

Enterprise Security Trends

Robeco



Frank van der Spek
Rotterdam, 09 April 2009

Agenda

- Introduction: Who am I and the company I work for?
- Introduction: Enterprise Security trends
- In Focus: Vulnerability and compliance management
- Questions

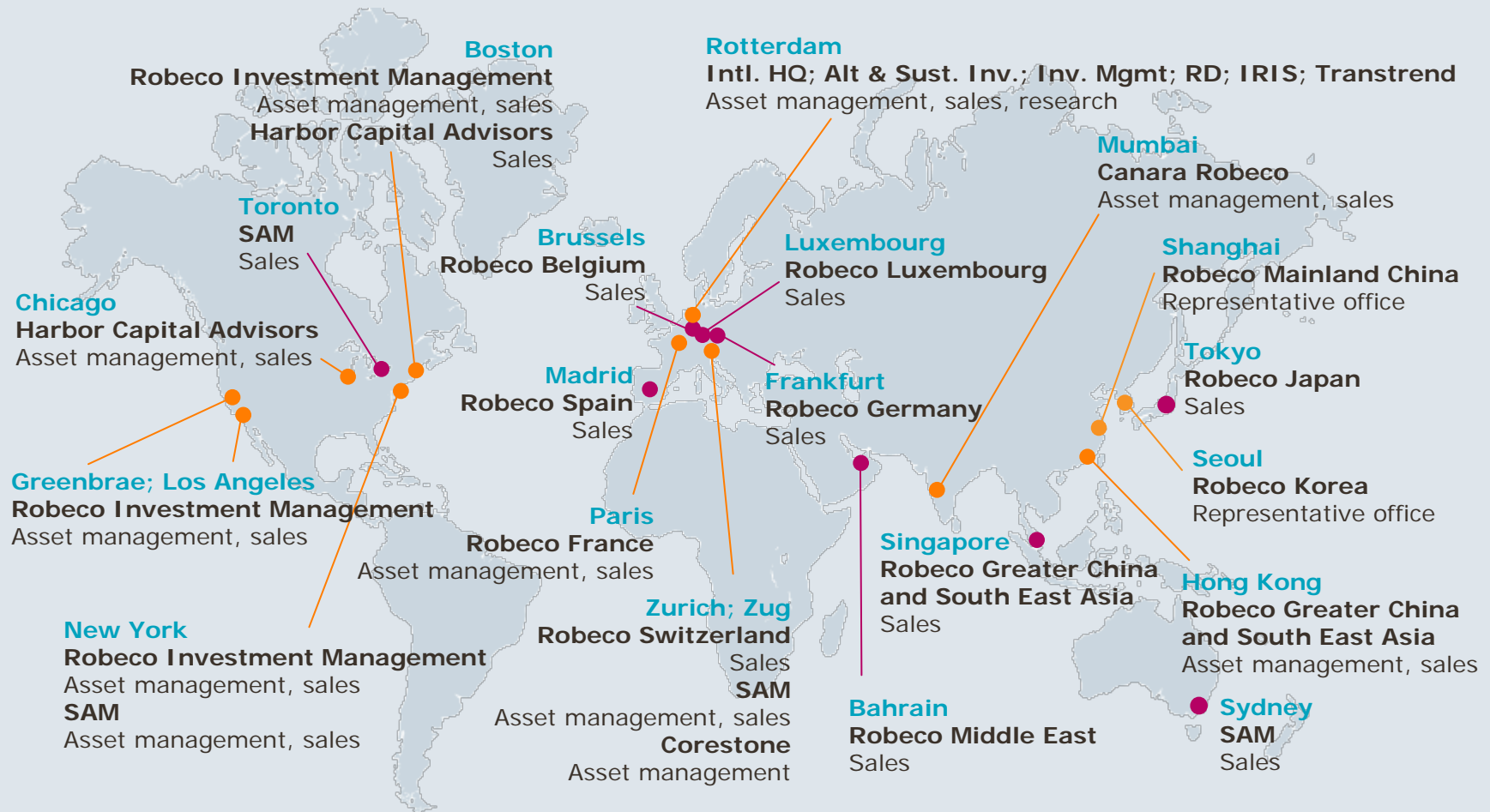
Who am I?

