Consulting. Integration. Outsourcing.

»NIČ PRSTNIH ODTISOV, NOBENE OSEBNE IZKAZNICE, NOBENEGA ZDRAVSTVENEGA ZAVAROVANJA.
GOSPA, BOJIM SE, DA VAŠ ŠE NEROJENI OTROK PREDSTAVLJA HUDO VARNOSTNO TVEGANJE«

Matej Saksida; CISM, CiS S&T Slovenija d.d.

Nekaj besed o predavatelju…

Matej Saksida

Svetovalec za inf. varnost
Vodja informacijske varnosti

matej.saksida@snt.si
www.snt.si

Certifikacije

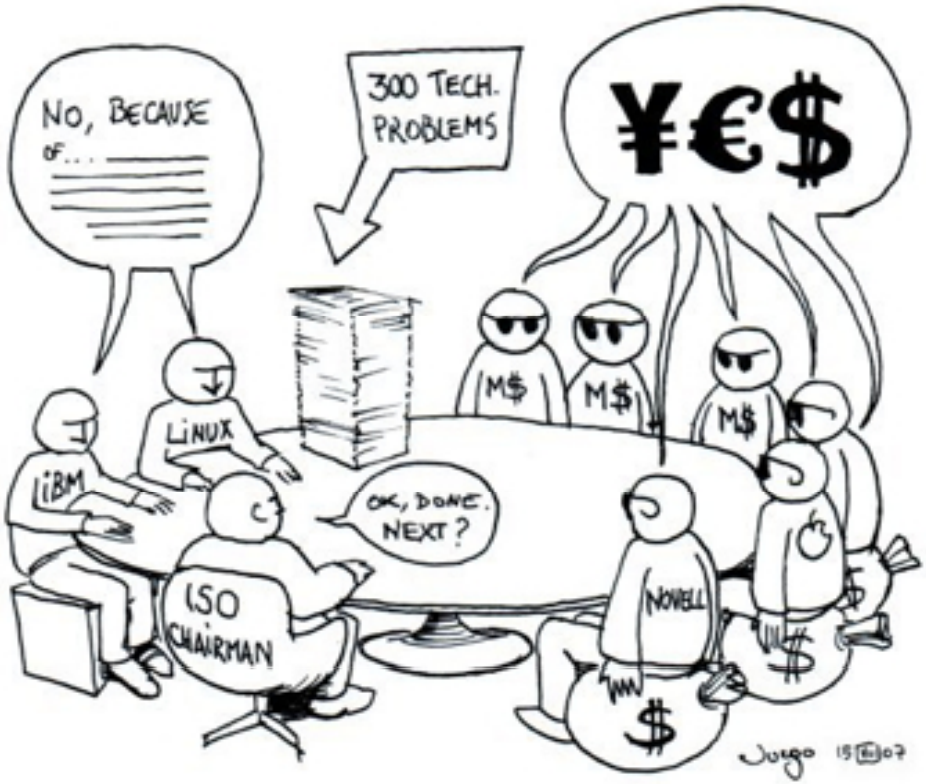
CiS, CISM

Vidnejša projekta

S&T Outsourcing
Geoplin Plinovodi

Namen predavanja…

- Prikazati pomen analize informacijskih tveganj
- Prikazati način izvedbe analize tveganj v praski


NO, BECAUSE OF...
300 TECH. PROBLEMS
¥€$
LINUX
IBM
ISO CHAIRMAN
OK, DONE. NEXT?
M$
M$
M$
NOVELL
$
Jugo 15/6/07

Primeri slabih praks…

HEKERJI

SVVI

NOTRANJI SOVRAŽNIKI

IZREDNI DOGODKI

Kako v praksi razporediti razpoložljiva finančna sredstva in kadre?

FINANČNA SREDSTVA

ČLOVEŠKI VIRI

ODGOVOREN ZA VAROVANJE INFORMACIJ (?)

USPEH

NEUSPEH


Kateri del računalniške opreme vam povzroča varnostne težave?
Tisti "strokovnjak" za tipkovnico!
AHS

Namen analize informacijskih tveganj

ANALIZA INFORMACIJSKIH TVEGANJ SLUŽI KOT SREDSTVO ZA:

- prepoznavo groženj, ranljivosti, verjetnosti in tveganj
- določitev prioritet pri vlaganju v informacijsko varnost
  - optimalno razporeditev razpoložljivih finančnih virov
  - optimalno razporeditev razpoložljivih kadrovskih virov

1. Analiza stanja na področju varovanja informacij

1) seznanitev z vizijo, poslanstvom in vrednotami organizacije
2) proučitev vseh internih aktov družbe
3) pregled stanja s pomočjo vprašalnika (plan!)

PRIMER VPRAŠALNIKA ZA IZVEDBO ANALIZE (PRESOJE)

ORGANIZACIJA INFORMACIJSKE VARNOSTI			
Zap. Št.	Vprašanje	DA/NE	Komentar
Notranja organizacije			
1	Ali imate v podjetju vodjo informacijske zaščite oziroma osebo, ki upravlja z varovanjem informacij?	DA	Funkcija je bila zaposlenemu dodeljena s sklepom uprave iz dne 04. 04. 2009.
2	Ali podjetje letno planira izobraževanje zaposlenih s področja informacijske varnosti?	NE	V zadnjem letu ni bilo izvedenih izobraževanj.
…	…	…	…

ISO/IEC 27002:2005

2. Popis informacijskih virov

1) popis vseh informacijskih virov v organizaciji
2) določitev njihove zaupnosti, celovitosti in razpoložljivosti
3) razvrstitev “enakih” informacijskih virov v skupine

PRIMER POPISA INFORMACIJSKIH VIROV

Klasifikacija	Informacijsko sredstvo	Oznaka	Serijska številka	Število kosov	Skupna vrednost virov ob nakupu (€)	Lokacija	Odgovorna/e oseba/e	Z	C	R
Prenonsik	Lenovo T61	6457-CTO	3425GDW	1	700	Outsourcing	Sistemski inženir	1	1	2
Informacije	Sistemska dokumentacija	Za stranke	/	/	/	/	/	4	3	3
	Reklamni letaki	Za konference	/	/	/	/	/	1	4	1
	...	...	...	...	...	...	...	...	...	...

