

Laat Beveiliging niet over aan Beveiligers!

Presentatie voor EAM 2014

22 mei 2014

Raymond Slot

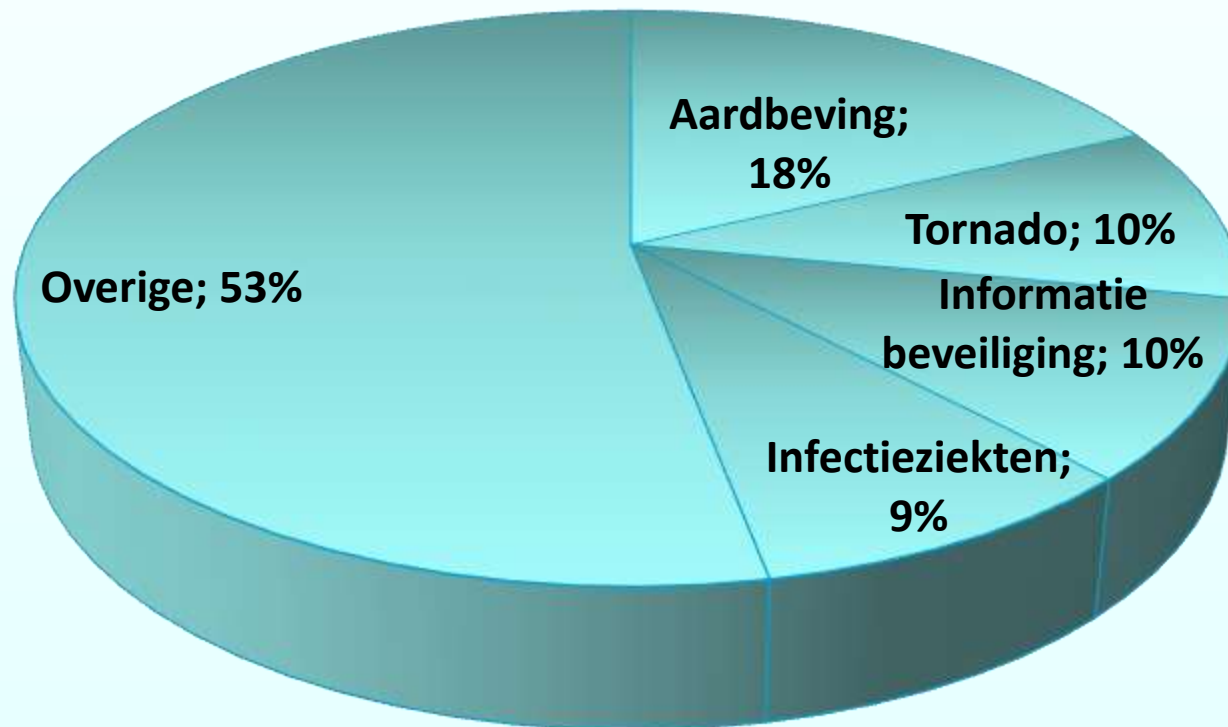


raymond.slot@hu.nl



nl.linkedin.com/in/raymondslot

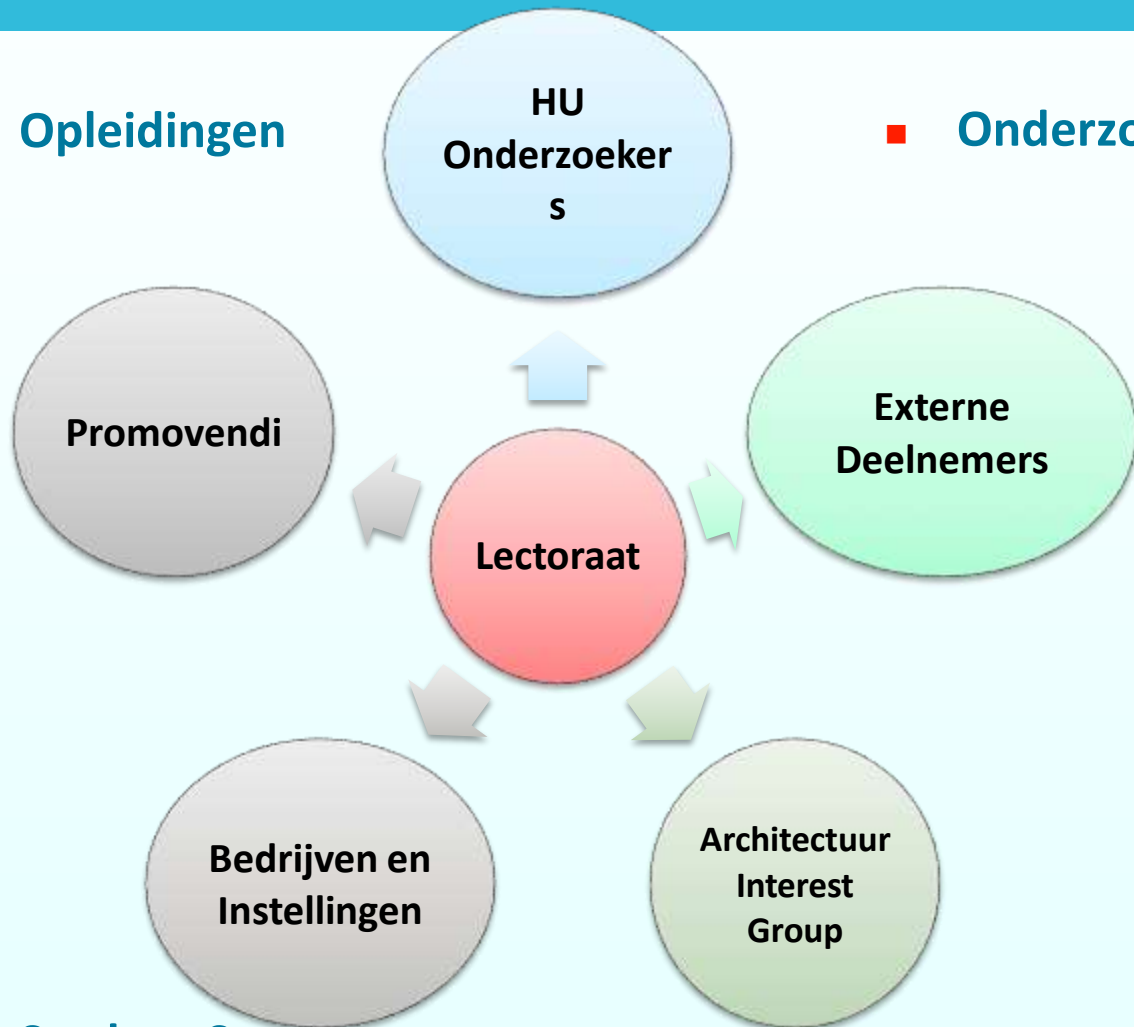
Continuïteitsbedreiging Bedrijven



US Cybersecurity capability.
National Preparedness Report, 2012

Focus op Toegepast Onderzoek

“Digitale architectuur is een coherente, consistente verzameling principes, verbijzonderd naar regels, richtlijnen en standaarden die beschrijft hoe een onderneming, de informatievoorziening, de applicaties en de infrastructuur zijn vormgegeven en zich voordoen in het gebruik.”*



■ Opleidingen

■ Onderzoek

■ Student Stages
en Opdrachten

■ Verspreiding
van kennis



Master of Informatics

Alignment and Architecture of Business and IT.

