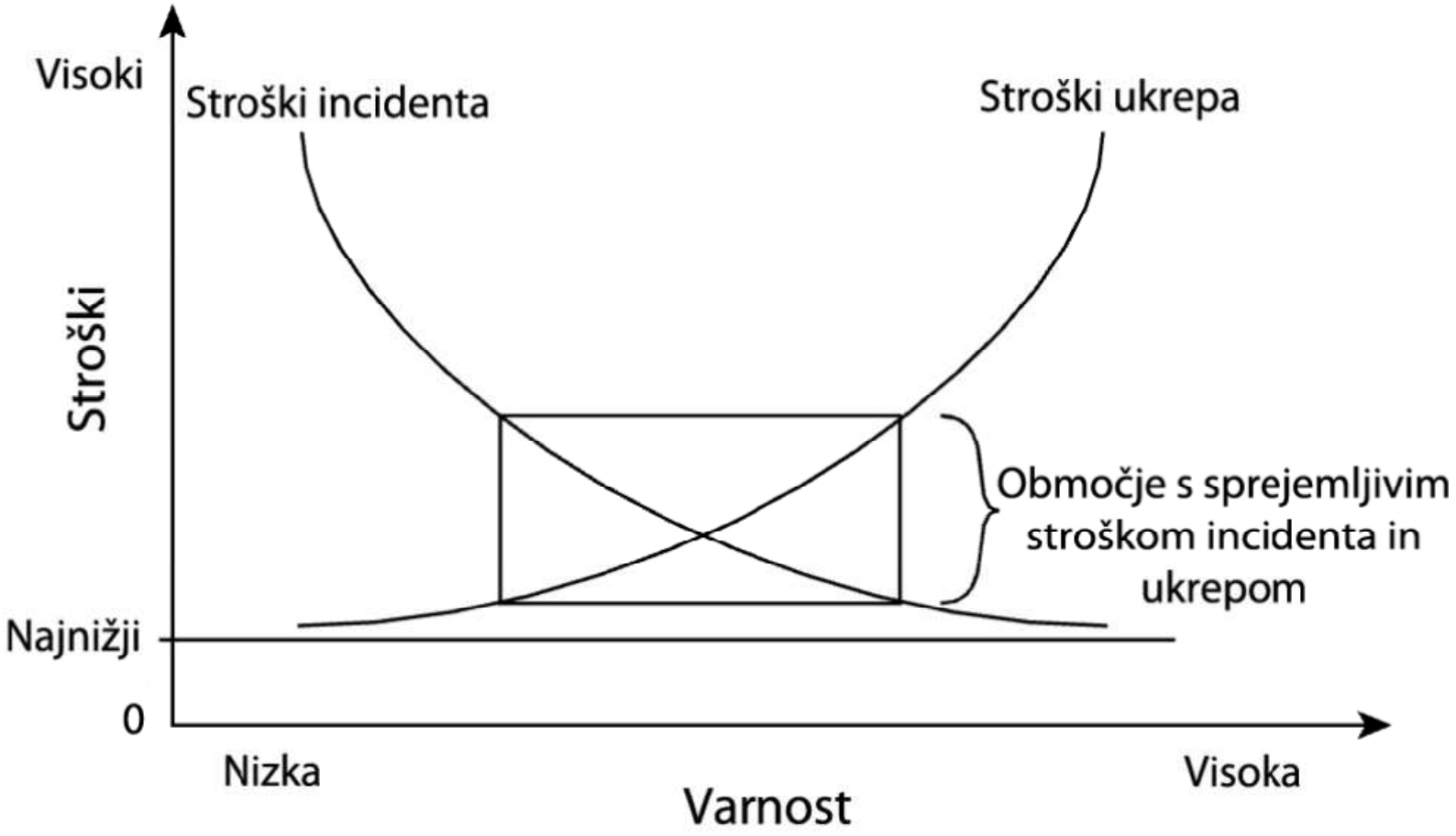
Ekonomski pristop k reševanju informacijske varnosti