3. Določitev izpostavljenosti tveganju

1) določitev naravnih, tehničnih in človeških groženj
2) ocena verjetnosti nastanka groženj (!)
3) ocena ranljivosti glede na specifičnost groženj

PRIMER OCENE IZPOSTAVLJENOSTI TVEGANJU

Grožnje	Verjetnost nastanka grožnje	Ranljivost	Izpostavlj. tveganju
Odpoved programske opreme	1	1	2
Izguba zaupnosti (npr. kraja).	2	3	5

ISO/IEC 27002:2005

4. Ocena informacijskih tveganj

1) ocena informacijskih tveganj
2) določitev sprejemljivega nivoja tveganj

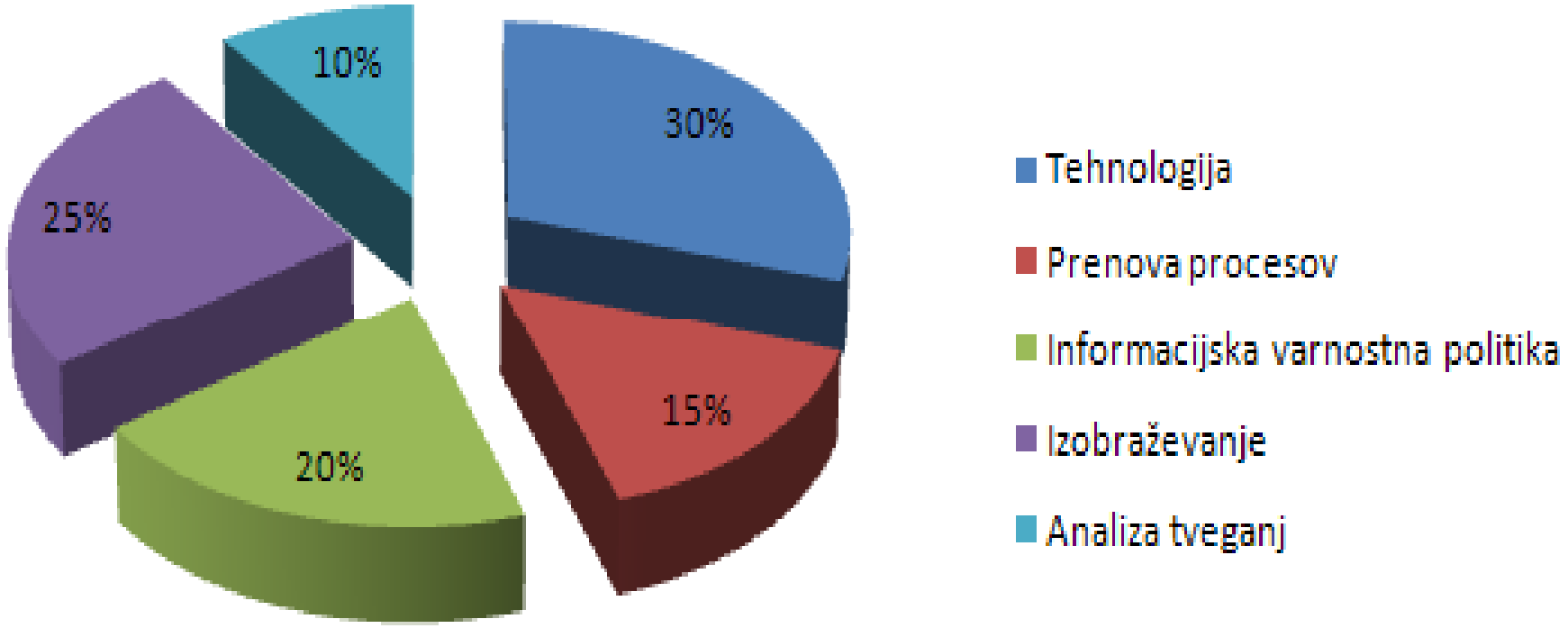
PRIMER OCENE INFORMACIJSKIH TVEGANJ ZA SIST. DOKUMENTACIJO

Grožnje	Izpostavlj. tveganju	Zaupnost	Celovitost	Razpoložlj.
		3	**2**	**1**
Odpoved programske opreme	**2**	5	4	3
Izguba zaupnosti (npr. kraja).	**5**	8	/	6

5. Obvladovanje tveganj

1) priprava plana za odpravo tveganj
2) odkrita tveganja lahko vodstvo:
   - ✓ sprejme (tudi posledice)
   - ✓ odpravi (npr. izbriše informacije)
   - ✓ omeji (npr. uvedba kontrol)
   - ✓ prenese (npr. zavarovalnica)

Idealna razporeditev razpoložljivih sredstev za varovanje informacij



Vir: Gartner - The "ideal" budget allocation

VPRAŠANJA?

HVALA ZA POZORNOST!

matej.saksida@snt.si