

Introduction, Definitions, and Context

Risk and Security Management – HS 2012

PD Dr. Hannes P. Lubich



What is This Lecture All About?



Security Technology



Security Risks, Threats, etc.



Security Processes, Laws, Regulation etc.



Security Culture, Awareness, People



Lecture Outline and Logistics



Lecture Outline

1. Introduction, Definitions and Context
2. Threats, Attackers and Intentions
3. IT Security Requirements, Standards, Baselines & Best Practices
4. *Lecture Project: Introduction, Rules and Expectations*
5. Overall Structure of an IT Security Architecture
6. Architecture Components: Identity & Access Management
7. Architecture Components: Threat Management
8. Architecture Components: Security Information & Event Management, Correlation and Forensics
9. Cost / Benefit Considerations for IT Security
10. Sourcing of Security Components and Services
11. Organisation of IT Security and Related Topics
12. Risk Mgmt: Standards, Best Practices and Governance
13. *Presentation / Defense of Lecture Project Results*
14. Security Culture and Awareness, Q & A, Lecture Project Results, Exam Preparation

The lecture project will be organised and conducted in cooperation with Detecon Consulting

Lecture Logistics

Lecturer: Hannes Lubich

Tutor(s): Abdullah Alhussainy, Ariane Keller

Lecture Dates: every Tuesday 3:15 – 5:00 pm from Sep. 18 to Dec. 18, lecture hall ETH Zentrum, NO C6 (18.9. only) and ETZ F78.1 (all subsequent events) (**and yes, we will start on time!**)

Exercise Dates: every Friday 3:15 – 5:00 pm (max) from Sep. 21 to Dec. 14, lecture hall ETH Zentrum, ETZ E8 (except 12.10, 14.12 and 21.12.)

Lecture Material: Slide handouts, exercises (Note: some screenshots refer to outdated products, in order not to indicate any market preferences).

Homework:

- Preparation / self-study
- Lecture Project (see additional information sheets)

Exams: individual (1:1) oral exam, 30 min each, during official exam time in spring 2013 ONLY!

Lecture Project

- Mandatory, pre-requisite for exam registration
- Includes both paperwork and presentation / defense
- Will be evaluated in binary mode „passed / not passed“
- If not passed, one additional opportunity to submit improved version
- Group work, 3 to 4 students for each project
- Exam question(s) may refer to „your“ project
- Registration in week 4 of the lecture cycle

→ See additional project information sheets

Lecture “Culture”

Language(s)

Slides: English

Lecture: German or English, depending on participants

Questions: German and/or English

Exercises: German and/or English, depending on participants

Exams: German and/or English, depending on participants

Questions

There are no stupid questions

Be curious

Be courageous

Opinions

There will often be more than correct/smart/“good enough“ solution

Access to Lecturer & Tutor(s)

Lectures & exercises

E-Mail



Working Together

This is a story about four people named Everybody, Somebody, Anybody, and Nobody.

There was an important job to be done and Everybody was sure that Somebody would do it.

Anybody could have done it, but Nobody did it.

Somebody got angry about this, because it was Everybody's job.

Everybody thought Anybody could do it, but Nobody realized that Everybody wouldn't do it.

It ended up that Everybody blamed Somebody when Nobody did what Anybody could have done.

Lecture 1: Introduction, Definitions, and Context



Outline

- How is „IT Security“ Defined?
- Threats and Protection: the CIAO Principle
- IT Security Scope
- IT Security Elements: Technology, Organisation, Processes, Management, Awareness
- IT Security Embedding and Context

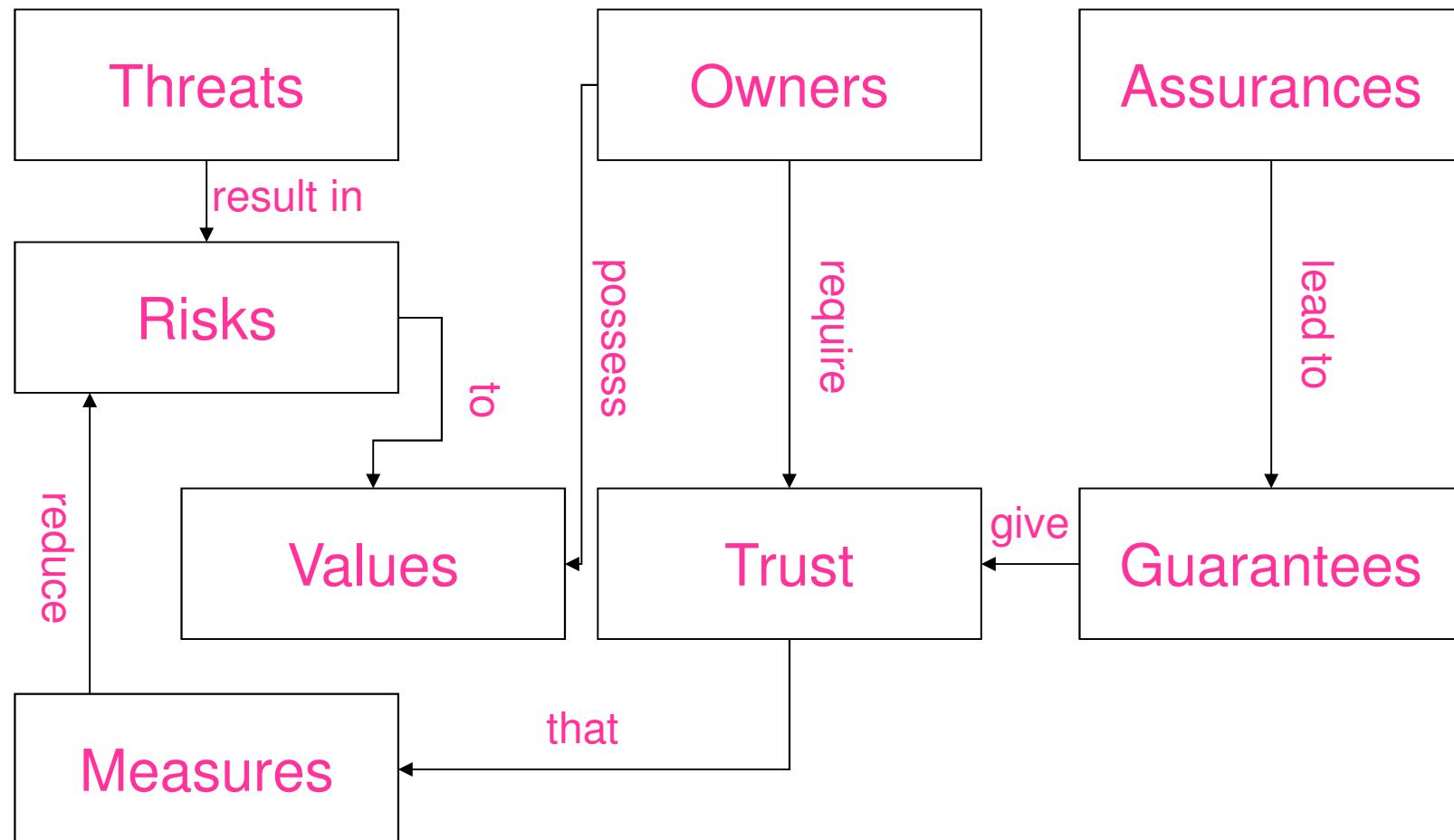
How is „IT Security“ Defined?



Definitions

- Danger: a potential
- Threat: a real danger to YOU
- Risk: the likelihood and scope of an incurred loss or damage
- **Security / IT Security: combination of all pro- and reactive measures against (IT) risks**
- Safety: mostly linked to physical dangers, but with strong ties to IT (disaster recovery)
- Laws and Regulation: general or sector/country-specific elements of governance
- Compliance: ability to prove that you have done the right things, and done them correctly or at least “good enough”
- Governance: supervision processes and structures

The „Big Picture“



Threats & Protection: the CIAO Principle



What are the Threats?

- Outsiders:
 - Hackers / Crackers / Pranksters
 - Information Collectors
 - Criminal Individuals or Organisations
 - (Foreign) Intelligence Community
 - Business Partners / Customers
 - Competitors / New Market Entries
 - Fanatics / Terrorists
 - Information Warfare
- Insiders:
 - Disgruntled Employees
 - Suppliers / (external) Maintenance Staff
 - System Specialists
 - Criminals
 - Careless Employees

What Needs to be Protected?

Basic Properties:

- Confidentiality (e.g. customer relation, contracts)
- Integrity (e.g. accounting, HR mgmt)
- Authenticity (e.g. transactions)
- Availability (e.g. Web portal)
- Obligation (e.g. legally binding signature)

but also:

- Quality / capability to react and improve
- License (e.g. for banking, telecommunication)
- Reputation (towards all stakeholders)