- Frank van der Spek: Information Security Officer
- Robeco
 - Pure-play asset manager since 1929
 - Active investment style
 - Equity, fixed income, money market, hedge funds, private equity, structured products, commodities, fiduciary management
 - Assets under management of around EUR 111 billion (31 December 2008)
 - Strong presence in Europe and the US
 - Global leader in sustainability investments
 - Part of Rabobank (rated Triple A)
 - Around 1650 employees (FTEs) in 14 countries (31 December 2007)

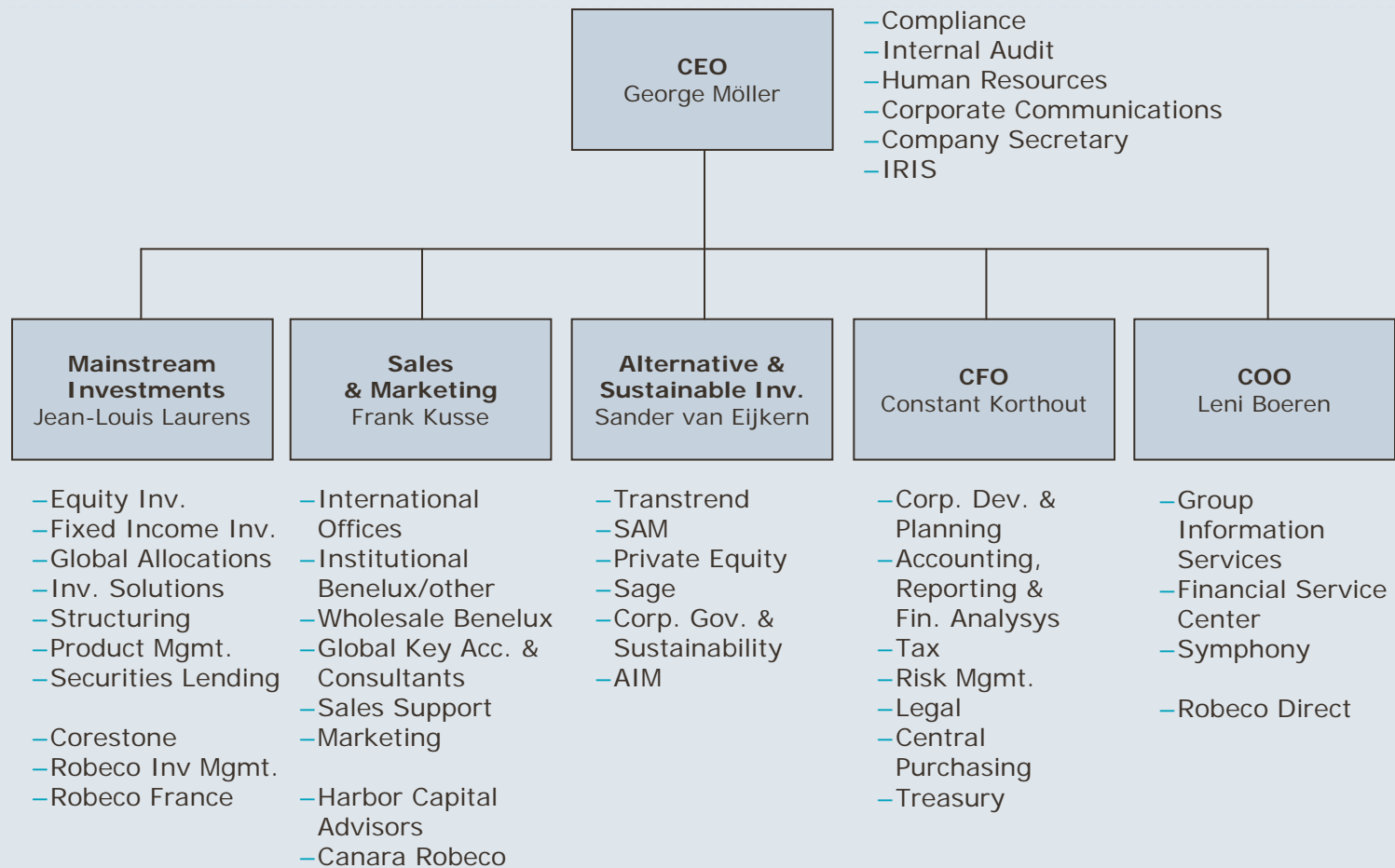


Global presence

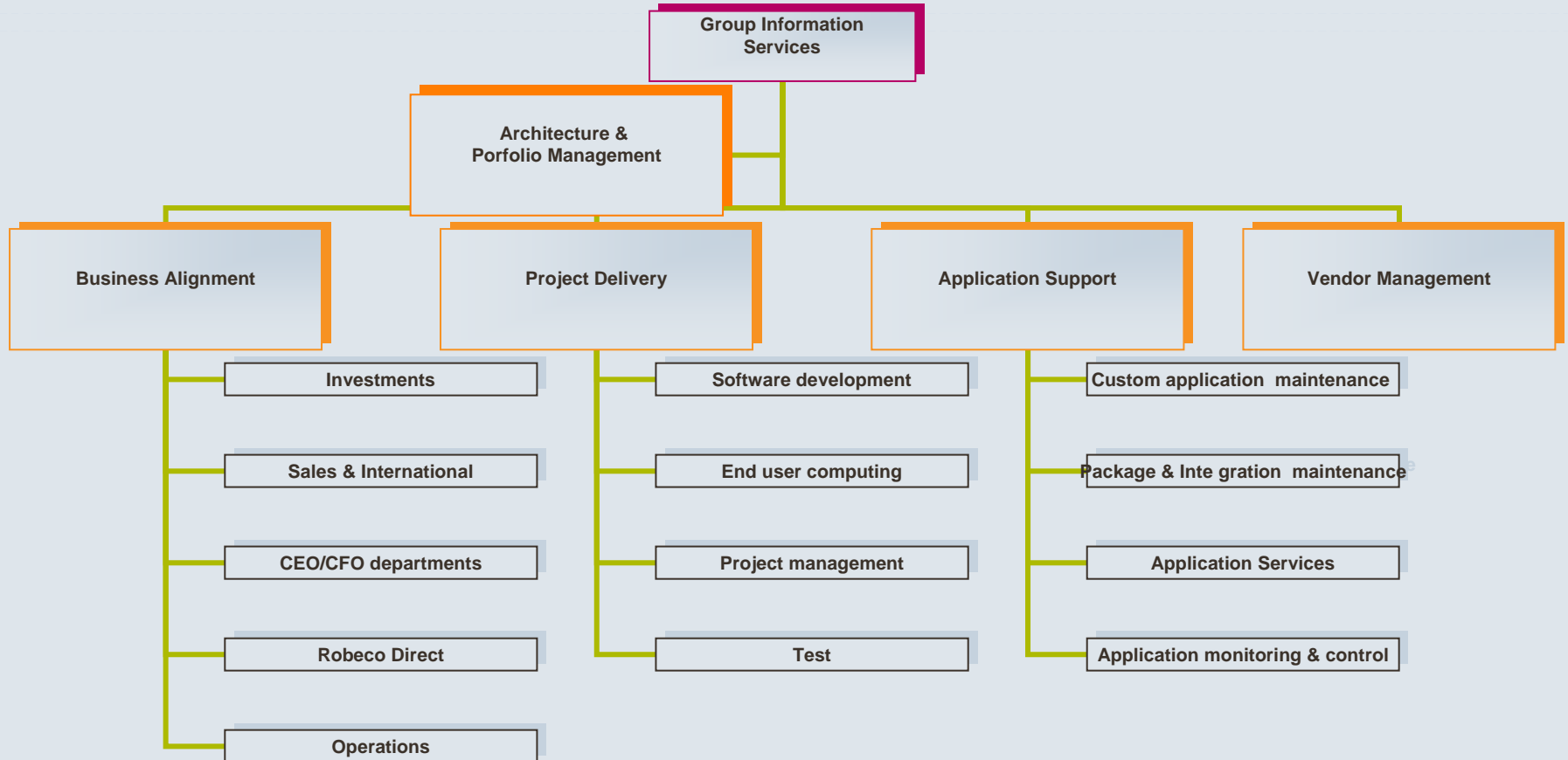
- = investment management and sales
- = sales only
- = representative office



Robeco Organization



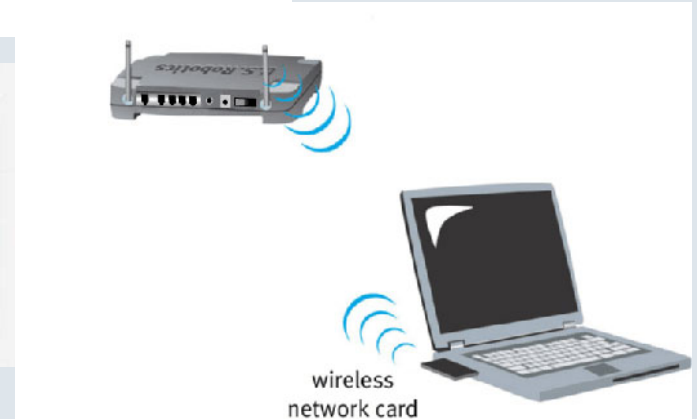
Group Information Services



Enterprise Security trends

- Mobile equipment security
- Protection of (transactional) data
- Social networks and privacy
- VOIP/IPT integration and security
- Web security: widgets
- Risk management / based approach
- Vulnerability and policy compliance