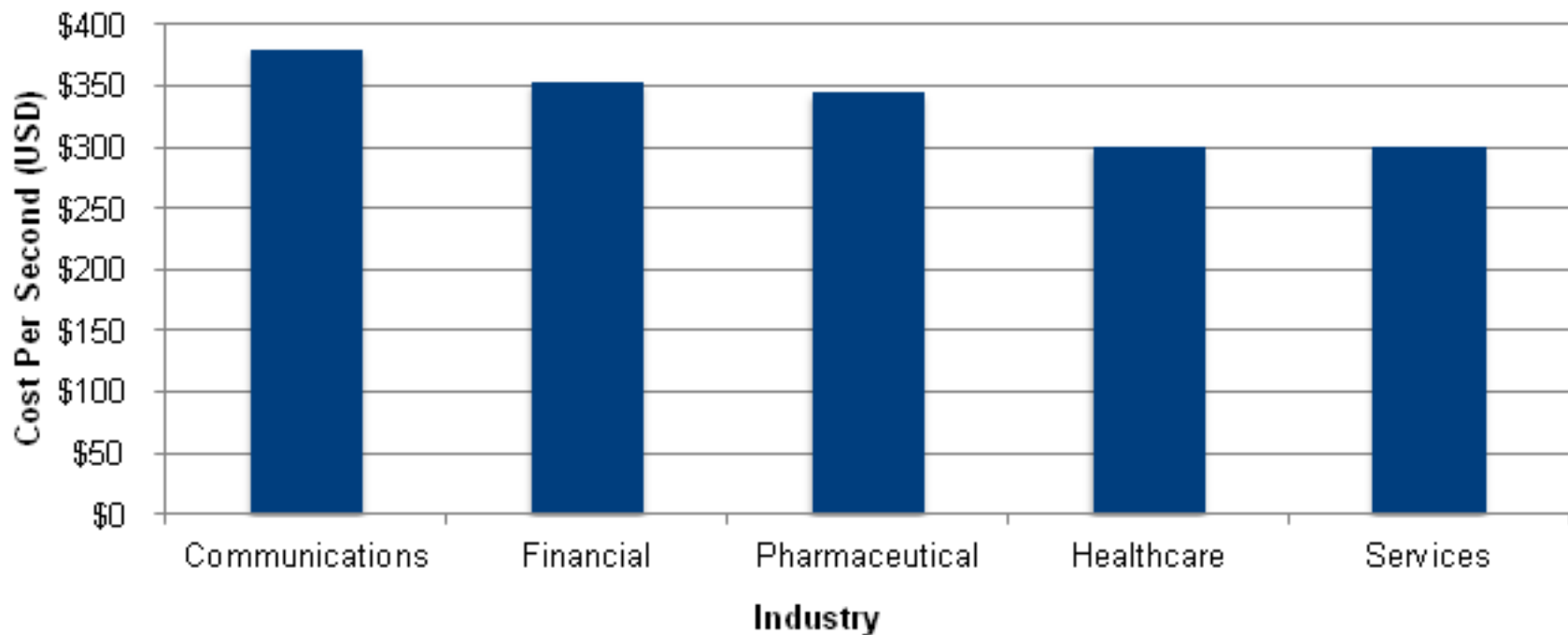
Specializations

- Business Information Management
- Business & IT Architecture



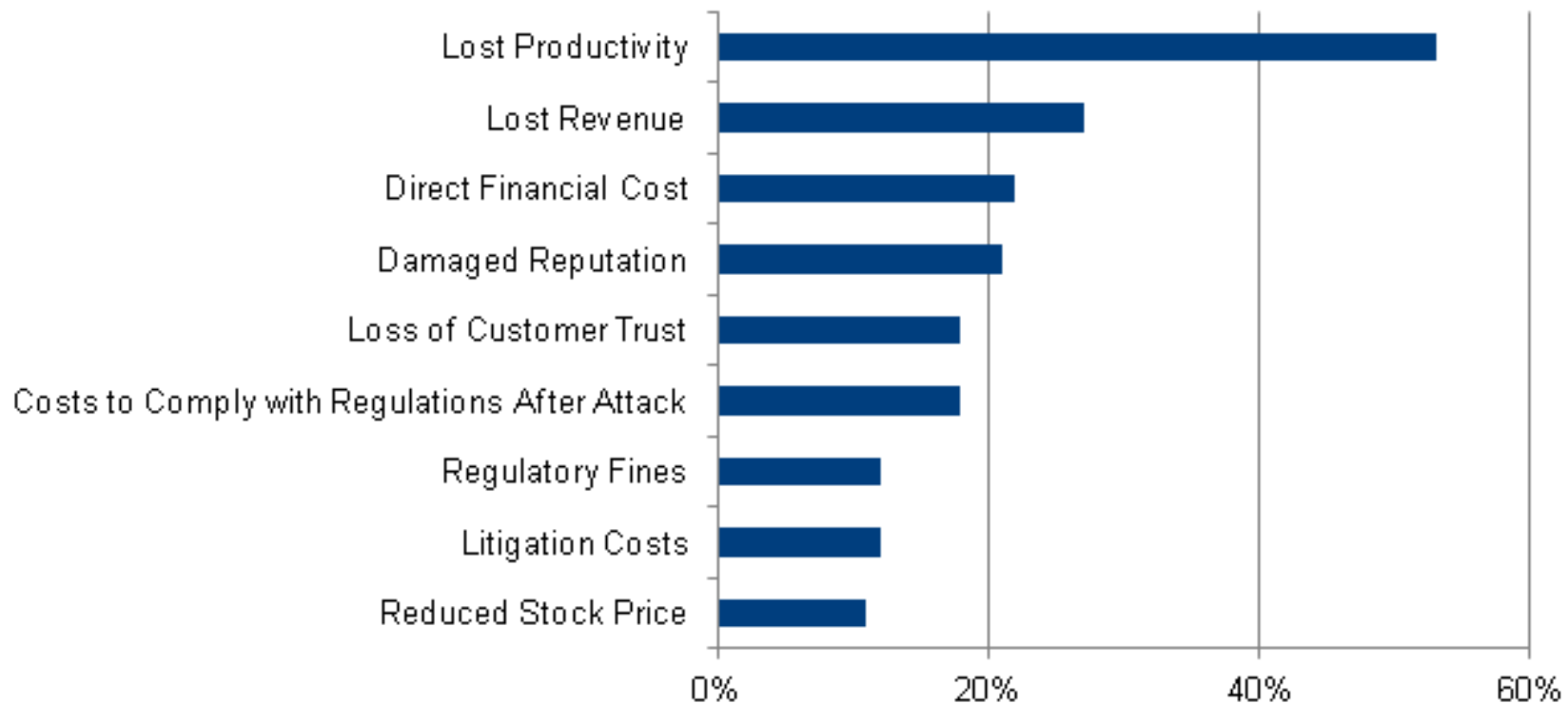
Beveiliging een Management issue?