Pause





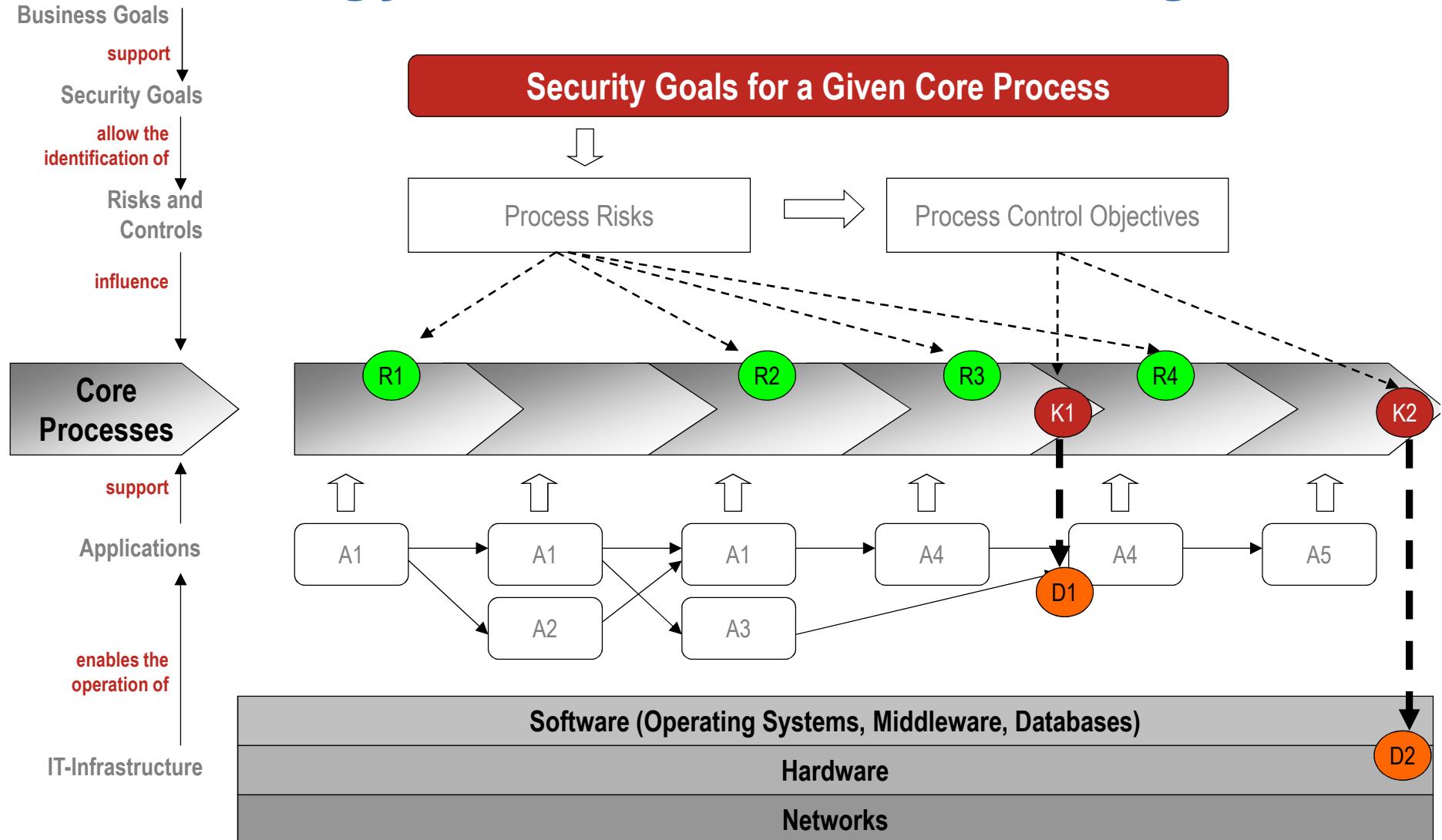
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

IT Security Scope



2012 ff

Technology → Processes → Risk Mgmt



Adapted from: Ernst & Young

IT Security Elements: Technology, Organisation, Processes, Management, Awareness



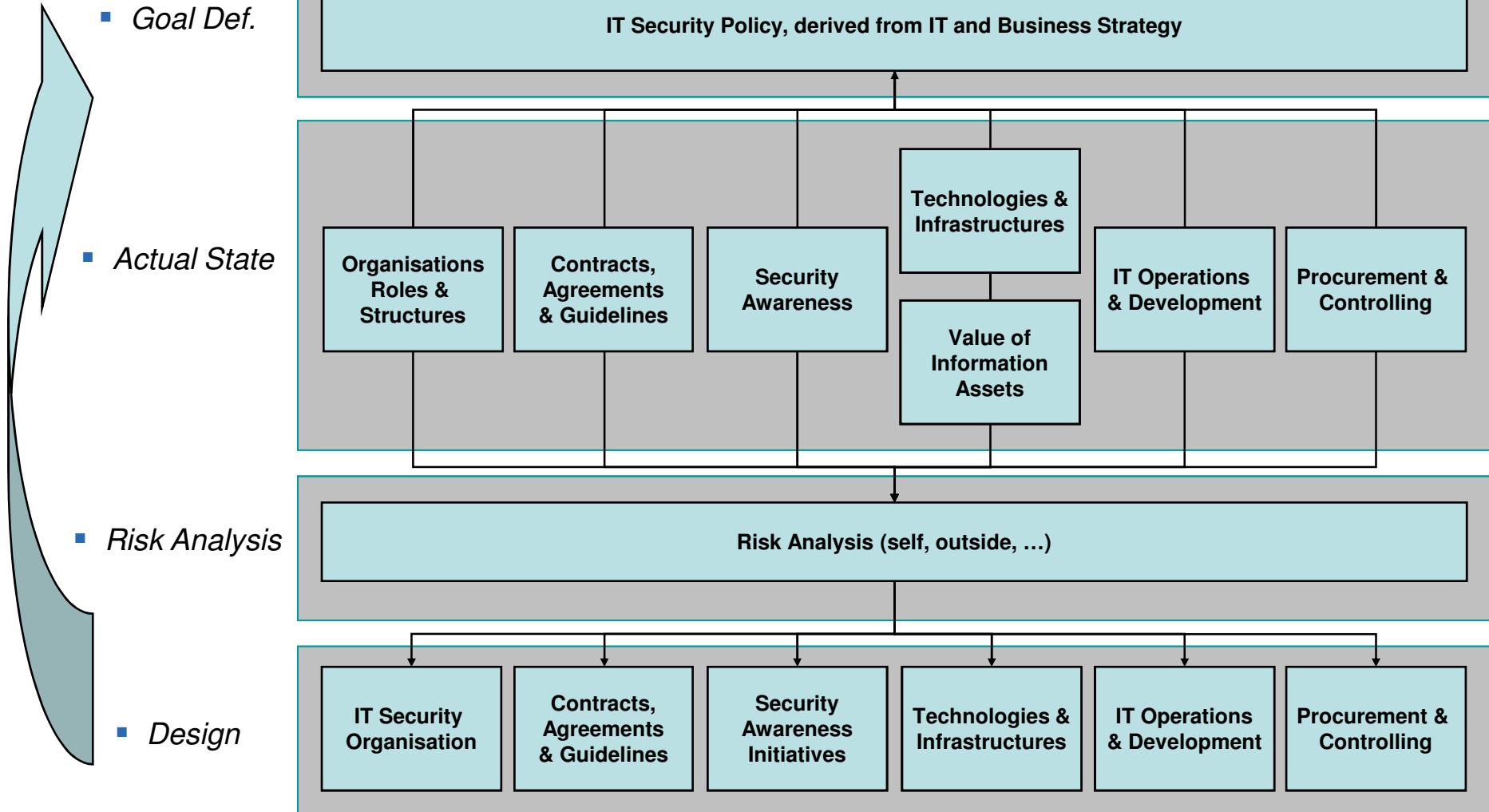
Risk Management: The PDCA Cycle



IT Security Organisation

- 3 main tasks:
 - Security Governance (pro-/reactive)
 - Security Operations
 - Security Engineering
- Deliverables:
 - Security process and key performance indicators
 - Security policy
 - Risk assessment and risk „landscape“
 - Security concept, architecture etc.
 - Security guidelines, manuals, checklists etc.
 - Project / procurement / operations consulting & reviews
 - „Firefighting“, escalations etc.

How to Approach IT Security Holistically



IT Security Embedding and Context



Business ↔ IT

Basic Principles:

IT supports business

Security supports IT
and risk management

Risks are assessed and
managed, not minimised

Source:

**IT-Trends und IT-Governance
in der Schweiz 2006**

Eine Studie von Accenture und Avanade

Wie werden IT-Governance und die Abstimmung von Geschäftsanforderungen und Informatik in Ihrem Unternehmen gelebt?

Strategie, Entscheide und Massnahmen in der IT-Abteilung weisen in dieselbe Richtung, in die sich das Unternehmen entwickelt.

Unternehmens- und Führungskultur haben einen klaren Fokus auf das Erzielen von Mehrwert.

Es besteht ein Prozess zur Priorisierung der Investitionen und die Zuteilung der Ressourcen.

Die Unternehmensleitung erhält regelmässige Statusberichte zum Kostenstand und Nutzen der IT.

Die Aufnahme und die Priorisierung der geschäftlichen Anforderungen an die IT sind standardisiert.

Die IT kann kurzfristig auf wechselnde Geschäftsanforderungen reagieren.

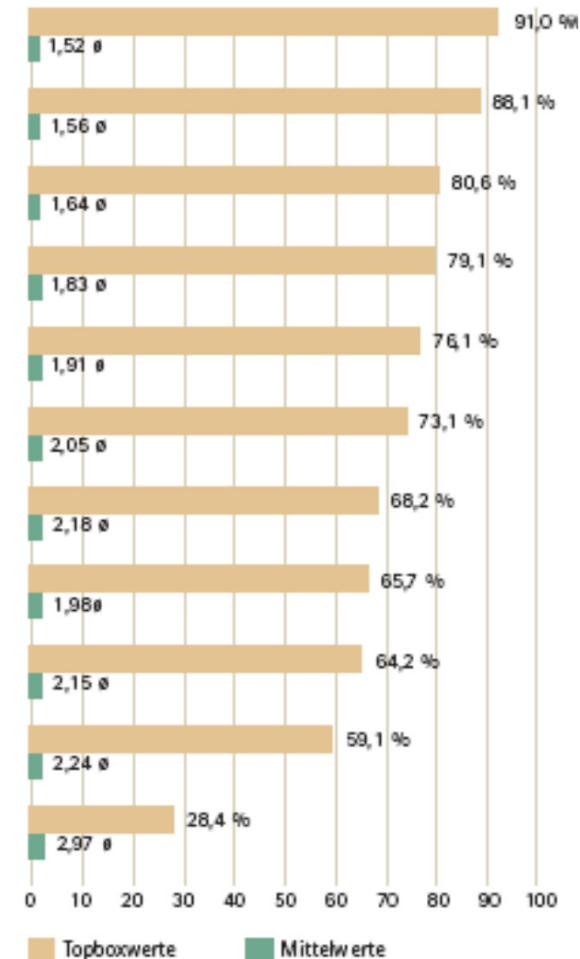
Die Prozesse, um Risiken zu steuern und zu vermeiden, sind definiert.

In der Unternehmensleitung ist IT-Fachkompetenz vertreten.

Die Unternehmensleitung erhält regelmässige Statusberichte zur Qualität der IT-Dienstleistungen.

IT-Dienstleistungen für die firmeninternen Kunden werden formell mit Hilfe von Service Level Agreements vereinbart.

Die festgesetzten Ziele und Strategien werden regelmässig von neutraler Seite geprüft.