Mobile equipment security



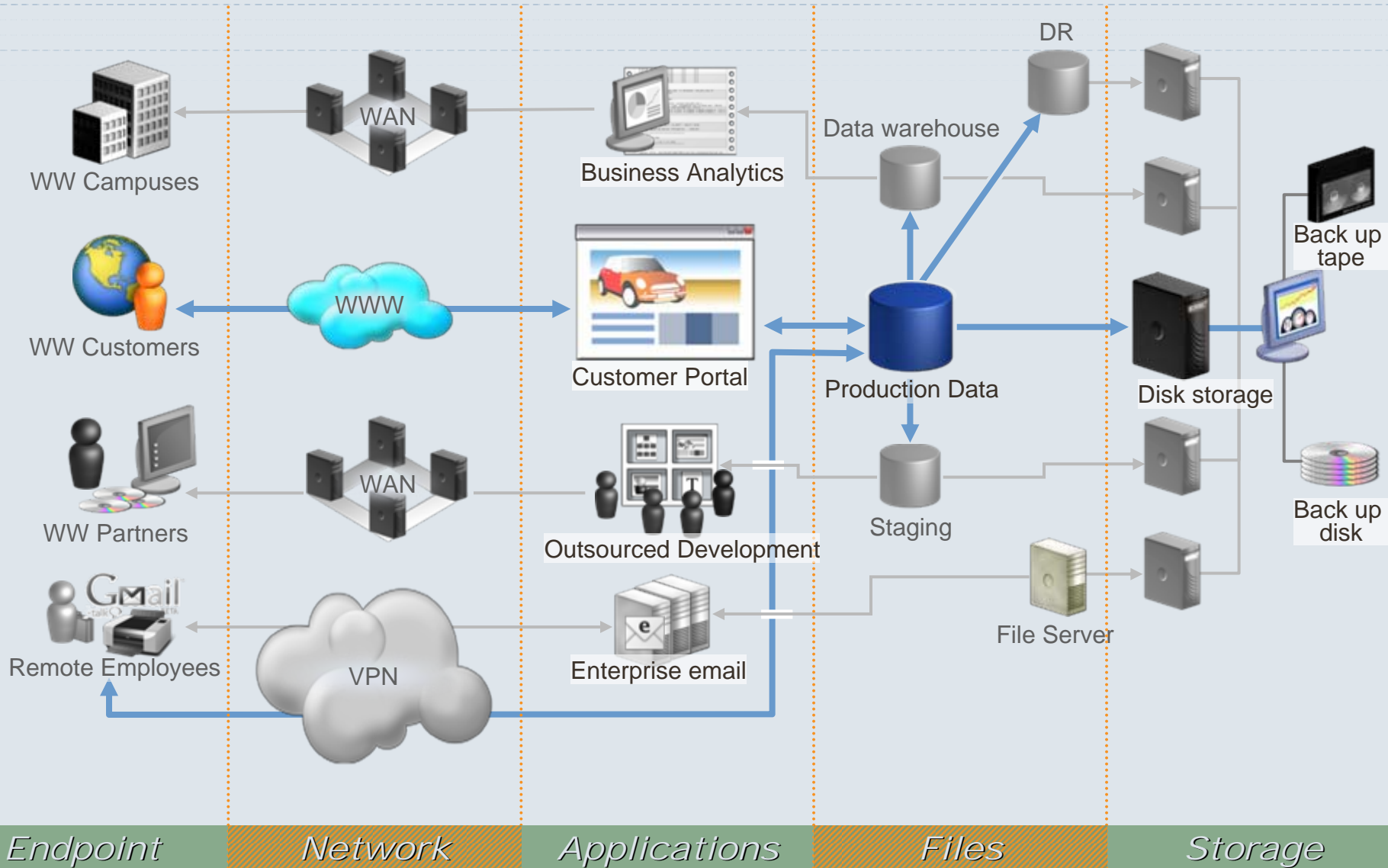
Don'ts:

- store your password(s) with your mobile device
- leave your mobile device in your car
- store your mobile in checked luggage
- carry mobile devices in easily identifiable carrying cases

Do's:

- secure your mobile device when unattended.
- keep track of your mobile device when you go through airport screening
- record identifying information and mark your equipment
- backup your files