Cost per Second of Cyber Attacks, by Industry

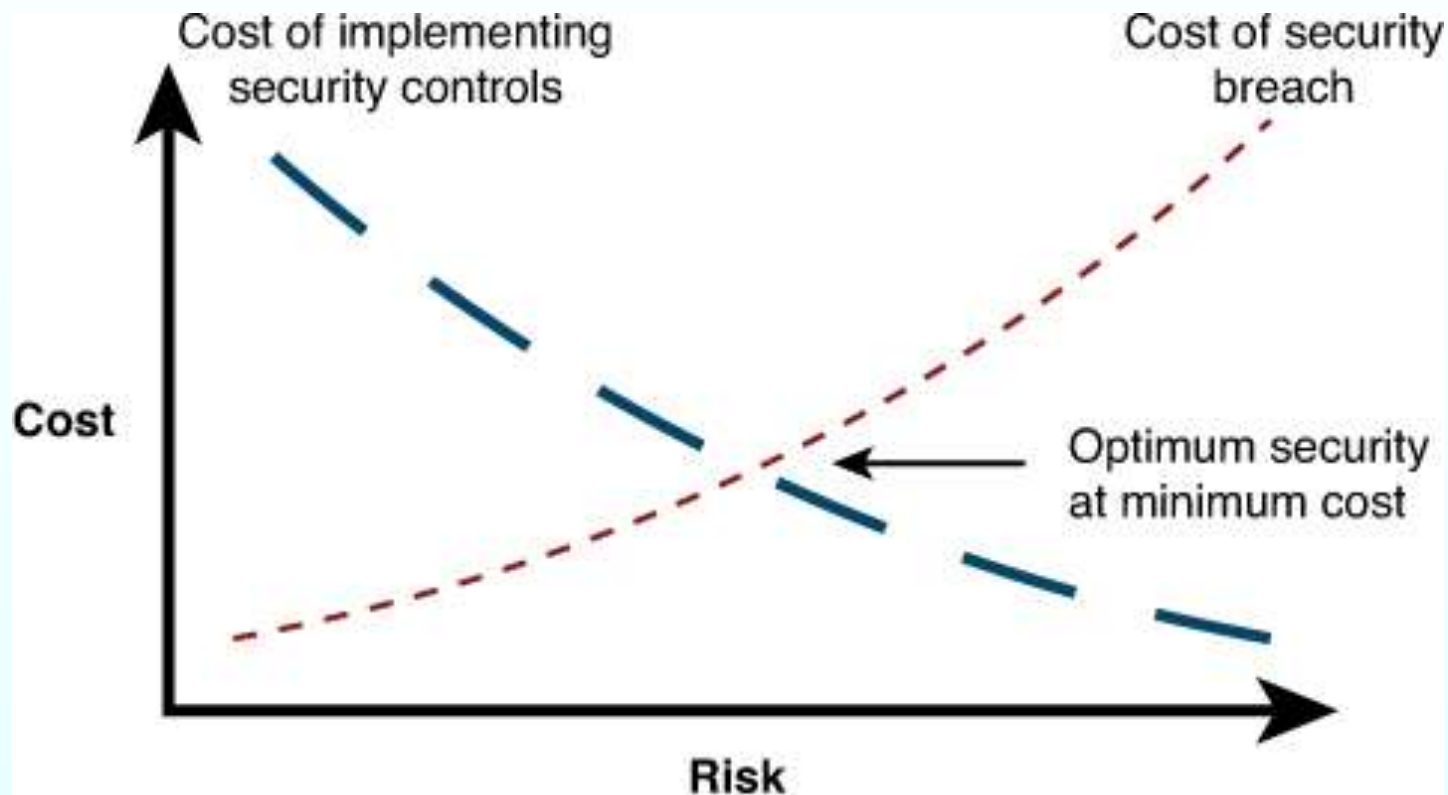


Enlight Research, 2012

Losses Incurred from Cyber Attacks



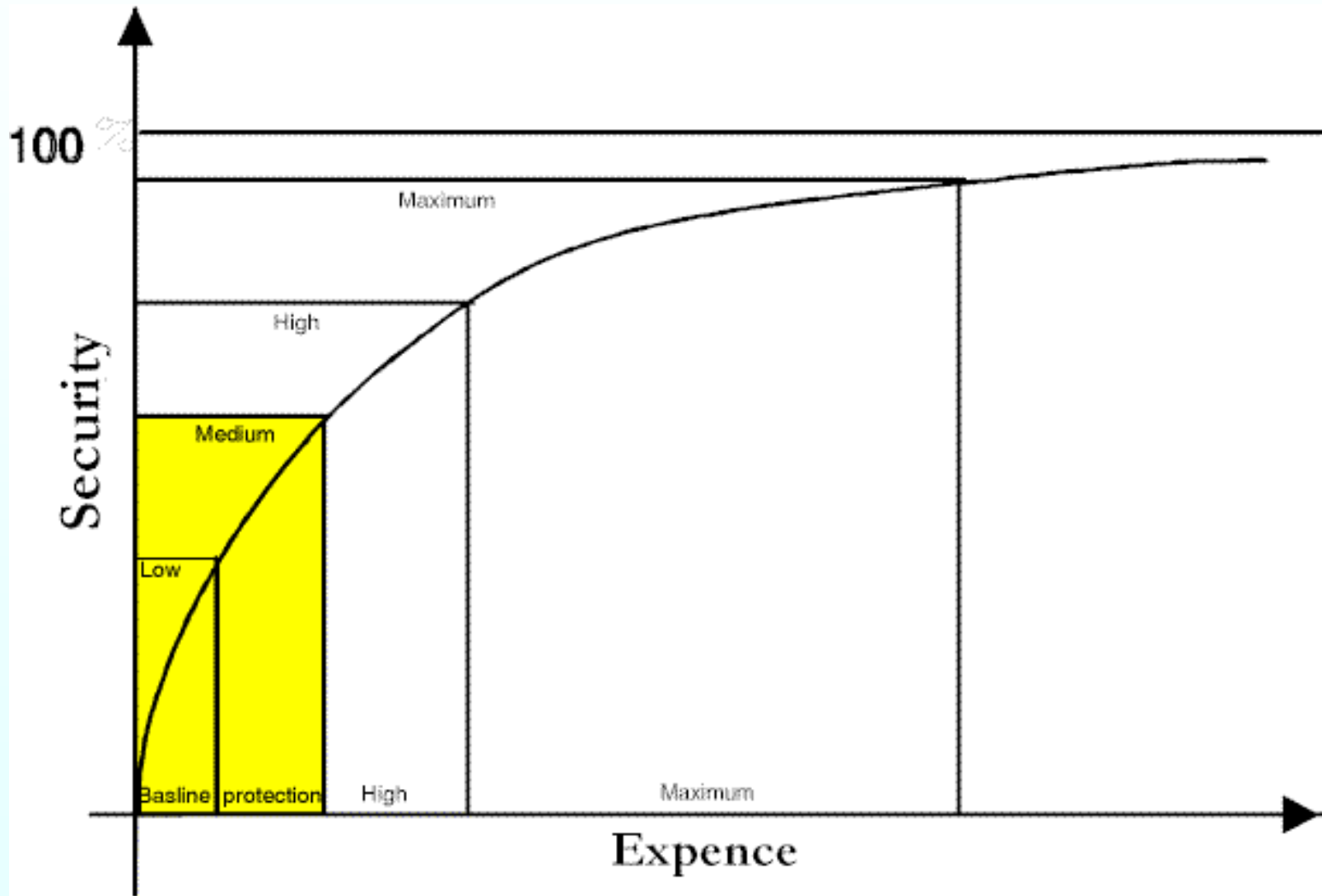
Enlight Research, 2012



Analysis of cost vs. risk
Cost of implementing security vs. cost of security breach

Uitgaven versus Niveau van Veiligheid

2014



ISO 27000



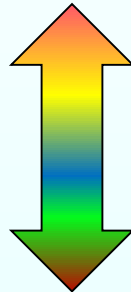
Strategisch



Beveiligingsbeleid

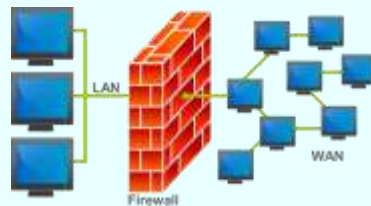
- Beveiligingsorganisatie
- Gewenst Niveau van Beveiliging
- Maatregelen (ISO 27000)