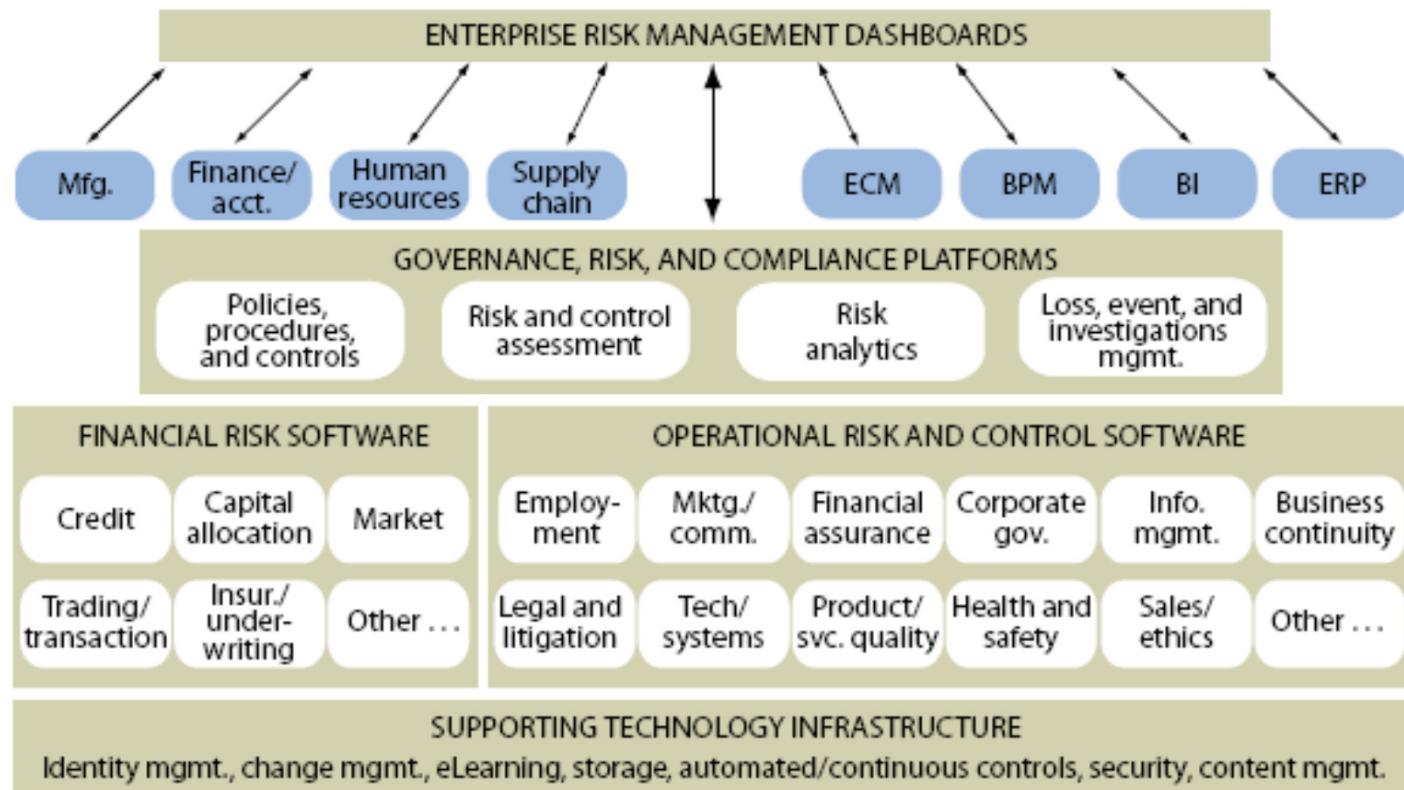


Basis: n = 67

Dargestellt sind die Topboxwerte (1+2) einer Skala von 1 bis 4 (1 = ja, 2 = eher ja, 3 = eher nein, 4 = nein) und Mittelwerte.

Security → Risk → Compliance → Governance

Figure 1 The Risk And Compliance Market Landscape



Source: Forrester Research, Inc.

Summary – Take Home Message

- IT Security employs a mix of technological, procedural, organisational and regulatory measures to protect all physical, logical and virtual IT assets against threats.
- IT Security by definition is a multi-disciplinary, “vertical” element of IT, with plenty of interfaces.
- IT Security contributes to a business-driven risk management and governance process

Threats, Attackers and Intentions

Risk and Security Management – HS 2012

PD Dr. Hannes P. Lubich



Motivation

The 5th Wave

By Rich Tennant



"They won't let me through security until I remove the bullets from my Word document."



Outline

- Risks and Threats
- Attackers, Weaknesses, Attack Scenarios
- Intentions and Motivations
- Case Studies
- What's Next?

Risks & Threats

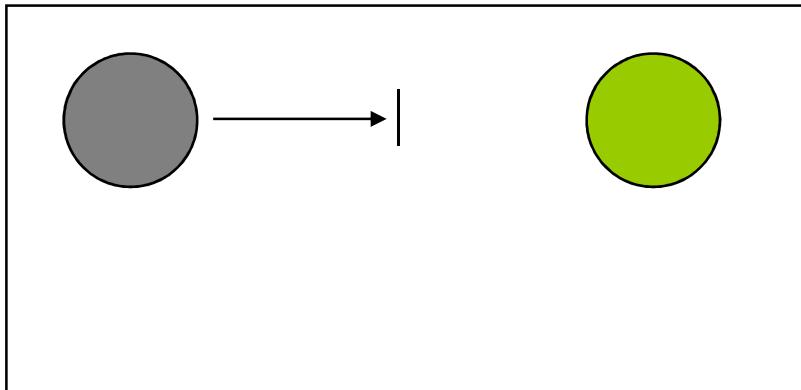


Risks in Electronic Environments

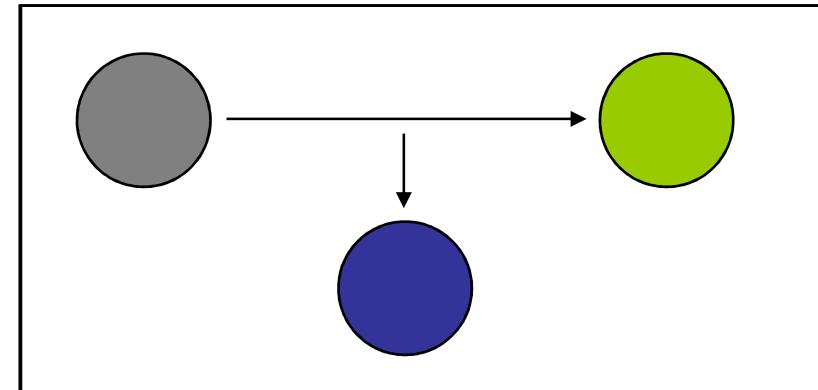
- Speed of introduction and complexity of IT environments result in an increase of (additive) weaknesses, that cannot be detected in due time.
- Networking and time/location independency of access allows better coverage of attacks, and the possibility to search for specific weaknesses.
- Better connectivity / tools benefit the attack side - e.g. through virus construction kits or use of foreign systems as platforms for an attacks (mostly denial of service).
- Origin and motivation of attackers varies substantially – so does the method of attack, and the resources used.
- Growing number of legal and compliance requirements, with personal liability to company officers.

Technical Threats

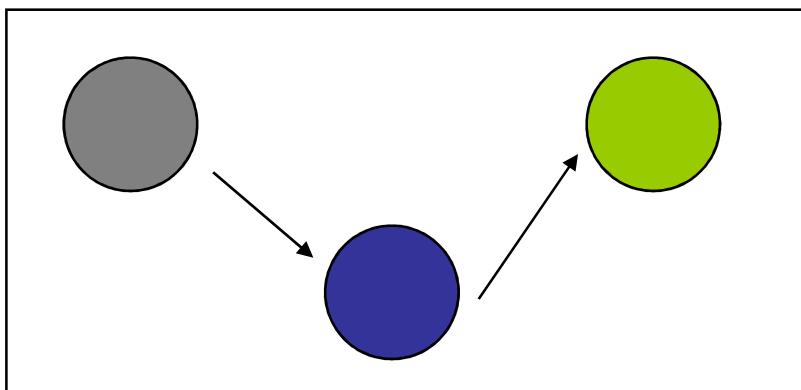
Disrupt / Delay / Delete



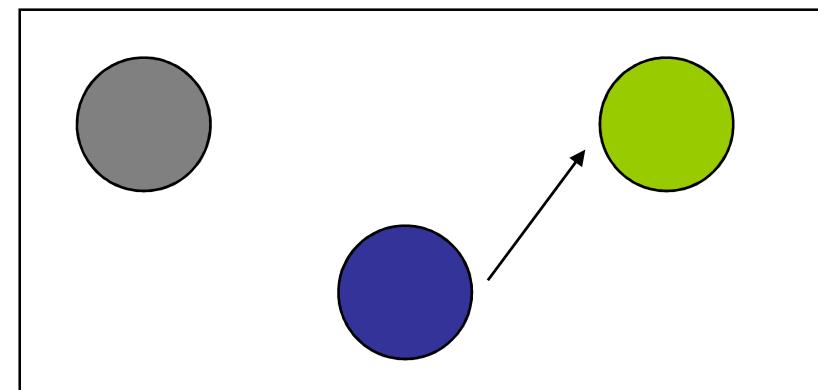
Eavesdrop / Analysis



Modify



Create



Business Threats

- Financial loss through delayed payments or forged orders
- Publication of client data or intentions
- Damaging of client data or systems
- Reputational damage, loss of license, bankruptcy
- Not allowing customers to act in time (as intermediary)

Legal / Regulatory Threats

- Publication of customer relationship (e.g. violation of banking secrecy)
- Liability for damages through IT systems / services delivered to customers
- Regulatory violations (e.g. declaration of suspicious financial transactions, accounting standards etc.).
- Violation of rules imposed by regulation / law (e.g. minimum time to retain business-critical data, non-compliance to audit requirements)
- Civil damages / contractual disputes

Societal Threats

- Blocking of a national economy or the world economy through massive blocking of payments/settlements or service delivery
- Annihilation of (financial) property in large quantities through a currency crisis or speculation on the stock markets
- Hindering of free business development up to the demise of a whole sector of a national economy through re-location of services, including loss of state tax income etc
- Denial of access for states to markets due to political pressure, embargo etc by other countries / federations

Attackers and Attack Scenarios



Knowing the Attackers

- Knowing the attacker allows you ..
 - to know his capabilities and motivations
 - the countermeasures that might thwart him / her
 - to evaluate the risks he poses
- Attackers can be categorized by ..
 - objectives, motivations, expertise, access, resources, and risk aversion
- If you mischaracterize your attackers
 - you're likely to misallocate your defenses
 - feel any difference in defending against your neighbour, me or the CIA?

