Risku vērtēšana

Sintija Deruma, CISM

ISACA Latvijas nodaļas biedre

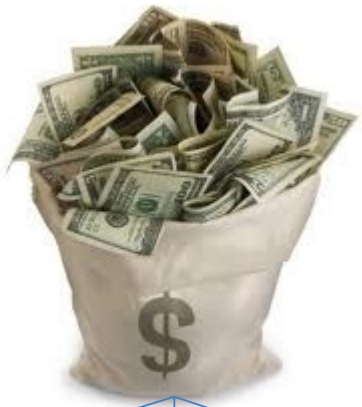
2012. gada 17. maijs

Ar ko sākt?

- Vertēšanas kritēriji:
  - Ietekme
  - Varbūtība
  - Riska atklāšanas ātrums

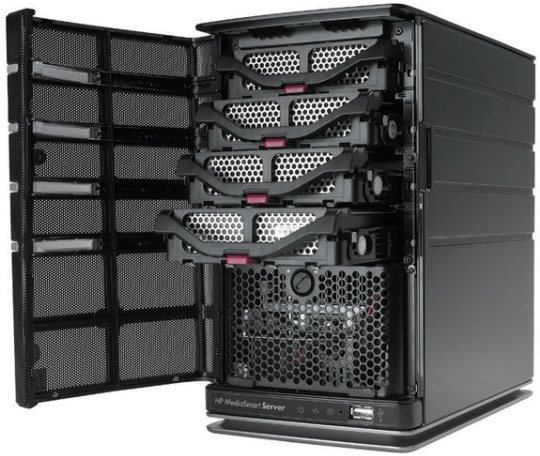
R= Ie x V x A

Kādi iespējami zaudējumi?



Informācijas resursi → Sankcijas, pārkāpumi

Tehniskie resursi



Tirgus, klienti, reputācija

Kādi iespējami zaudējumi?

Tehniskie resursi	Informācijas resursi	Sankcijas, pārkāpumi	Reputācija, klienti, tirgus	
Līdz 10 000	7 000	10 000		1
50 000 – 100 000		50 000	100 000	2
100 000 – 500 000	300 000			3
virs 500 000			virs 500 000	4

Apkopojiet visus iespējamos zaudējuma veidus un izmantojiet reālas, pierādāmas summas.

Cik bieži tas atgadās?

10 gadi	
5 gadi	
2 gadi	
1 x gadā	
1 x ceturksnī	
1 x nedēļā	
1 x dienā	

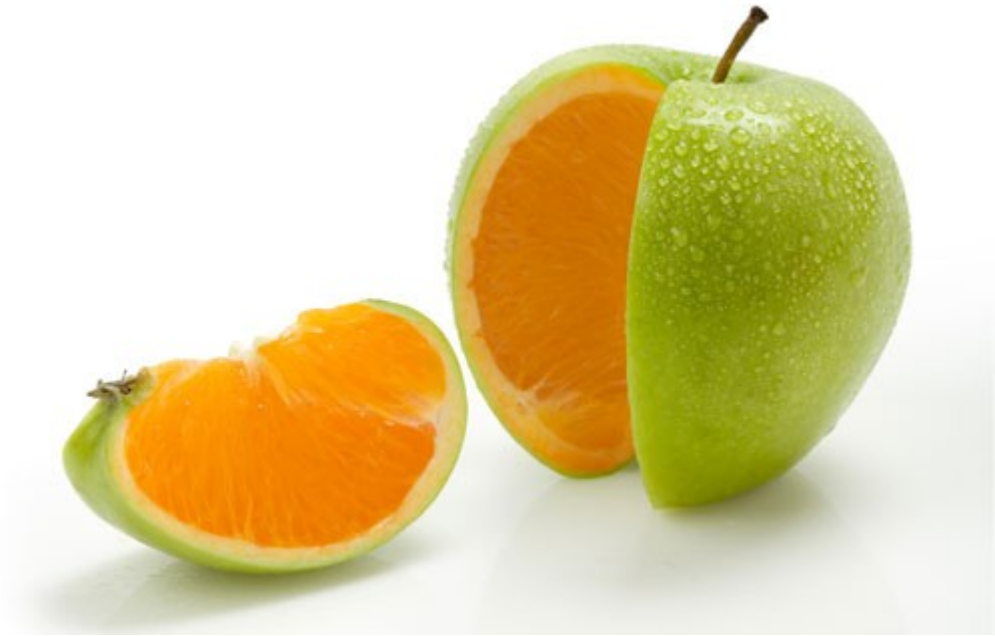
Varbūtību vēlams izteikt gada robežās, ņemot vērā cilvēkfaktoru un intuīciju…

Problēmas atklāšanas ātrums

laiks	**metode**	
stundas	Automātiski rīki, kontroles	1
dienas	Atskaites, pārbaudes	2
mēneši	Cilvēka vērtējums	3
	Pēc fakta	4

Definējiet jūsu organizācijai atbilstošus, piemērotus kritērijus, kas reāli varētu palīdzēt novērtēt esošo stāvokli, esošos aizsardzības pasākumus.

Stāsts



Rosiniet stāstīt vēsturiskus atgadījumus, notikumus, negadījumus,
jo tajos slēpjas riski, kuri iespējams aktuāli arī šobrīd.

Problēmas…

1. Ielaušanās rūpnīcas teritorijā – vāja perimetra aizsardzība.
2. Fiziski bojājumi iekārtām, ierīcēm – vai ir aizsardzības mehānismi?
3. Iekārtu vadības pārņemšana – pakalpojuma traucējumi, atteice (drošības caurumi).
4. Datu pārtveršana (labošana, iznīcināšana, izpaušana)…
5. Pēdu dzēšana (auditācijas pierakstu trūkums).
6. Apsardzes dienestu ierašanās ātrums (12 minūtes) – vai tas ir pietiekami?
7. Cilvēks?

Aplūkojiet problēmu no dažādiem rakursiem: tehnoloģija, vide, cilvēki, dabas stihijas, nepārvarama vara

Kā sašķirot problēmas?

Problēma/Risks	ietekme	varbūtība	atklāšana	aprēķinātais risks
Ļaundaris ielaužas serveru telpā un fiziski sabojā iekārtas, tā rezultātā rodas pakalpojuma atteice, dīkstāve, sistēmas nepieejamība vairāk kā uz 24h	2 50 000 – 100 000	5 (1 x ceturksnī)	1 Automātiski rīki, kontroles Var atklāt stundās	15
Ļaundaris ielaužas serveru telpā, pārņem iekārtu vadību, pārtver un nopludina biznesa informāciju	3 100 000 – 500 000	5 (1 x ceturksnī)	3 Cilvēka vērtējums	30

Ko darīt tālāk?

- mazināt
- novērst
- samierināties
- nodot citam – apdrošināt
- «koplietot»
- uzraudzīt