Tactisch



Kloof tussen Beleid en Uitvoering

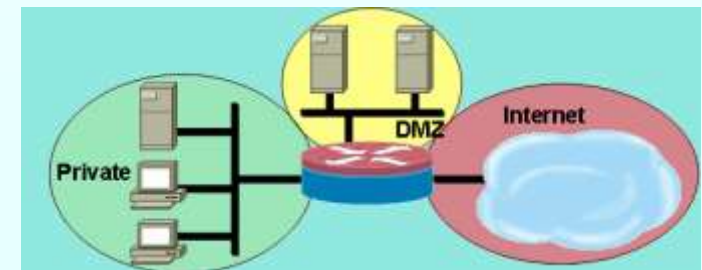
Operationeel



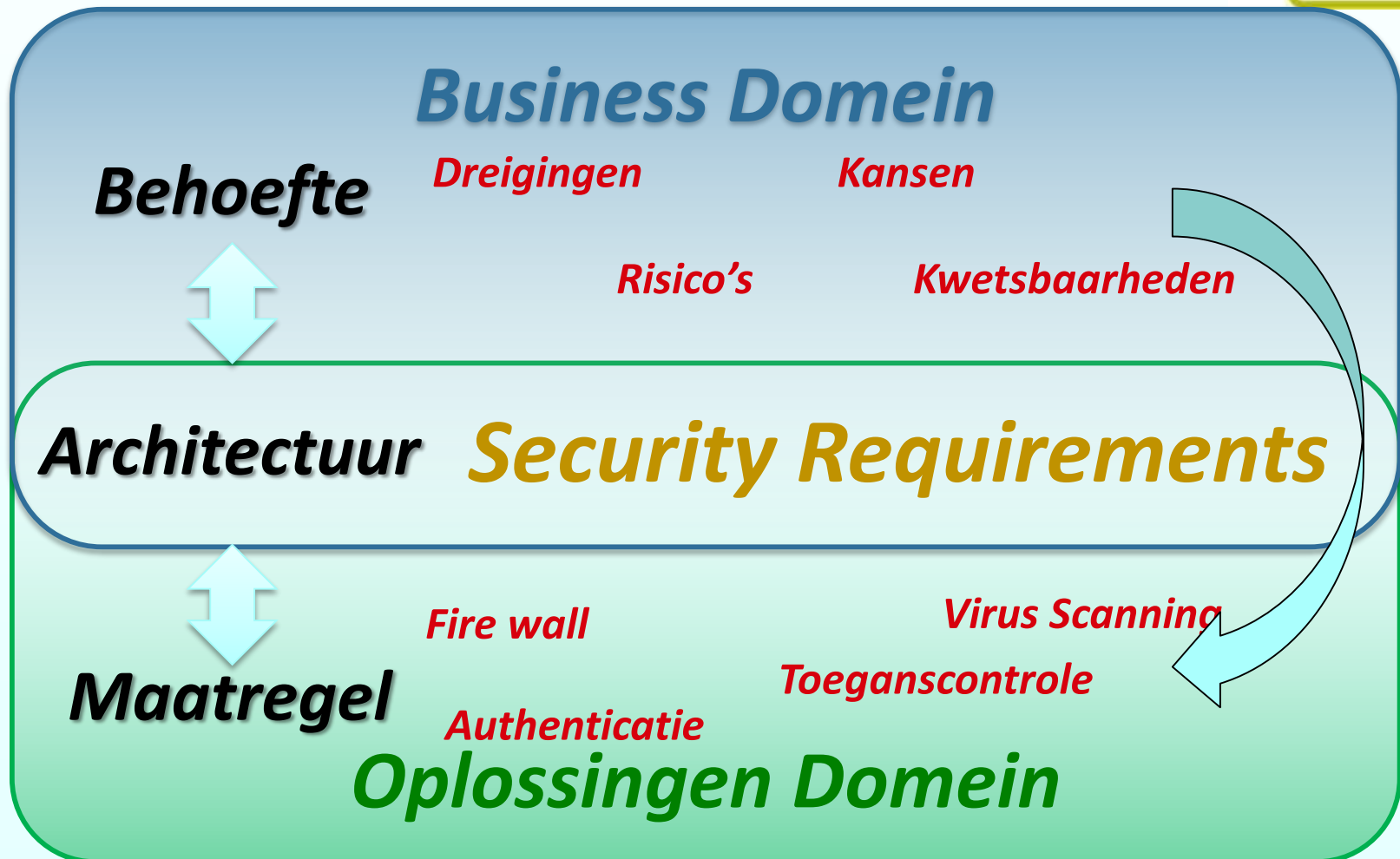
Fire Wall



Virus Checking



Netwerk Zones



Voorbeeld van Security Requirements (Vertrouwelijkheid)

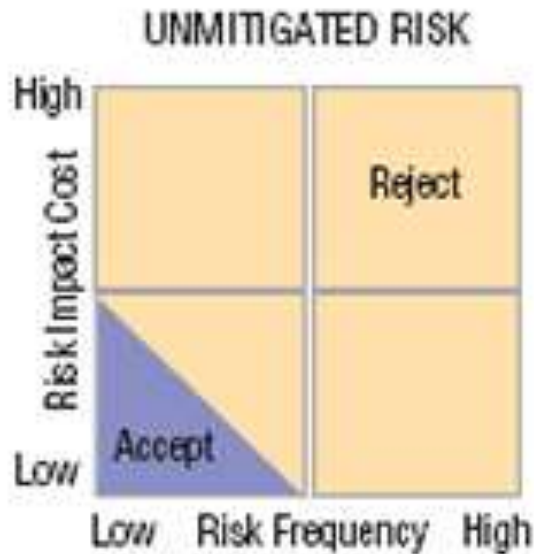
<i>Niveau</i>	<i>Omschrijving</i>
<u><i>Geheim</i></u>	Alleen daartoe specifiek geautoriseerde personen hebben toegang tot deze informatie. Het is zeer moeilijk voor niet-geautoriseerde personen om toegang te krijgen.
<u><i>Vertrouwelijk</i></u>	Alleen personen die in het kader van het bedrijfsproces de noodzaak hebben tot toegang tot deze informatie. Het is moeilijk voor personen buiten het bedrijfsproces om toegang te krijgen.