Source: Stefan Frei, Network Security - WS 2006/07

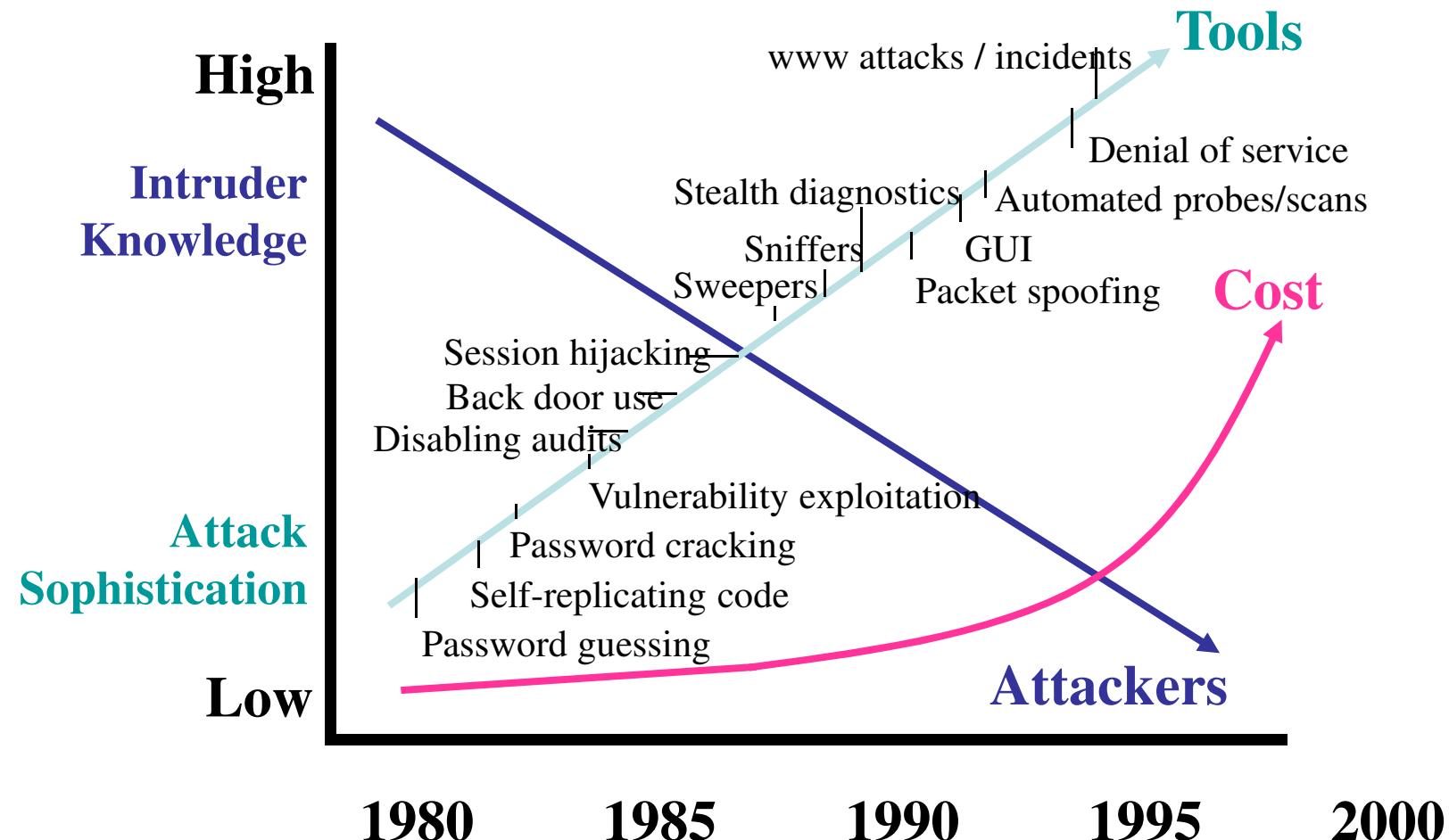
Who is Attacking?

- **Outsiders:**
 - Hackers / Crackers / Pranksters
 - Information Collectors / Press
 - Criminal Individuals or Organisations
 - (Foreign) Intelligence Community
 - Police / Law Enforcement
 - Business Partners / Customers
 - Competitors / New Market Entries
 - Fanatics / Terrorists
 - Information Warfare
- **Insiders:**
 - Disgruntled Employees
 - Suppliers / (external) Maintenance Staff
 - System Specialists
 - Criminals
 - Careless Employees
 - “Friends & Family”

Classification:

- Script Kiddie
- Intermediate
- Professional
- Elite

What Drives the Attack Curve?



Source: Telekommunikation heute, Nr. 28

The Race is on ...

Zero Day Attacks:

- No/little advance warning
- Cause and effect are difficult to differentiate
- Countermeasures must be effective in real time
- Countermeasures must be able to react to „unknown“ threats and effects

Potential Weaknesses / Attack Targets

- Physical access (premises, entry points, cabling, delivery area etc.)
- Production, distribution, installation, integration of hardware and software
- Interfaces, data feeds and applicational communication outside-in and inside-out.
- People (employees, suppliers, external maintenance personnel etc.)
- Insufficient processes, no best practices
- Facilities and processes for business continuity in case of a physical or logical crisis



Attack Scenarios

- Technology-based (hacking, viruses, worms, (distributed) denial of service, botnets, ...)
- Social (request PIN code or other information by phone or e-mail)
- Combined (Phishing, pharming, spam)
- Organisational (bribery, blackmail, staff injection)

Pause



Intentions, Motivations, Case Studies





Intentions

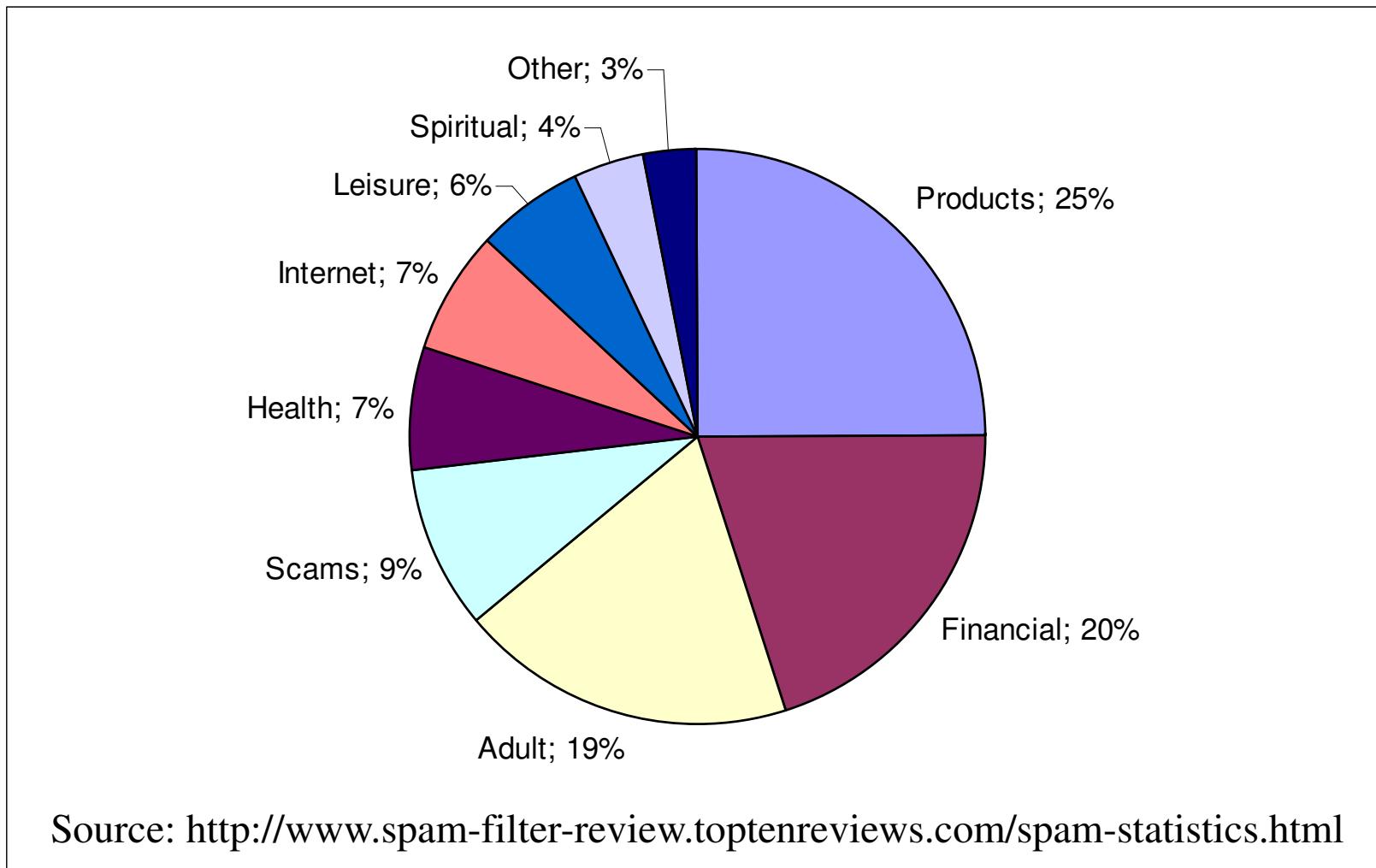
- Reputation (community, friends, public, ...)
- Being Bored (often linked to age of offender)
- Damage / Revenge (former employee, private, ...)
- Competition (offers, customers, patented infos, ...)
- Direct Benefit (software, music, ...)
- Indirect Benefit (license, information, passwd, ...)
- Private Request (commercial/industrial espionage)
- Government Request (counter-terrorism, military intelligence, ...)