- V preteklosti: tehnološki vidik informacijske varnosti
- Pred desetimi leti: Premik iz **tehnično mogoče -> ekonomsko optimalno**

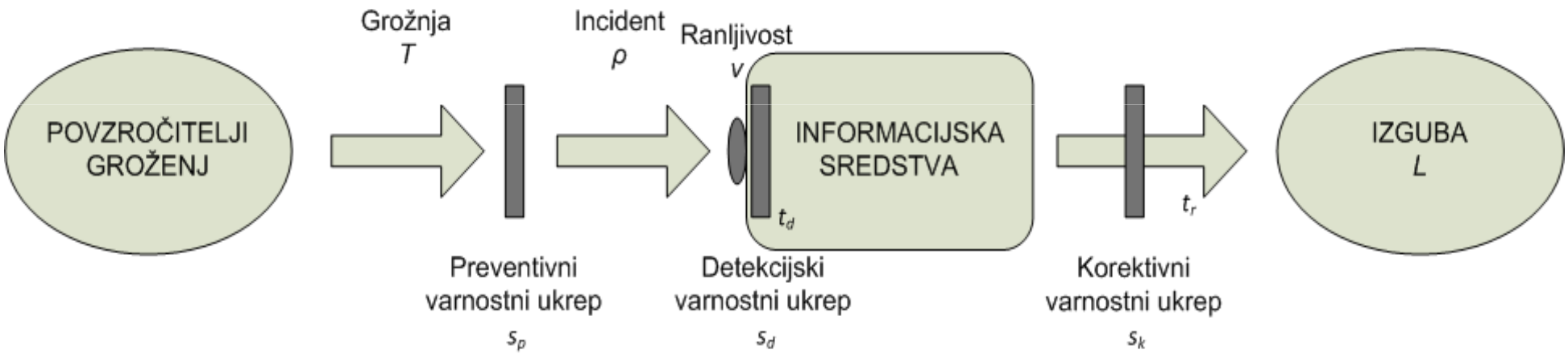
Prednosti ekonomskega pristopa

- Lahko odgovori na vprašanja:
  - Koliko investirati in v katero rešitev investirati?
  - Kakšna stopnja varnosti je ustrezna?
  - V katero rešitev investirati?
  - Zakaj se uvedba določene tehnologije ni prejela?
- Ekonomski pristop bližje vodstvu
  - Povzročena škoda predstavljena kot finančna izguba, ne kot tehnična analiza
  - Vodstvo pogosto zahteva racionalni pristop za varnostne investicije