<u><i>Intern beschikbaar</i></u>	De informatie is intern beschikbaar voor medewerkers van de organisatie.
<u><i>Beschikbaar</i></u>	De informatie is vrijelijk beschikbaar binnen en buiten de organisatie.

Processen	Beschik:	1. Hoog			2. Midden					3. Laag				
	Vertr:	IO	V	G	O	IO	S	V	G	O	IO	S	V	G
ABS Proces												◆		
Alliance Proces												◆		
Applicatie 5 proces					◆									
GEO Proces												◆		
Arti Proces											◆			
Asset Proces							◆							
Bouw proces												◆		
Calculatieproces												◆		
Info proces				◆										

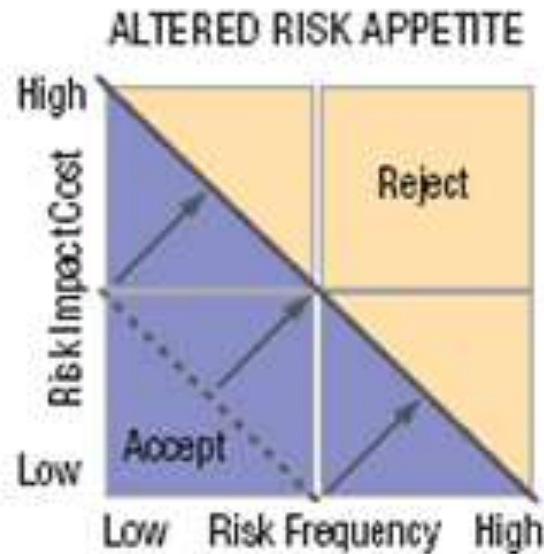
Requirements zijn gekoppeld aan Maatregelen (Voorbeeld)