Case Study - Spam

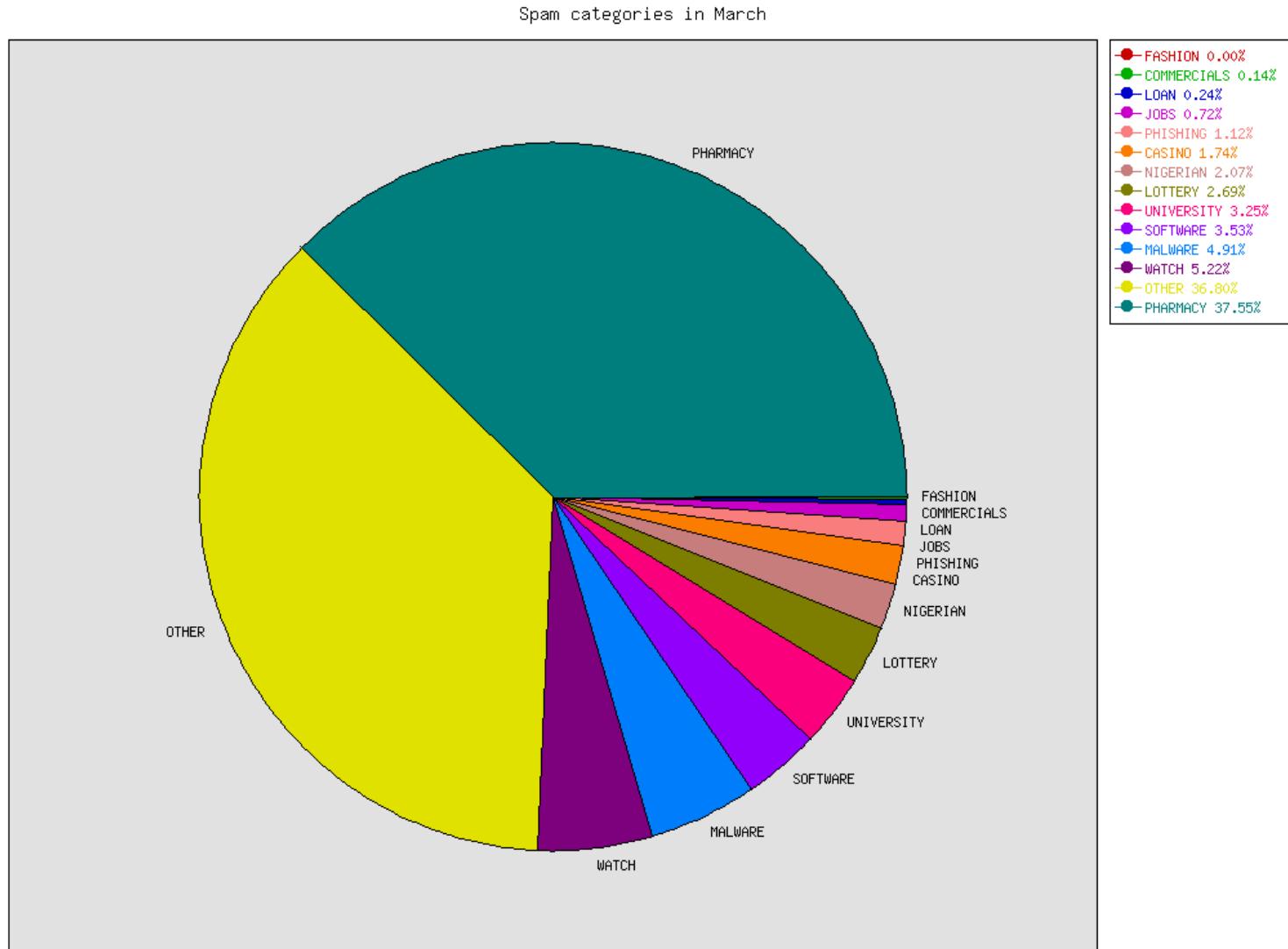


Slides courtesy of Prof. P. Heinzmann, cnlab

Spam Categories (% of total Spam): 2003



Spam Categories (% of total Spam): 2012



Source: Avira

Register Of Known Spam Operations



<http://www.spamhaus.org/rokso/>

- **100 Known Spam Operations**
 - **responsible for 80% of your spam**
 - operate 'offshore' using servers in Asia and South America
- spammer
 - listed in ROKSO if terminated by a minimum of 3 consecutive ISPs for AUP violations
 - spammers IP addresses are automatically sent to Spamhaus Block List
- ROSLO assists
 - ISP Abuse Desks
 - Law Enforcement Agencies (with special, sensitive information version)

Slides courtesy of Prof. P. Heinzmann, cnlab

Spam ... Mass Mailing Offerings on eBay

<input type="checkbox"/>		@8-MILLION VERIFIED-NEW-eMAIL-ADDRESSES-@-ADVERTISING		GBP 1.20	2	11m
<input type="checkbox"/>		210+ MILLION EMAIL ADDRESSES ON CD-ROM		C \$9.95	-	4h 02m
<input type="checkbox"/>		696 MILLION EMAIL ADDRESSES ADDRESS ON 5 CDS + MORE		\$19.95	-	5h 03m
<input type="checkbox"/>		243 Million Worldwide Email Addresses Package Mailing L		\$5.00	1 	9h 33m
<input type="checkbox"/>		243 Million Worldwide Email Addresses Package Mailing L		\$5.00	- 	10h 04m
<input type="checkbox"/>		210+ MILLION EMAIL ADDRESSES ON CD-ROM		C \$9.95	-	1d 10h 48m
<input type="checkbox"/>		1MILLION Sectored Email Addresses		GBP 29.99	-	1d 17h 55m
<input type="checkbox"/>		Why pay so much? Read on...				
<input type="checkbox"/>		@8-MILLION VERIFIED-NEW-eMAIL-ADDRESSES-@-ADVERTISING		GBP 0.99 GBP 19.95	- 	1d 22h 33m
<input type="checkbox"/>		230 Million+ Email Addresses and Bulk Email Software		\$10.00	- 	1d 22h 37m
<input type="checkbox"/>		210+ MILLION EMAIL ADDRESSES ON CD-ROM		C \$9.95	-	2d 04h 03m
<input type="checkbox"/>		5 MILLION USA/CA/UK EMAIL ADDRESSES LIST+SOFTWARE		\$2.99	- 	2d 06h 30m
<input type="checkbox"/>		244 M Email Address/Addresses List+ Software Package		\$14.99	- 	2d 11h 17m

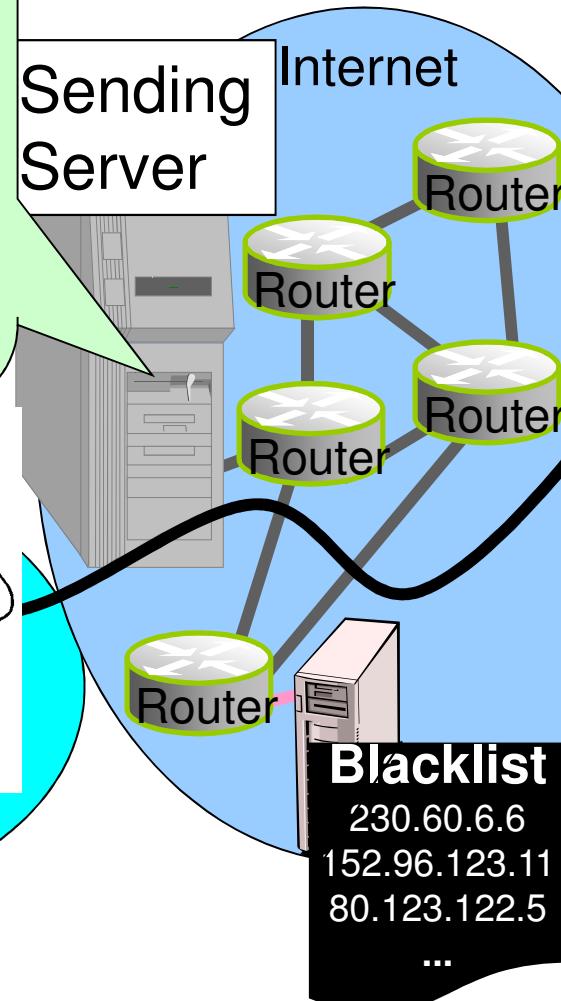
Slides courtesy of Prof. P. Heinzmann, cnlab

Spam Defense

- Accept mails from local clients only (no relaying)
- Client Authentication
- Artificial delay (tarpit)



Spammer



Blacklist
230.60.6.6
152.96.123.11
80.123.122.5
...

Receiving Server

- Filtering (Sender, Content, Tag)

- Rejection of mails (blacklists)
- Refer back to sender (SPF, greylisting)
- Filtering (Sender, content, number of similar mails etc)

Slides courtesy of Prof. P. Heinzmann, cnlab

Case Study - Spyware

- Personal Information (addresses)
- Credit Card Information
- Banking Information (→ Phishing)
- Spyware / Trojan Installation
 - Keyboard logger
 - Bots/Botnets (Zombies)
 - User Behaviour
 - Hijacking
 - Root Kits

Spyware Typology

SECURITY THREAT

Adware and Cookies

- Track user activity on the Internet
- Collect personal information

Pop-Up Ads

- Collect information for cookies
- Interrupt user transactions on the Internet
- Flood users with ads and freeze machines
- Install utilities that modify user services

Hijackers

- Modify content of web pages
- Block access to websites
- Redirect users to unintended websites
- Install hidden/backdoor processes and services that are tightly bound to OS
- Disrupt websites used for mission-critical applications

Spyware (Overt)

- Gains a remote control capability, which includes searching and reading local files
- Has a self-updating capability
- Often includes a network sniffer
- Can usually activate webcam or microphone
- Usually logs all keystrokes

SYSTEM DEGRADATION

© Computer Associates

Making Money

- "You can buy a U.S. identity - a credit card, bank account, Social Security, date of birth - for US\$ 20. A single U.S.-based credit card ranges from \$1 to \$6, with U.K.-based cards a little higher, \$2 and \$12. Access to an online bank account with \$9,900 in it would go for about \$300."