Iskanje optimalne rešitve



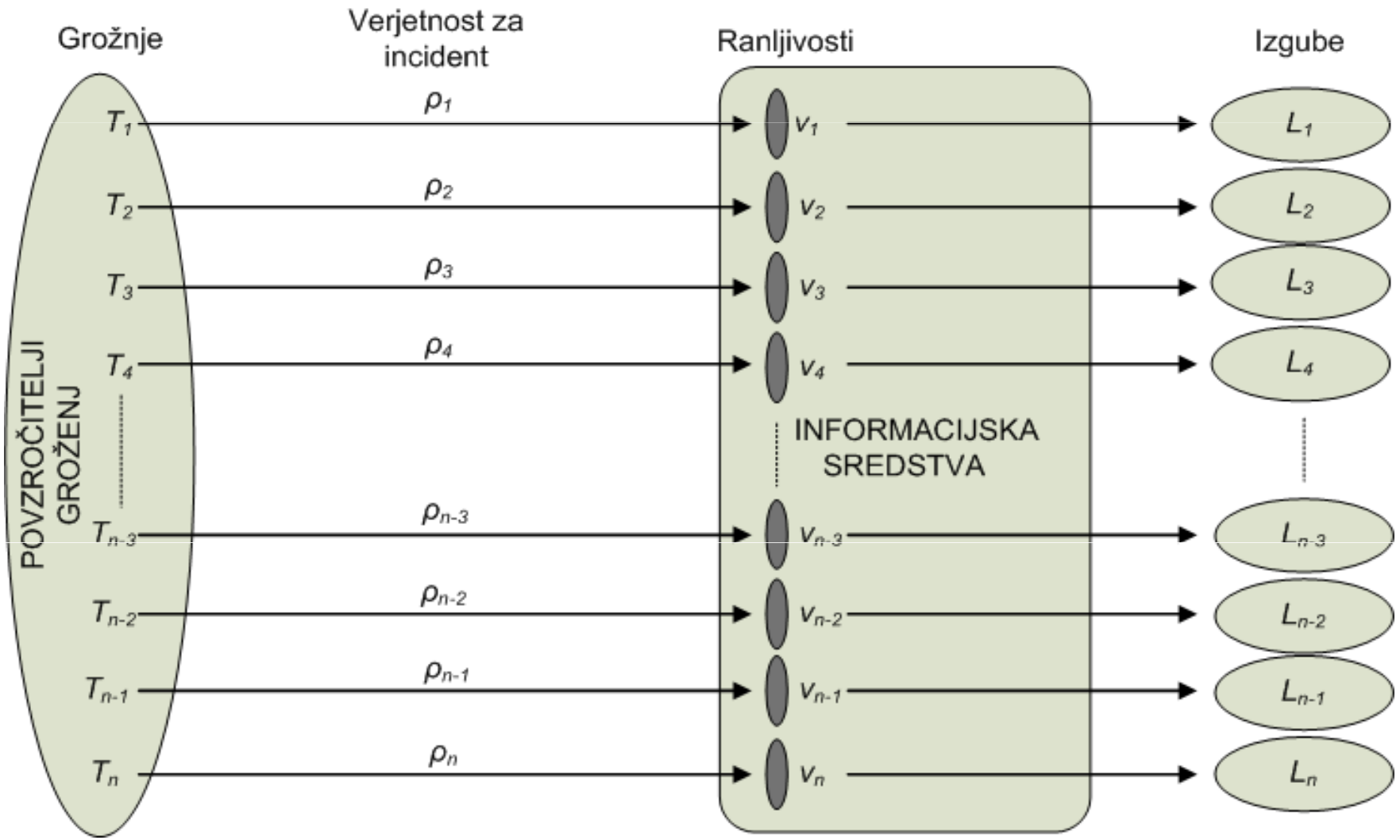
Model kvantitativnega merjenja ocene tveganj



Osnovni elementi modela

- Informacijska sredstva
  - Identifikacija, določitev vrednosti
- Grožnje
  - Povzročitelji grožnje
- Ranljivosti
- Izguba
- Varnostni ukrepi