Protection of (transactional) data



Endpoint

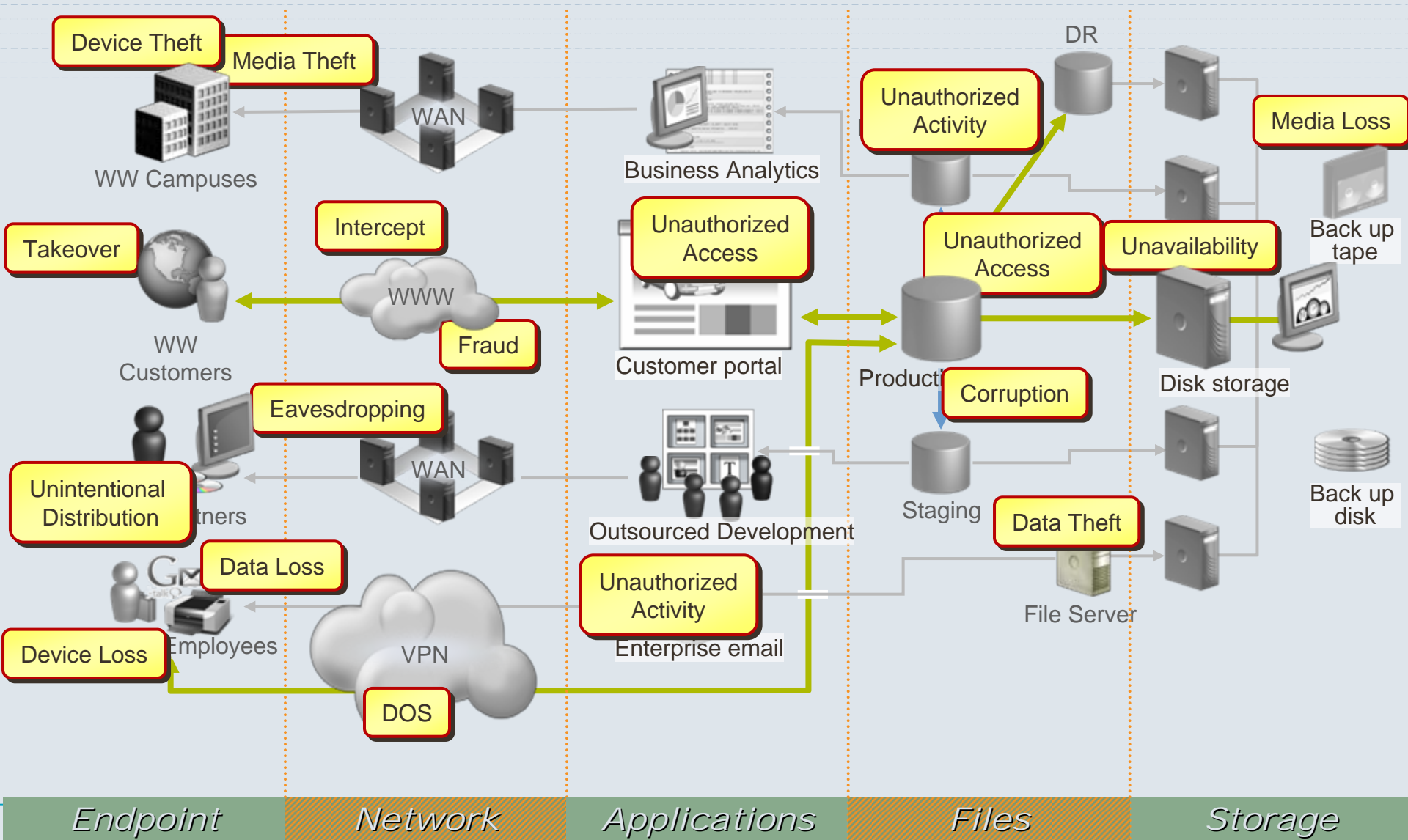
Network

Applications

Files

Storage

Protection of transactional data



Social Networks



- A lot of identity information
 - Identity theft
 - Social engineering

VOIP/IPT integration and security

- Internal Threats
 - Inquisitive staff
 - Staff who take advantage
 - Disgruntled staff
 - Cleaners
 - Security guards
- Attacks
 - Hacking
 - Eavesdropping
 - Packet spoofing & masq.
 - Replay attacks
 - Message integrity compromise
 - Malicious call redirection and hijacking
 - Malicious calling and voicemail bombing
 - Man-in-the-middle
 - Malware
 - Denial of Service (DOS)
 - Rogue devices
- External Threats
 - Hacking by organized crime
 - Hacking for profit
 - Hacking for revenge
 - Disgruntled ex-employees
 - Competitors
- Vulnerabilities
 - Mis-configuration/implementation
 - Application vulnerabilities
 - Operating System vulnerabilities
 - Separation data / voip network
 - Poor architectural design
 - No encryption
 - Leaving unused services enabled
 - Inadequate security on enabled services.

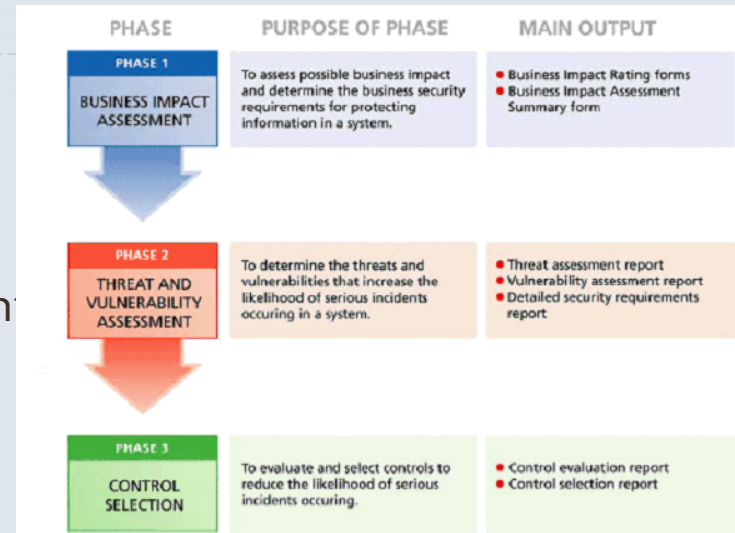
Web security: widgets

- Widgets are small applets that usually run in a web browser or on the desktop and provide a specific functions.
- Vulnerabilities in widgets and gadgets enable attackers to gain control of user machines, and should be developed with security in mind.
- As any program code, widgets can be used for malicious purposes. One example is the Facebook “Secret Crush” widget, reported in early 2008 by Fortinet as luring users to install Zango adware.