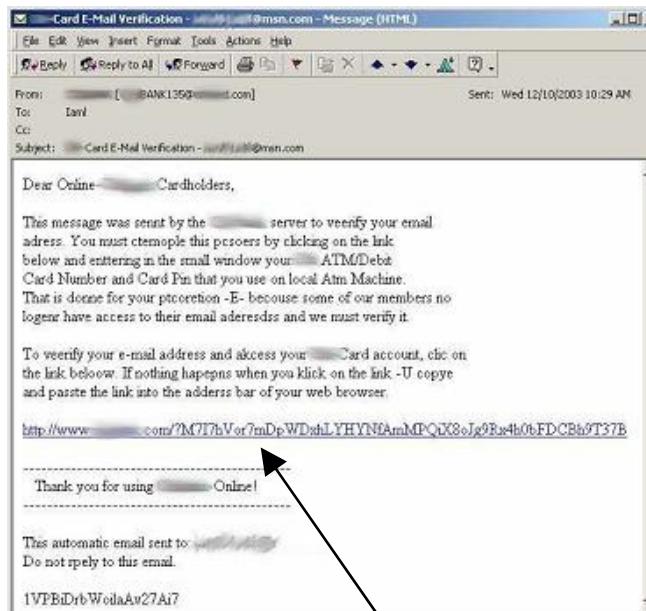
(Alfred Huger, vice president of engineering, Symantec, 2007)

Spyware Defense

- Real – time protection (mostly integrated into personal firewalls and/or anti-virus offerings)
- Local scanners (AdAware, Spyware, Pestpatrol, ...)
- Traffic / behaviour-based scanners (e.g. through access routers with forensics capabilities or dedicated network forensics)
- Collateral-based: what information has been compromised (e.g. credit card, phone number)