Model kvantitativnega merjenja ocene tveganj 2



Metodologija

Določitev kvantitativnih vrednosti za incident

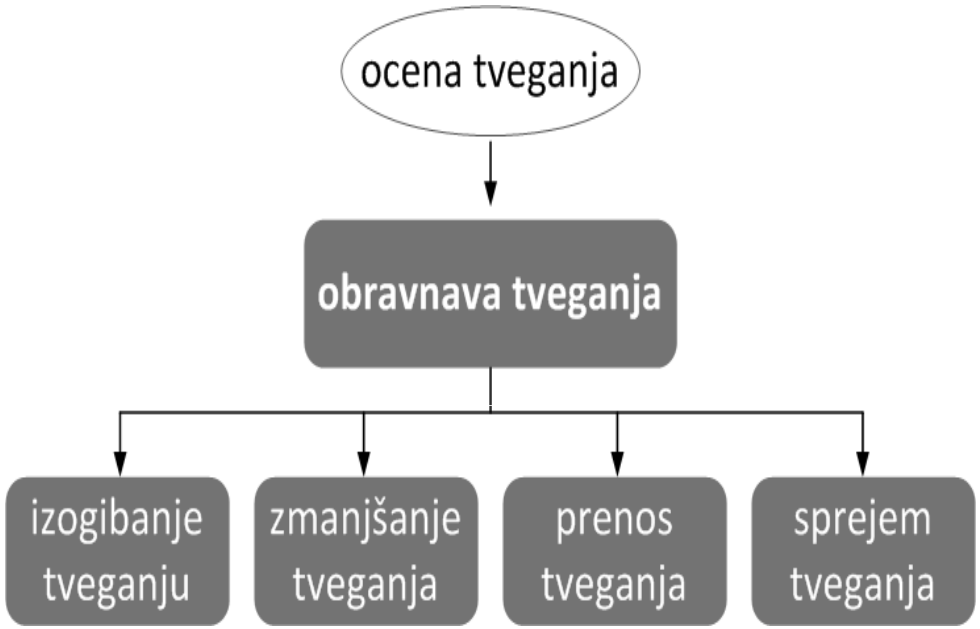
- Funkcija verjetnosti za grožnjo in ranljivosti
  - Ranljivosti za informacijska sredstva
  - Verjetnost za izvedeno grožnjo