Risk management / based approach

- IRAM methodology of ISF
- 3 phases:
 - Business impact Assessment
 - Threat and Vulnerability Assessment
 - Control Selection



Business Impact Rating Availability						
Ref.	Business impact type	Business impact rating				
	Business impact of a prolonged outage of the system (most serious case)	Business impact of an unplanned or unauthorized disclosure of information (most serious case)				
		Duration of outage				
		All time	1 day	2-3 days	1 week	1 month
Financial						
F1	Loss of sales, orders or contracts	B	B	B	A	A
F2	Loss of tangible assets	E	D	C	C	C
F3	Penalties/legal liabilities	E	D	C	C	C
F4	Unforeseen costs	E	D	C	C	B
F5	Depressed share price	E	D	D	C	C
Operational						
O1	Loss of management control	E	D	C	B	B
O2	Loss of competitiveness	E	D	C	C	C
O3	New ventures held up	E	D	B	B	A
O4	Breach of operating standards	E	E	E	E	E
Customer-related						
C1	Delayed deliveries to customers or clients	E	D	C	C	C
C2	Loss of customers or clients	E	D	C	C	B
C3	Loss of confidence by key institutions	E	D	C	C	C
O4	Damage to reputation	E	D	C	C	C
Employee-related						
E1	Reduction in staff morale/productivity	E	D	C	C	C
E2	Injury or death	E	E	E	E	E
Overall Rating						
		All time	1 day	2-3 days	1 week	1 month
	In summary, what is the most serious impact which would arise from an outage of the system? (This would normally be at least as high as the highest individual rating)	C	B	B	A	A
	In summary, taking into account the ratings noted above and any other consequence, what is the most serious impact which would arise from unplanned or unauthorized disclosure of information? (This would normally be at least as high as the highest individual rating)		X			

Business Impact Rating Confidentiality						
Ref.	Business impact type	Business impact rating				
	Business impact of unplanned or unauthorized disclosure of information (most serious case)	Explanatory comments				
		A	B	C	D	E
Financial						
F1	Loss of sales, orders or contracts		X			
F2	Loss of tangible assets				X	
F3	Penalties/legal liabilities				X	
F4	Unforeseen costs			X		
F5	Depressed share price			X		
Operational						
O1	Loss of management control			X		
O2	Loss of competitiveness		X			
O3	New ventures held up			X		
O4	Breach of operating standards					X
Customer-related						
C1	Delayed deliveries to customers or clients			X		
C2	Loss of customers or clients		X			
C3	Loss of confidence by key institutions				X	
O4	Damage to reputation		X			
Employee-related						
E1	Reduction in staff morale/productivity				X	
E2	Injury or death					X
Overall Rating						
		A	B	C	D	E
	In summary, taking into account the ratings noted above and any other consequence, what is the most serious impact which would arise from unplanned or unauthorized disclosure of information? (This would normally be at least as high as the highest individual rating)		X			

Table 1: ISF business impact types

Ref.	Business impact type	Examples	Appropriate measure
Financial			
F1	Loss of sales, orders or contracts	Sales opportunities missed, orders not taken or contracts that cannot be signed.	Financial impact (%)
F2	Loss of tangible assets	Fraud, theft of money and lost interest.	Financial impact (\$)
F3	Penalties/legal liabilities	Breach of legal, regulatory or contractual obligations.	Financial impact (\$)
F4	Unforeseen costs	Recovery costs, uninsured losses, increased insurance.	Financial impact (\$)
F5	Depressed share price	Sudden loss of share value, prolonged loss of share value, random share value fluctuation.	Loss of share value (%)
Operational			
O1	Loss of management control		
O2	Loss of competitiveness		
O3	New ventures held up		
O4	Breach of operating standards		
C1	Delayed deliveries to customers or clients		
C2	Loss of customers or clients		
C3	Loss of confidence by key institutions		
O4	Damage to reputation		
Employee-related			
E1	Reduction in staff morale/productivity		
E2	Injury or death		
F5	Verlaagde prijs aandelen	Verlies van de waarde van aandelen (%)	Meer dan 25%
			11% tot 20%
			6% tot 10%
			1% tot 5%
			Minder dan 1%
Operationeel			
O1	Verlies van management toezicht	Toename van verliezen	Groot verlies van
			Eerstig van controle
			Belangrijk verlies van
			Gemiddeld verlies van
			Minimaal verlies van

Referentie Tabel

Niveau van impact	Niveau van impact				
	A (Hoog)	B (Medium)	C (Laag)	D (Heel laag)	E (Heel laag)
dan 6	11% tot 20%	6% tot 10%	1% tot 5%	Minder dan 1%	
dan 100	€50.000 tot €100.000	€10.000 tot €50.000	€100 tot €10.000	Minder dan €100	
dan 100	€50.000 tot €100.000	€10.000 tot €50.000	€100 tot €10.000	Minder dan €100	
dan 100	€50.000 tot €100.000	€10.000 tot €50.000	€100 tot €10.000	Minder dan €100	

Vulnerability management

- Some definitions:
 - A Vulnerability: A weakness in the IT infrastructure or IT components that may be exploited for a threat to destroy, damage, or compromise an IT asset.
 - Vulnerability Assessment: A methodical evaluation of an organization's IT weaknesses of infrastructure components and assets and how those weaknesses can be mitigated through proper security controls and recommendations to remediate exposure to risks, threats, and vulnerabilities.
 - Vulnerability Management: The overall responsibility and management of vulnerabilities within an organization and how that management of vulnerabilities will be achieved through dissemination of duties throughout the IT organization.