Domein	Classificatie	Maatregel	Toelichting
Applicatie	Geheim	Toegang op basis van bezit en kennis	Een gebruiker kan alleen toegang krijgen tot een applicatie door middel van twee-factor authenticatie, bijvoorbeeld een token of biometrische autorisatie.
Externe toegang	Geheim	Beperking applicatie toegang	Gebruikers kunnen via externe toegang geen gebruik maken van applicaties met classificatie geheim.
Autorisatie-procedure	Geheim	Procedure Gebruikers-autorisatie	Gebruikers dienen expliciet geautoriseerd te worden door de security officer, volgens de wettelijke eisen (WBP, Hoofdstuk 2).
Data	Geheim	Distributie van gegevens	Distributie van data met classificatie "geheim" is alleen toegestaan met toestemming van de eigenaar van de gegevens.

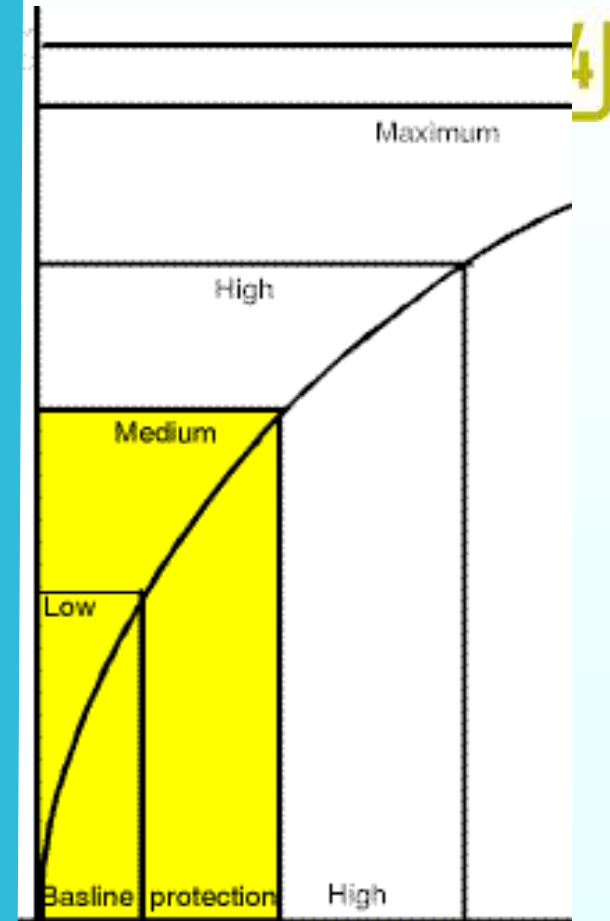
Doel: te komen tot acceptabele restrisico's



The diagonal line represents the company's risk appetite.



The diagonal line represents the company's risk appetite, shifted through experience, superior tools, etc.