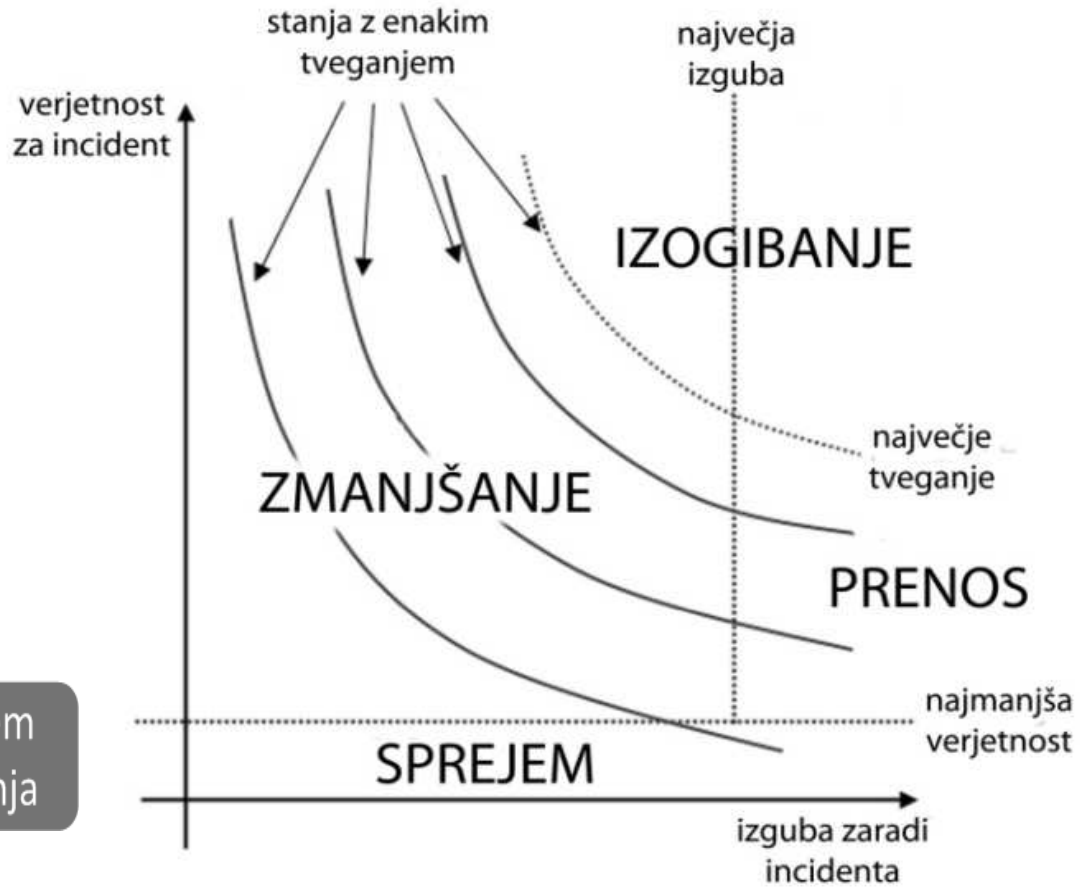
Ocena izgube v primeru incidenta

- Takojšnje izgube
  - Strošek zamenjave opreme (kraja, uničenje, izguba, okvara…)
  - Strošek popravila
  - Izguba prihodkov podjetja
  - Izguba produktivnosti podjetja
  - Izguba zaradi nespoštovanja zakonskih predpisov
- Posredne izgube
  - Lahko zelo velike