Case Study – Phishing

1. Spoof E-Mail (Spam)

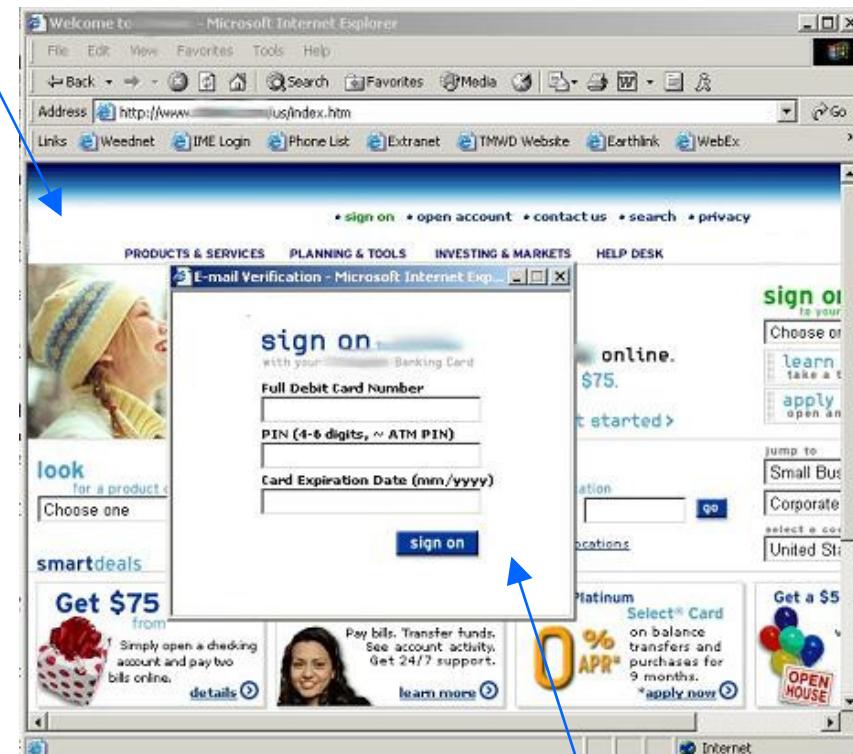


2. Camouflaged Hyperlink

www.yourbank.com/myaccount

Real site

3. Spoofed Web Site



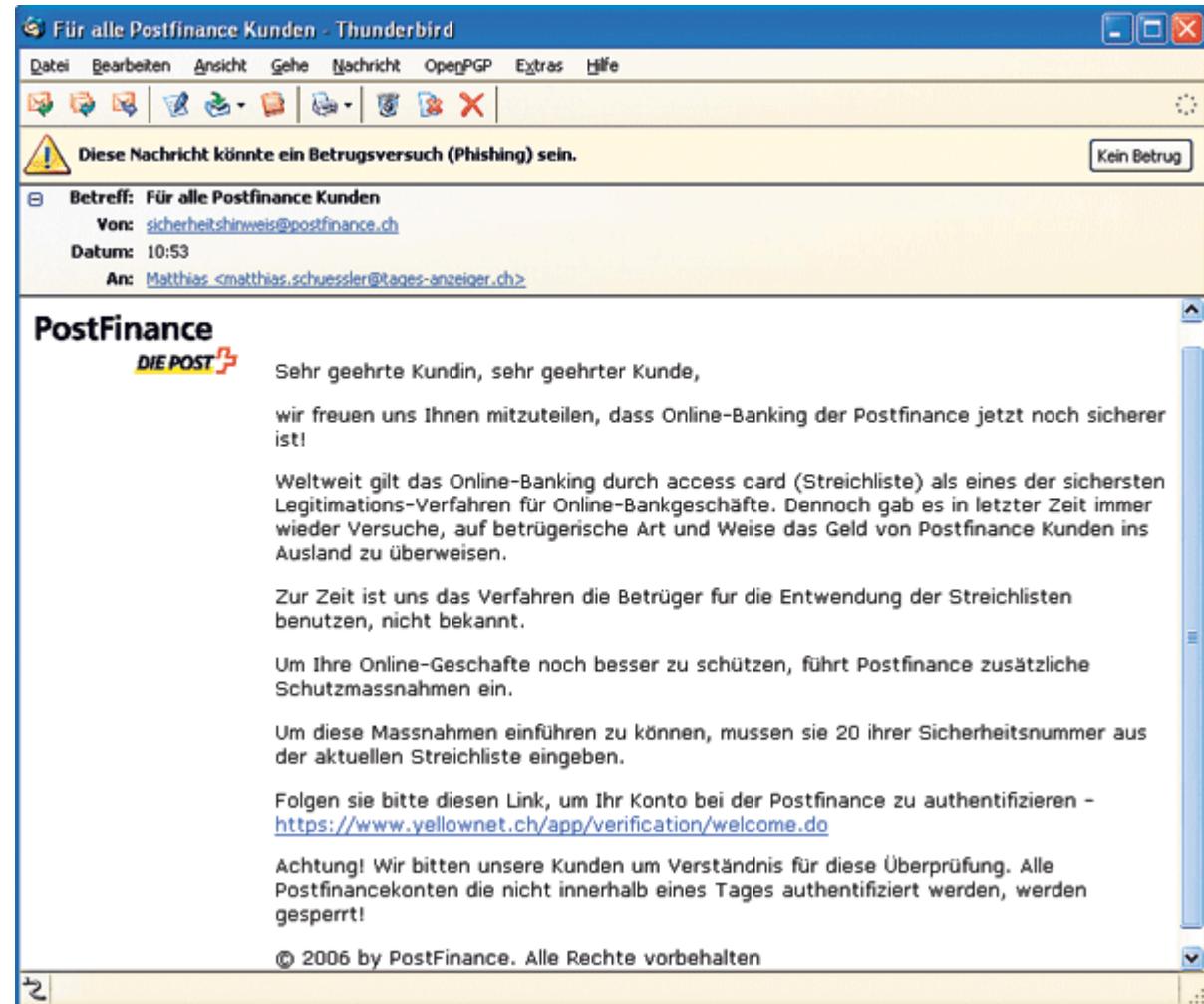
Phishing Defense

Blacklists

Tag Scans

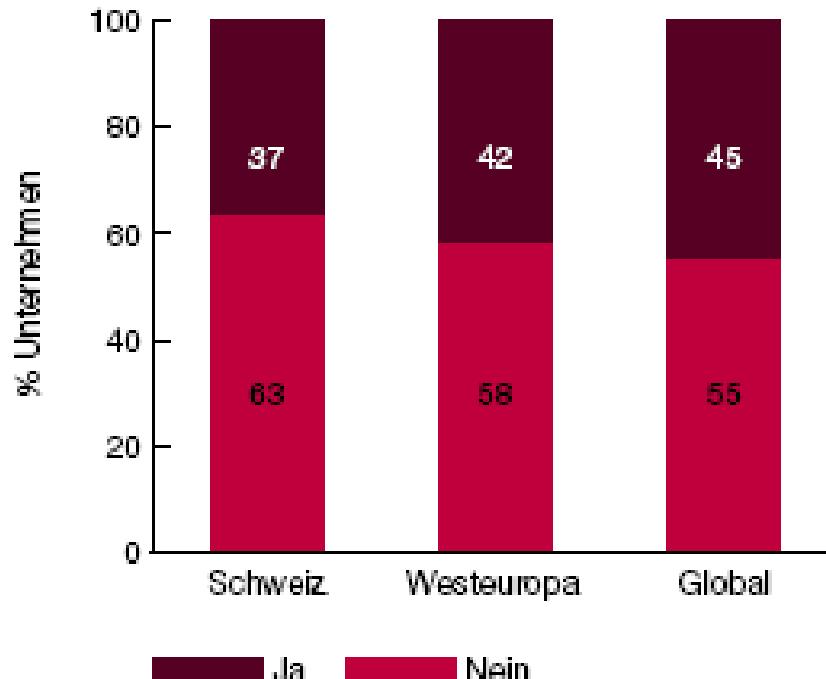
Content Scans

Active Testing

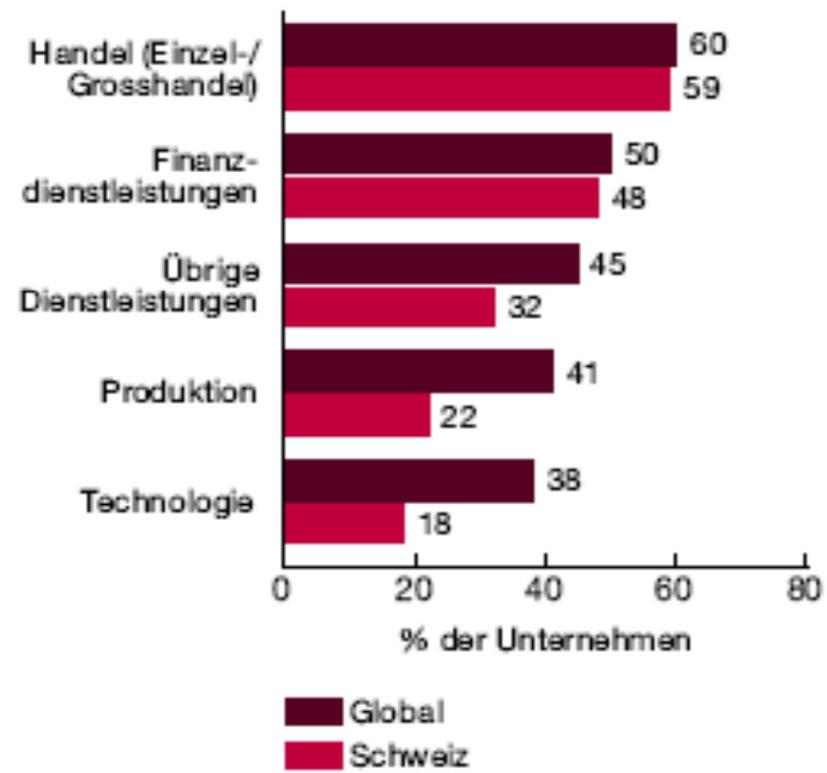


Case Study – Industrial Espionage

Opfer von Wirtschaftskriminalität gemäss Umfrage 2005



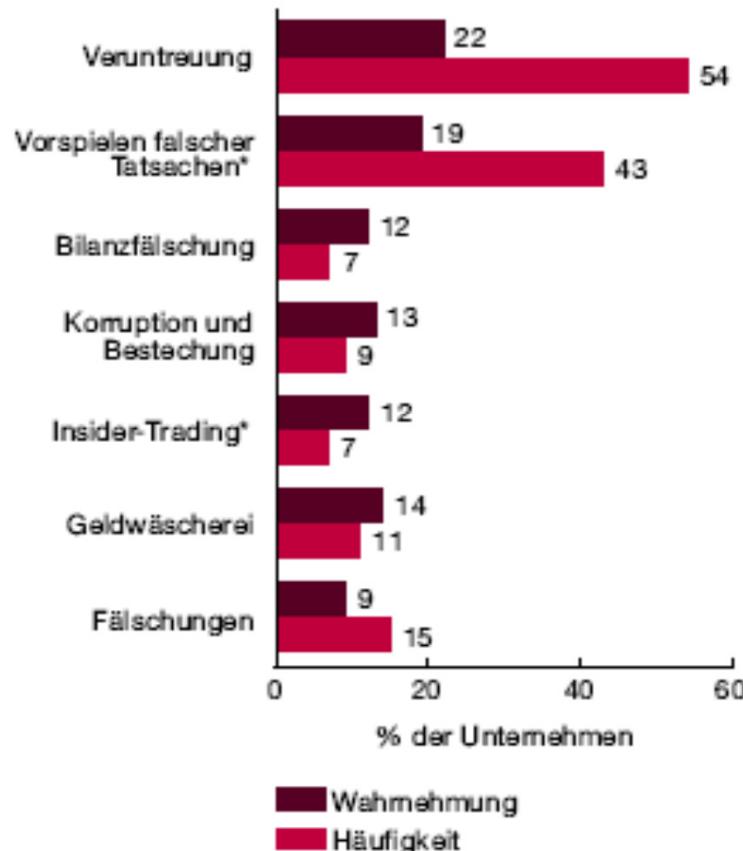
Opfer von Wirtschaftskriminalität (nach Wirtschaftszweig)



PwC Umfrage zur Wirtschaftskriminalität 2005 Schweiz

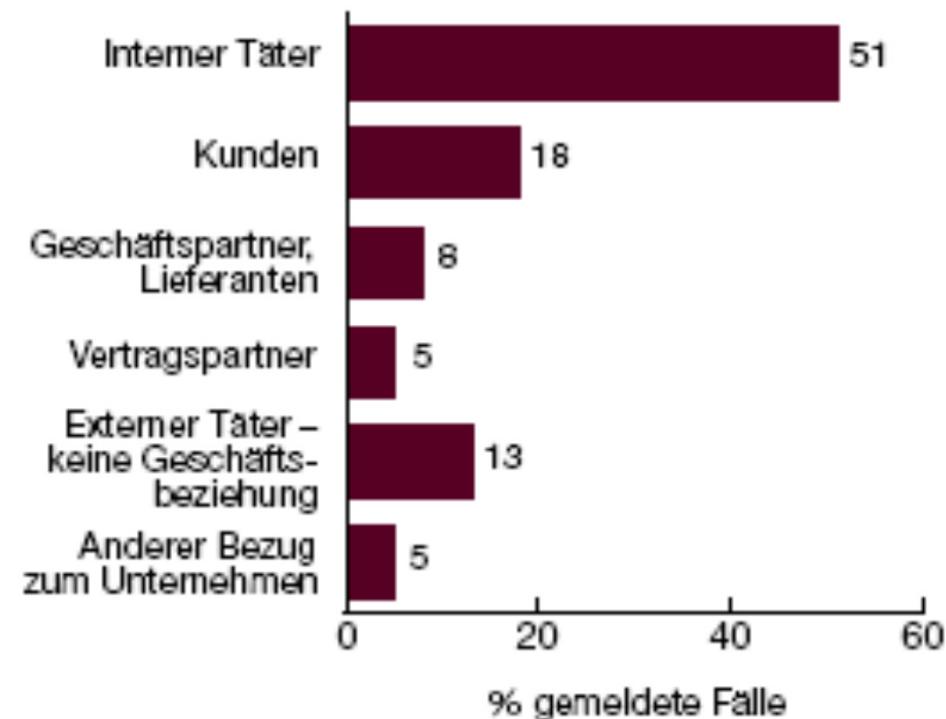
Case Study – Industrial Espionage

Wahrnehmung und Häufigkeit der verschiedenen Deliktarten



* Diese beiden Kategorien wurden der Umfrage 2005 neu hinzugefügt.

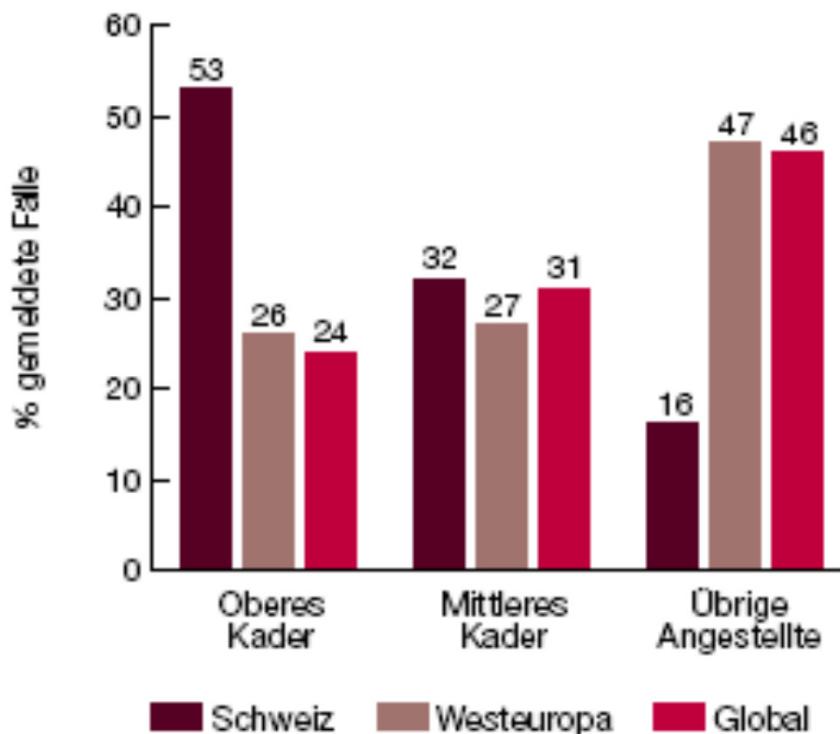
Beziehung des Täters zum Unternehmen



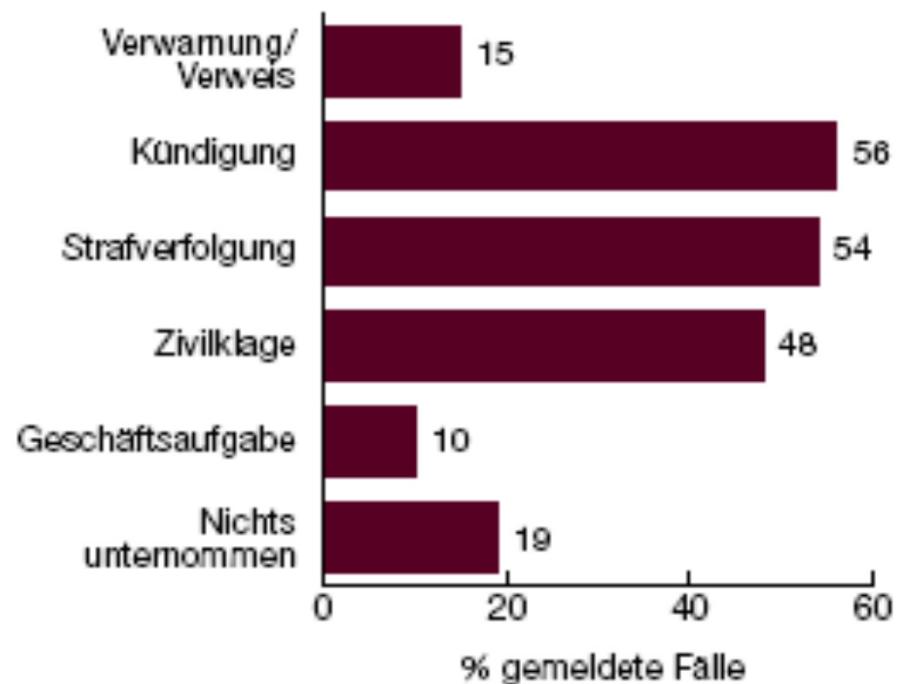
PwC Umfrage zur Wirtschaftskriminalität 2005 Schweiz