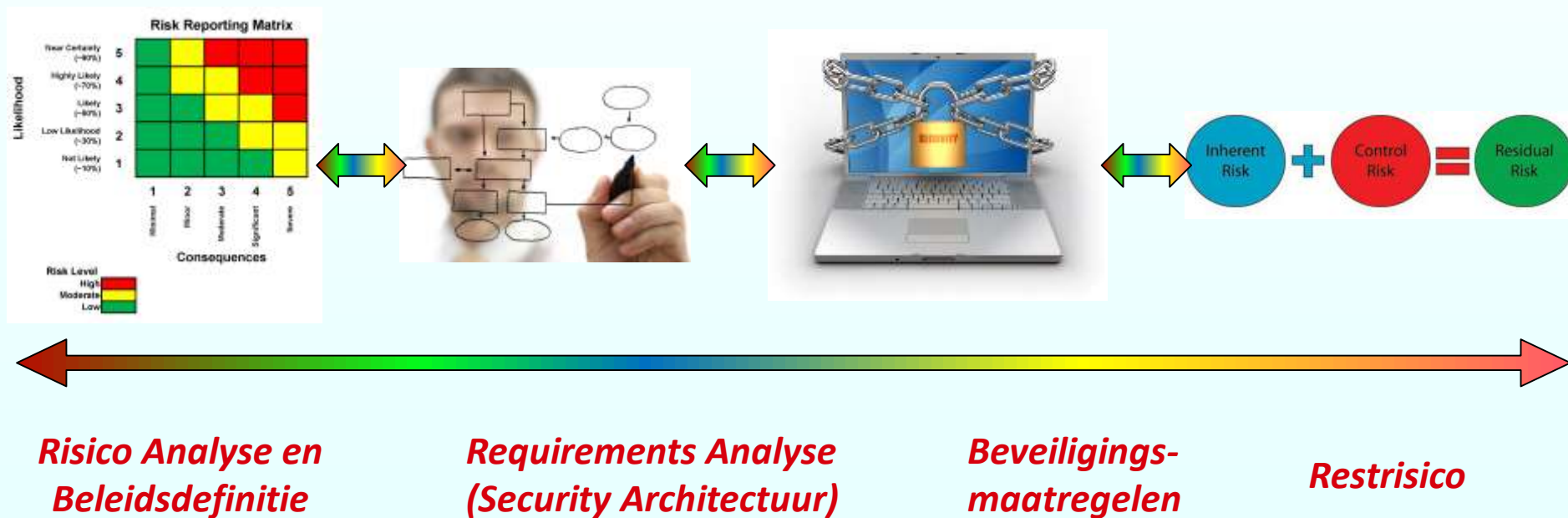


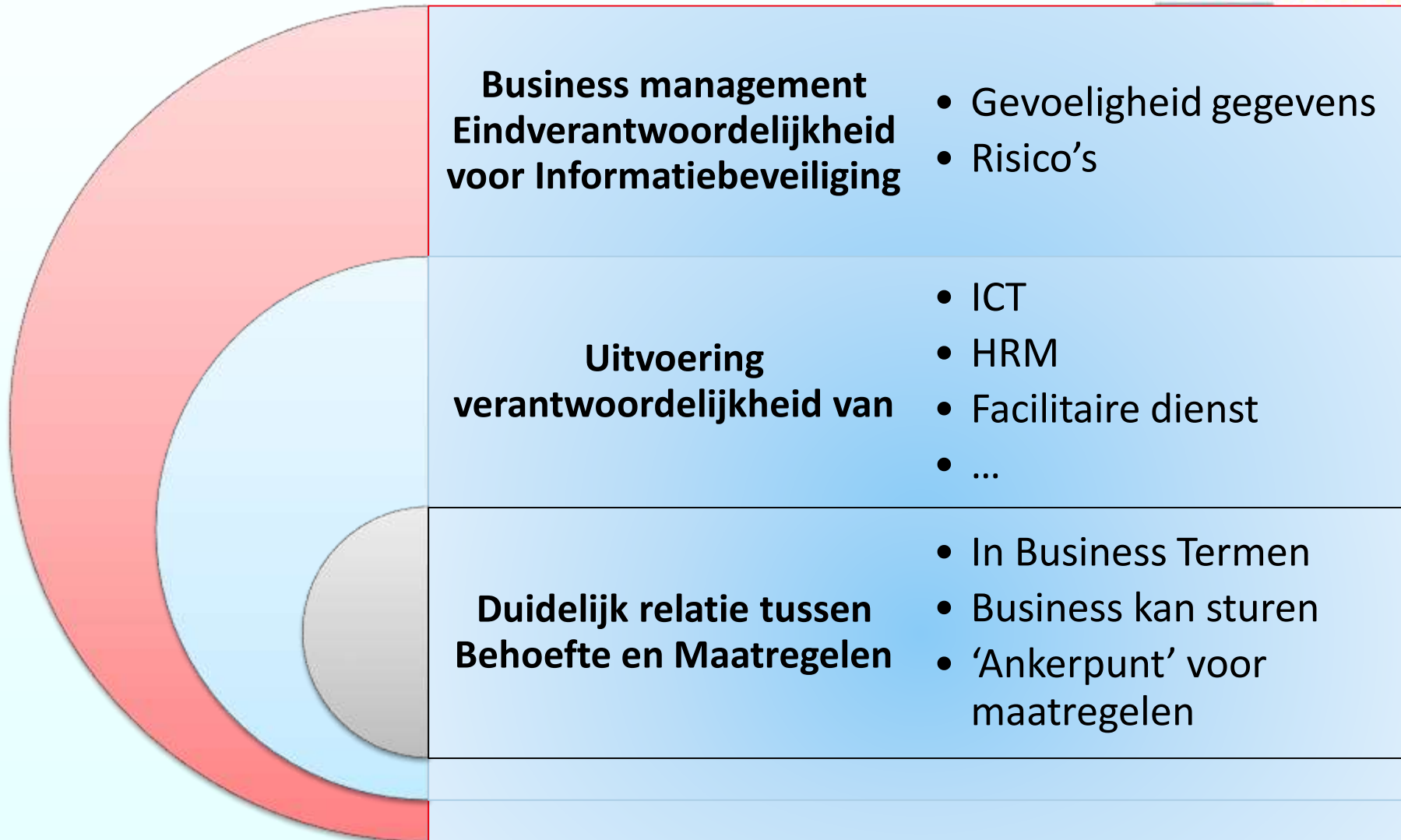
Inzicht in acceptabele Restrisico's

..... Tegen acceptabele kosten

Beveiligingsproces

Samenhang tussen Risico's en Maatregelen wordt geborgd door de Security Architectuur





Lessons Learned

1. Ga er niet van uit dat beveiliging 'wel geregeld' is
2. Neem als lijnverantwoordelijk zelf het heft in handen voor Informatiebeveiliging
3. Bedrijfscontinuïteit en justificatie van beveiligingskosten zijn de verantwoordelijkheid van Business management
4. Structurele analyse van behoeften versus beveiligingsniveau toont aan:
 1. Overbeveiliging ("7 x 24, maar we weten niet waar het minder kan")
 2. Onderbeveiliging ("Oei, worden in dat proces ook medische gegevens verwerkt!?!")
5. Business management dient inzicht te hebben in de Gewenste en de Actuele Restrisico's en de Gaps
6. Plan hoe om te gaan met de Gaps

EAM 2014



Laat Beveiliging niet over aan Beveiligers!

R & A