Obvladovanje varnostnih tveganj

Tveganje je funkcija verjetnosti za incident in izgube ob incidentu





Vrste varnostnih ukrepov

Preventivni varnostni ukrepi

zmanjšujejo verjetnost za varnostni incident (zmanjšujejo ranljivost)

- Varnostna politika
- Šifriranje
- Digitalni podpisi
- Varna arhitektura
- Ažurno posodabljanje
- Požarni zid
- IPS sistemi
- Avtorizacija
- Protivirusni programi
- Izobraževanje uporabn

Korektivni varnostni ukrepi

zmanjšujejo izgubo zaradi uspešnega incidenta (zmanjšujejo čas popravila)

- Okrevalni načrt
- Načrt neprekinjenega poslovanja
- Varnostno kopiranje
- Uporaba programa za prijavo incidentov
- Redundančni sistemi
- Zavarovanje tveganja
- Nadomestni sistemi električnega napajanja

Detekcijski varnostni ukrepi

zmanjšujejo čas za odkritje incidenta

- IDS sistemi
- Limanica (honeypot)
- Zaznavanje vdorov na računalnikih

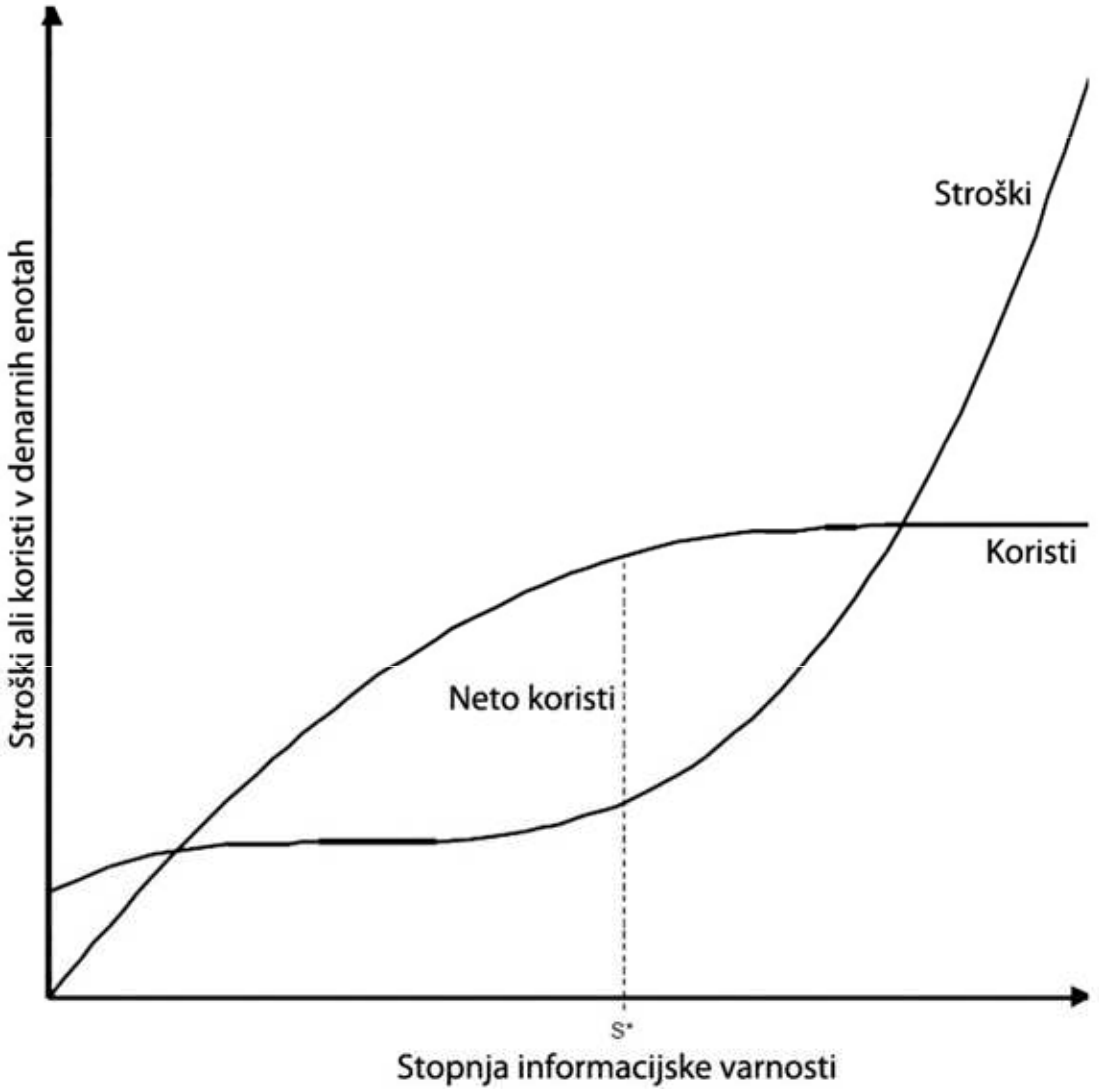
Analiza stroškov in koristi ukrepa

Strošek ukrepa

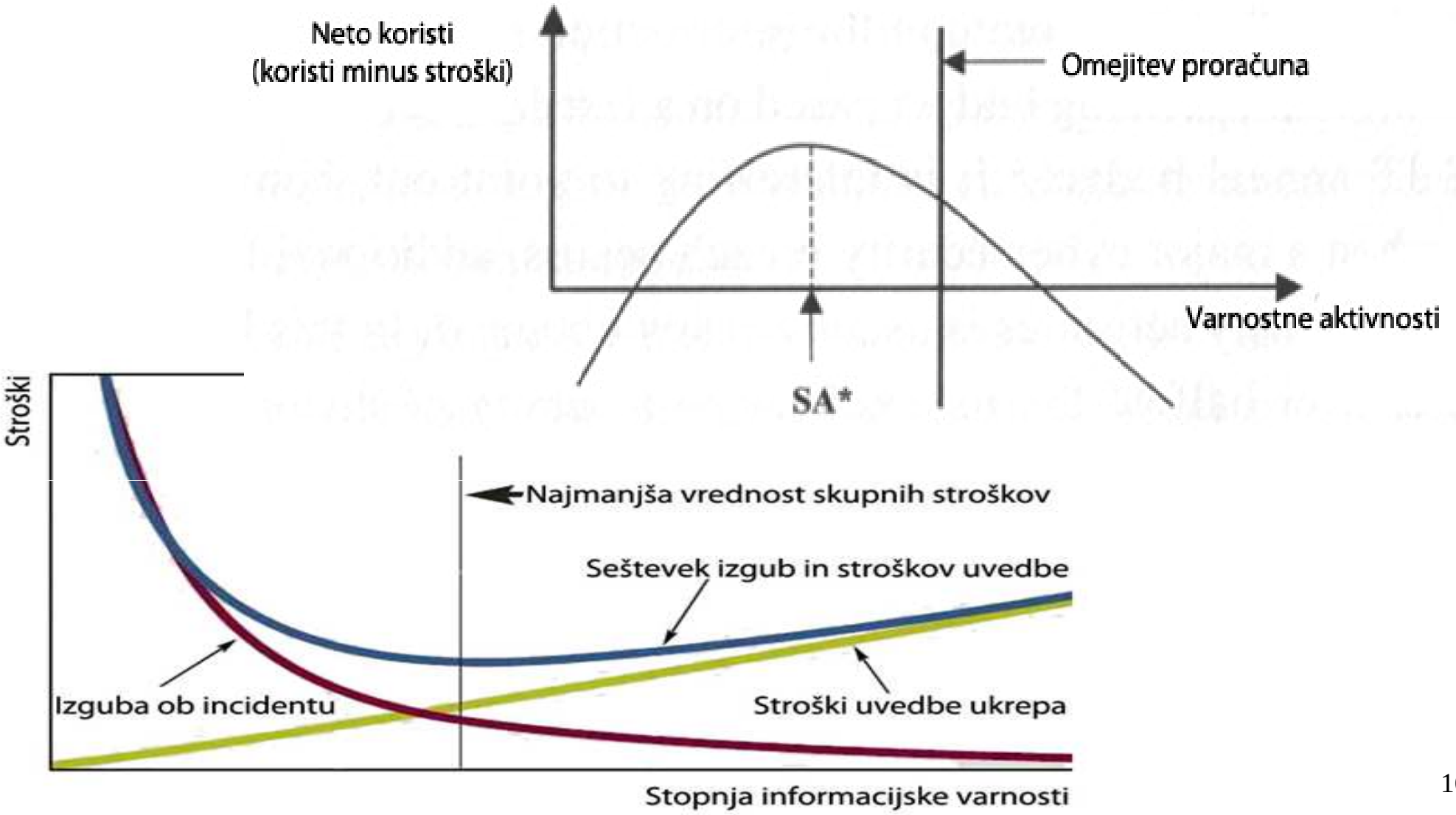
- Strošek nabave
- Strošek uvedbe, testiranja, izobraževanja
- Strošek nadgradenj in popravkov
- Strošek vzdrževanja
- Ostali stroški povezani z uvedbo