Vulnerability management at Robeco

- The vulnerability management process of Robeco is a responsibility of operational security within the outsourced infrastructure (EDS). This process consists of monitoring vulnerabilities in the market with information from ie. Symantec DeepSight Alert Service, different CERTs etc. Vulnerabilities are classified (on ease, local/remote, impact, complexity, reliability) and mapped on the infrastructure of Robeco. If applicable, vulnerability management triggers patches and updates to infrastructure and software components.
- Vulnerability assessment, by scanning the infrastructure on patch-level and vulnerabilities in services is also part of vulnerability management.

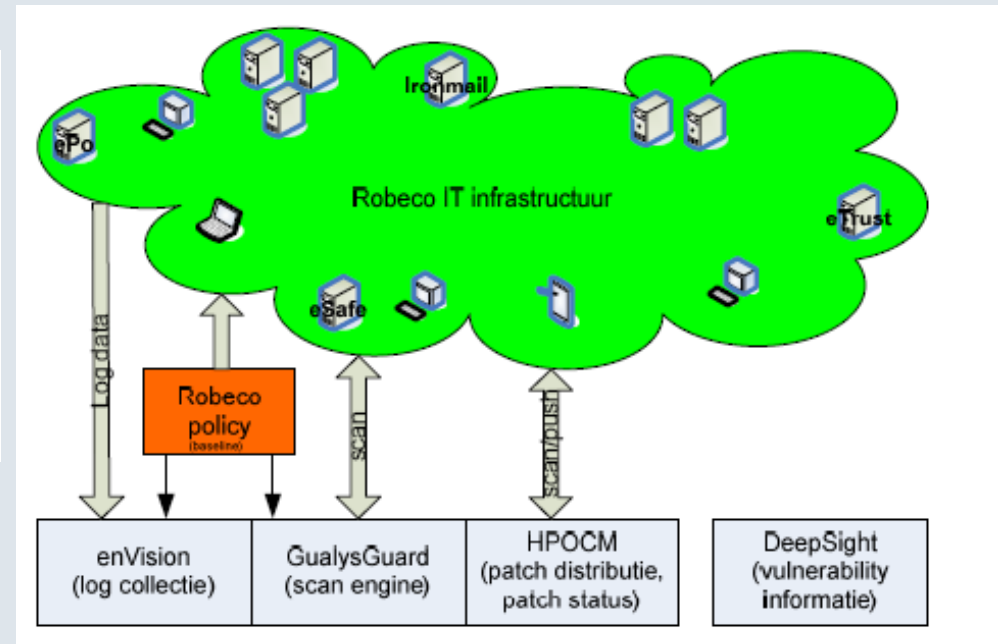
Vulnerability management at Robeco

- Main goals of vulnerability management:
- Check infrastructure against implementation guidelines.
- Assess on known vulnerabilities.
- Fix vulnerabilities with patches/updates/deactivating services.