Koristi uvedbe ukrepa

- Ni mogoče enostavno meriti
- Razlika tveganja pred in po uvedbi varnostnega ukrepa

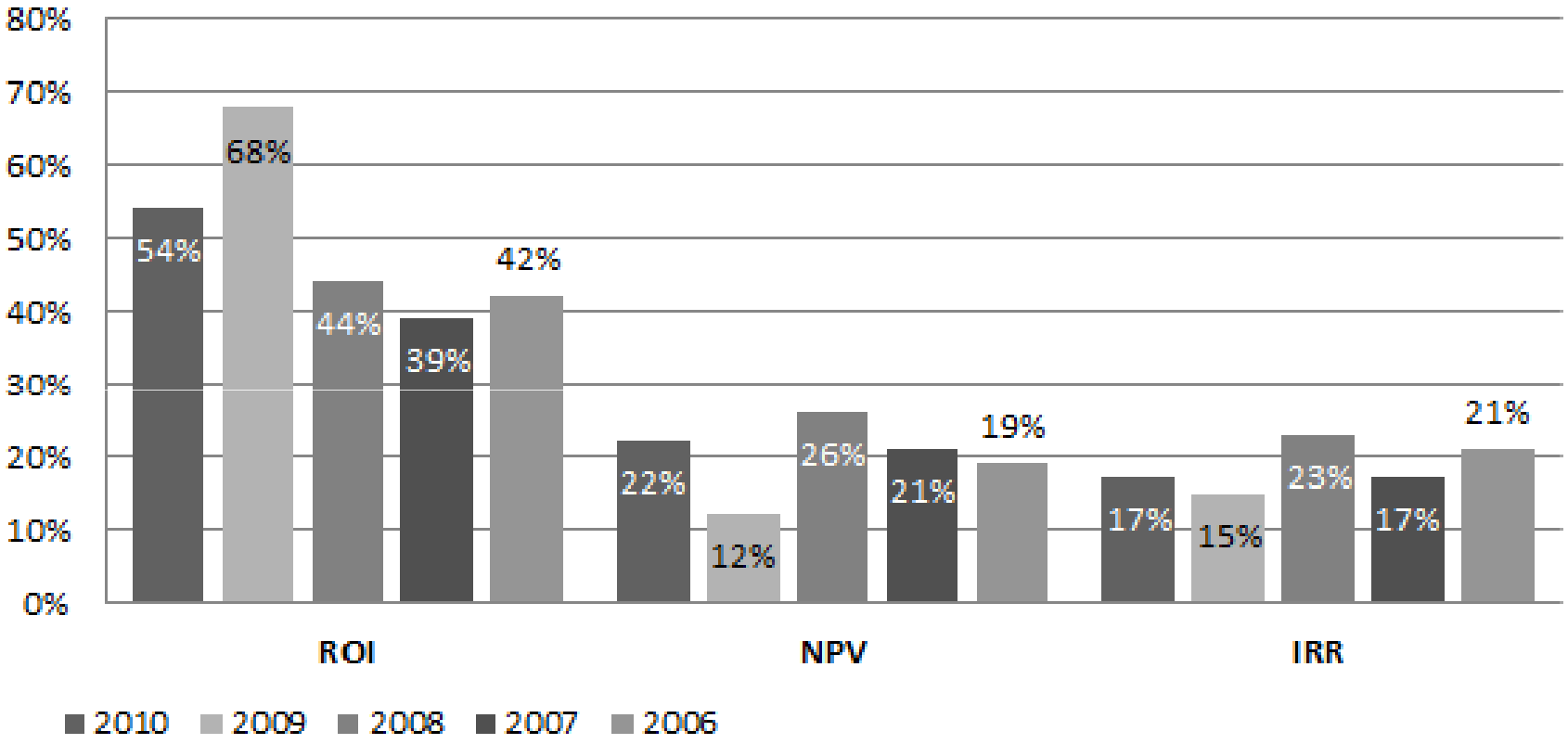


Iskanje optimalne stopnje varnosti



Merjenje donosnosti varnostnega ukrepa

- Donosnost investicije (ROI)
- Neto sedanja vrednost (NPV)
- Notranja stopnja donosa (IRR)



Zaključek

- Obvladovanje tveganja (ocena in obravnava) je ena od temeljnih aktivnosti upravljanja informacijske varnosti (zahteva ISO 27001…)
- Večina obstoječih metod za oceno tveganja uporablja kvalitativen pristop
  - Ne omogoča analizo stroškov in koristi
- Kvantitativna oceno tveganja omogoča oceniti optimalno količino potrebnih vlaganj (stopnjo varnosti)
  - Metodologija za vrednotenje in izbor varnostnih rešitev omogoča izbiro optimalne varnostne rešitve
  - Omogočena primerjava in vrednotenje različnih obravnav tveganja (zmanjšanje, prenos, izogibanje, sprejem)
  - Ekonomsko vrednotenje varnostnih rešitev podprto s kazalci ROI, NPV in IRR

Hvala za vašo pozornost !

Vprašanja?

Pripombe?

Predlogi?

ZZI eStoritve

Več **kot 600 podjetij** uporablja ZZI eStoritve in omrežje od **1999**

– **Države**: Slovenija, Avstrija, Makedonija, Črna Gora,Hrvaška, Švedska…

– **PARTNERSKA omrežja** izmenjave - Mednarodni in lokalni x.400, Panteon (Mercator, Tuš, Špar,..), GXS, EBA, ….

– **UPORABNIKI omrežja**: Gorenje, Merkur, Intereuropa, Shenker, Hidria, Impol, Acroni, IskraAvtoelektrika, Lek, Kemofarmacija, Unika, Istrabenz Plini, Helios, Henkel, Iskraemeco, Renault Nissan, Sava, Salus,Tosama, Mercator, Tuš, Spar, …, **Institucije**: Carinske uprave, Statistični uradi, Davčne uprave,…

– **Obseg izmenjave cca.** 1.000.000 dokumentov (mesečno)

– **Podpora povezovanja**: kreiranje in distribucija računov, eNaročanje v trgovini in proizvodnji, logistika, B2G (eCarina, eDavki, eZdravje, …)

– **ERP ponudniki**: Pantheon (Datalab), Infor, SAP, Navision, SAOP, ProBit…

– Podpora varnostnim standardom **podpisa in časovnega žiga** (x.509)