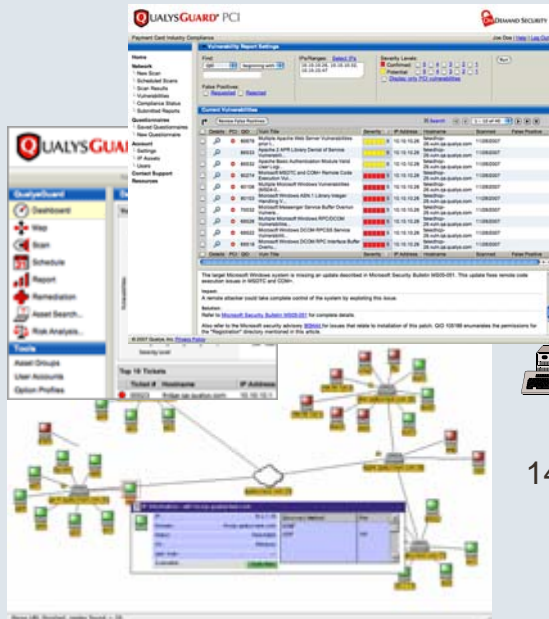
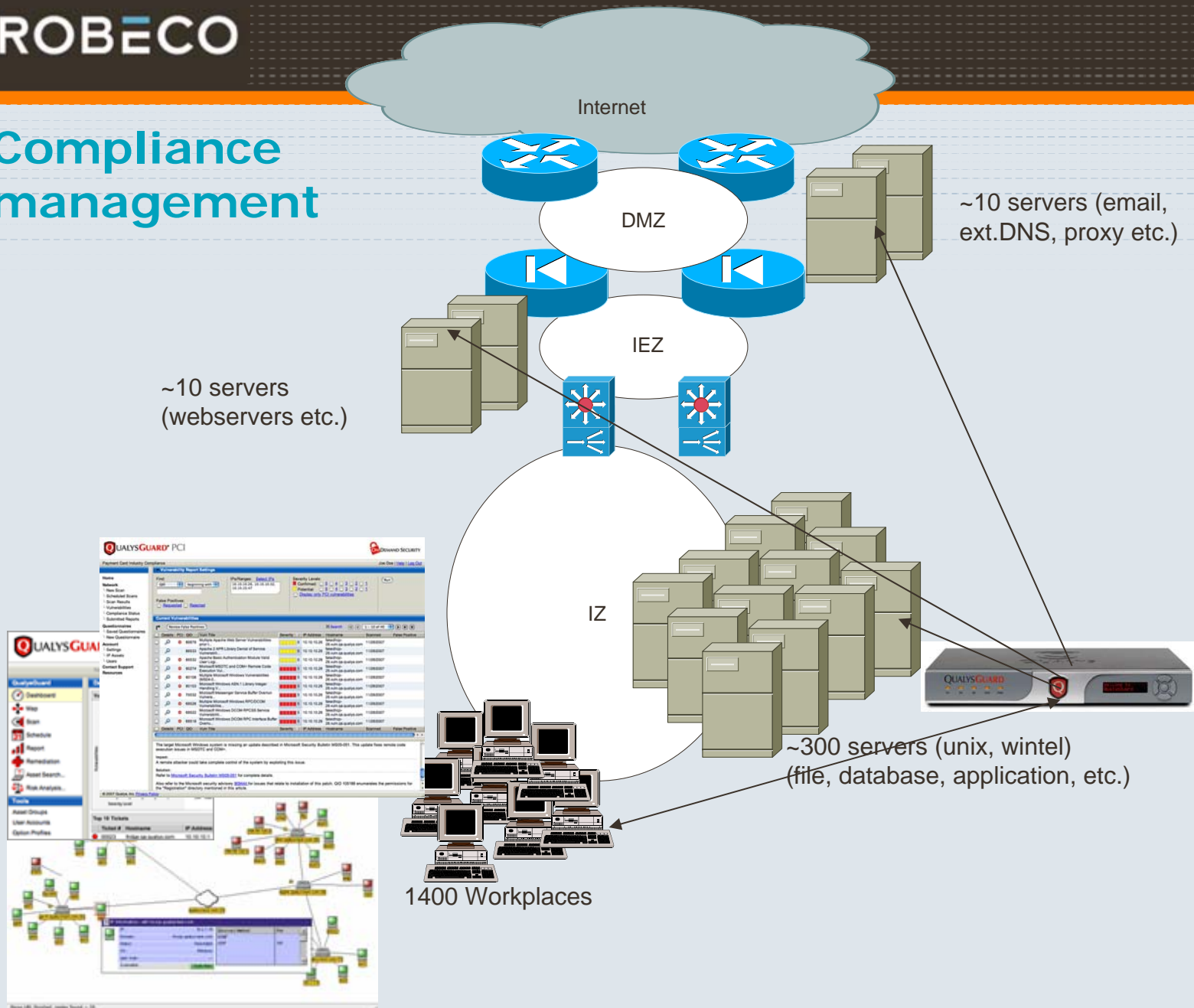
G.ICT 7.08.03

System vulnerability management			Netwerk security assessment	Verificatie virus scanners	Patch management
Unix AIX & SUN	MicroSoft	Werkplekken			
Unix scan policy	MicroSoft Servers scan policy	MicroSoft Werkplekken scan policy	Netwerk scan policy	Viruspolicy	Patch scan policy
Analyse & rapportage, <small>Initiate change, incident of problem</small>					
Reparatie via Change Incident Problem					

Baselines →



Compliance management



QualysGuard

- Qualysguard supports the Vulnerability and Patch management process in an optimal way. The key features of QualysGuard are:
- **Discover and prioritize all network assets**
Identify all network devices and software applications that reside within your infrastructure, and identify host details including operating system and open services.
- **Proactively identify and fix security vulnerabilities**
Safely and accurately detect and eliminate the vulnerabilities that make network attacks possible.
- **Manage and reduce business risk**
Reduce risk by automating vulnerability identification and prioritizing remediation based on mission critical systems and high-severity vulnerabilities.
- **Ensure compliance with laws, regulations and corporate security policies**
Document regulatory compliance via automated agent-less auditing, tamper resistant audit trails and the certainty that comes with third-party assessment.
- **Achieve compliance with Payment Card Industry (PCI) Data Security Standard**
Achieve PCI compliance status with QualysGuard's testing and compliance application.

Questions / Discussion