Case Study – Industrial Espionage

Position innerhalb einer Organisation



Vorgenommene Strafmaßnahmen



See also: FBI / CSI Annual Computer Crime Survey

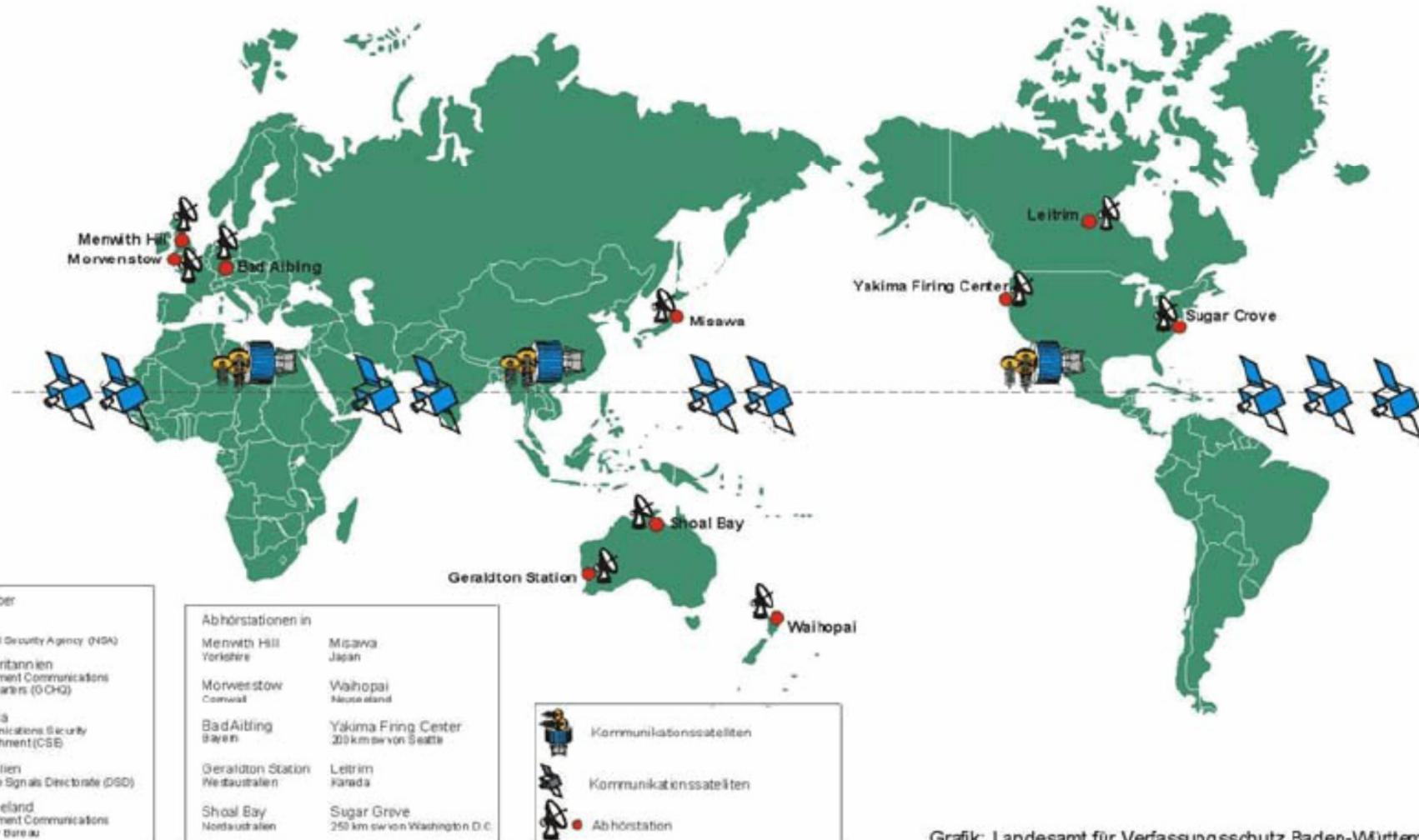
PwC Umfrage zur Wirtschaftskriminalität 2005 Schweiz

Case Study – Intelligence Community

- Economic Espionage (borders on industrial espionage) – after the end of the cold war, a large number of countries ended up with intelligence agencies having to justify cold-war budgets.
- One way to „re-use“ these skills is to help protect / sustain / grow the national economy base, e.g.:
 - South Korean High Speed Train (ICE vs. TGV): 1993
 - Wind Power Stations (Enercon/DE vs. NSA): 1998

Globales elektronisches Aufklärungssystem Echelon

Echelon hört ungefiltert den gesamten eMail-, Telefon-, Fax- und Telexverkehr ab, der weltweit über Satelliten weitergeleitet wird.



Ecole de guerre économique - Intelligence économique, guerre de l'information, infowar - Microsoft Internet Explorer

Datei Bearbeiten Ansicht Ebenen Eigene 2

Zurück Voriges Abbrechen Aktualisieren Startseite Suchen Favoriten Verlauf E-Mail Drucken

Adresse: <http://www.ege.esisca.ch/> Wechseln zu Links

EGE

Rechercher

Pourquoi l'EGE
Historique
Programme
Formation continue
Revue de presse
Bibliographie
Intelligence Eco.

Événements
Liens

Forums

Travaux d'étudiants
S'inscrire

E-MAIL

école de guerre économique
de groupe esisca

"Se faire battre est excusable, se faire surprendre est impardonnable"
Napoléon

Nous remercions M Didier Pineau-Valencienne d'avoir accepté d'être le parrain de la troisième promotion de l'Ecole de Guerre Economique.

Déroule cycle de stratégies d'intelligence économique
eslsca

Frappes informationnelles contre les entreprises : l'offensif prime sur le défensif par Christian Harbulot.
Article à paraître dans le numéro d'été 2000 de la revue "Pouvoir d'entreprise". Elle est distribuée auprès des 2000 premiers chefs d'entreprise en France.

Dans la mesure où les affrontements économiques ont été dominés par des réalisations offensives d'envergure militaire, la renommée n'enait alors

Intelligence Community

- Military Intelligence / Counter-Terrorism / Homeland Protection (9/11 aftermath)
- Critical Infrastructure Protection
 - Water
 - Energy production / distribution
 - Food
 - Transportation
 - Communication
 - Information Processing
- Active (Mis)-Information Dissemination

Al-Qaeda plot to bring down UK internet-News-UK-Crime-TimesOnline - Microsoft Internet Explorer provided by CA

File Edit View Favorites Tools Help

Back Favorites Address <http://www.timesonline.co.uk/tol/news/uk/crime/article1496831.ece> Go

TIMESONLINE

The "war on drugs" is a tabloid fantasy India Knight
[Send your views](#)

NEWS COMMENT BUSINESS SPORT LIFE & STYLE ARTS & ENTERTAINMENT OUR PAPERS AUDIO / VIDEO CLASSIFIEDS

UK WORLD POLITICS WEATHER TECH & WEB RELATED REPORTS

Where am I? > Home > NEWS > UK > Crime Sponsored by Windows Live SEARCH

From The Sunday Times MY PROFILE OFFERS SITEMAP

Al-Qaeda plot to bring down UK internet

David Leppard

SCOTLAND YARD has uncovered evidence that Al-Qaeda has been plotting to bring down the internet in Britain, causing chaos to business and the London Stock Exchange.

In a series of raids, detectives have recovered computer files revealing that terrorist suspects had targeted a high-security internet "hub" in London.

The facility, in Docklands, houses the channel through which almost every bit of information on the internet passes in or out of Britain.

The suspects, who were arrested, had targeted the headquarters of Telehouse Europe, which houses Europe's biggest "web hotel", containing dozens of "servers", the boxes which contain the information that makes up the web.

Security experts say the plot against Britain's internet "hub"

EXPLORE CRIME

- › CRIME
- › EDUCATION
- › HEALTH
- › SCIENCE

TIMES RECOMMENDS

- › Focus: Cash for honours: The end game
- › The flight now leaving Heathrow is...empty
- › Neglected war veterans wait on NHS

LAW PANEL >

Your passport to international business. **TIMESONLINE**



Done Internet

New Threats and Attack Scenarios

- Uncontrolled mobility/ ubiquitous computing, spontaneous networking
- Information warfare, “hacktivism” and cyber-terrorism
- Dependency on technology / critical infrastructure protection
- Multinational regulation issues
- New Technologies (e.g. quantum computing, knowledge-based systems)

Summary – Take Home Message

- Several types of threats (from technical to organisational or social) offer ways to attack ICT infrastructures.
- Several types of attackers make use of a broad range of security weaknesses with different motivations.
- Motivations range from reputation issues to commercial or political reasons.
- As there will always be new threats and weaknesses, there will always be new exploit motivations and attacks.

IT Security Standards, Baselines and Best Practices

Risk and Security Management – HS 2012

PD Dr. Hannes P. Lubich



Motivation



Outline

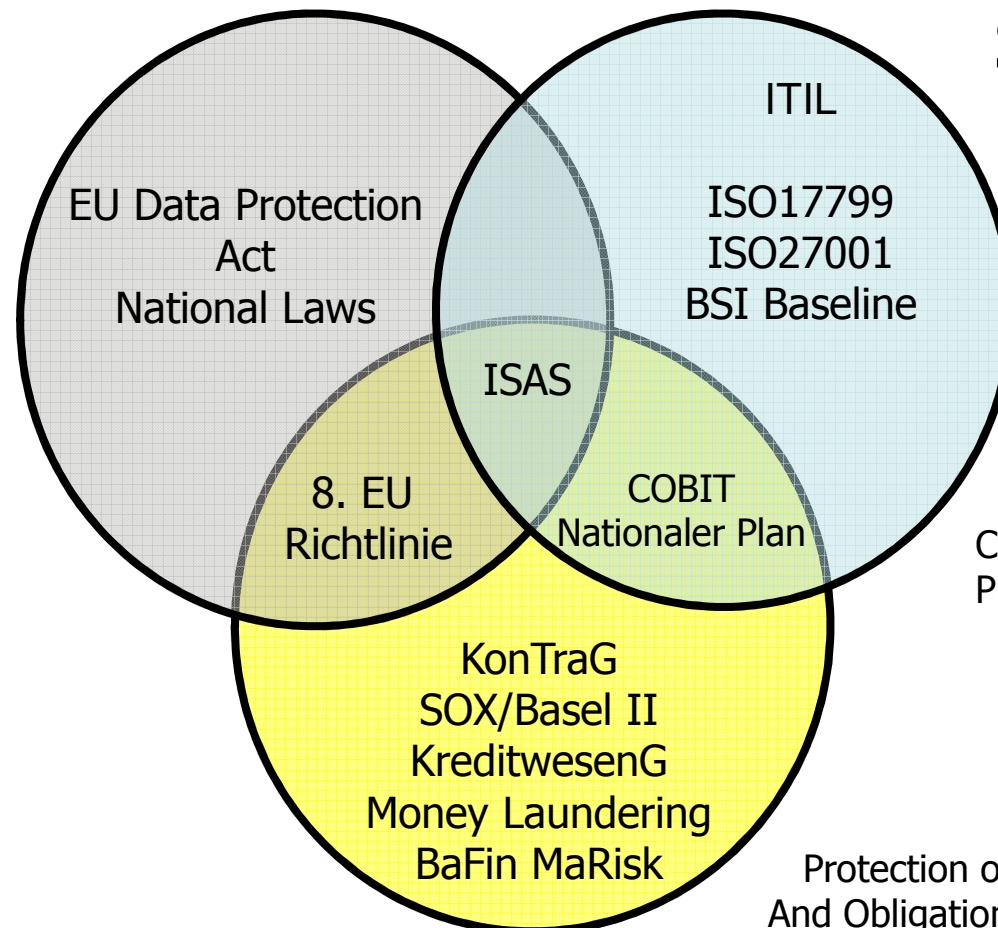
- Why Standards?
- How are Standards Created?
- Which Standards Exist?
- Baseline Protection Model
- Best Practices

Why Standards?



Standards „Drivers“

Privacy

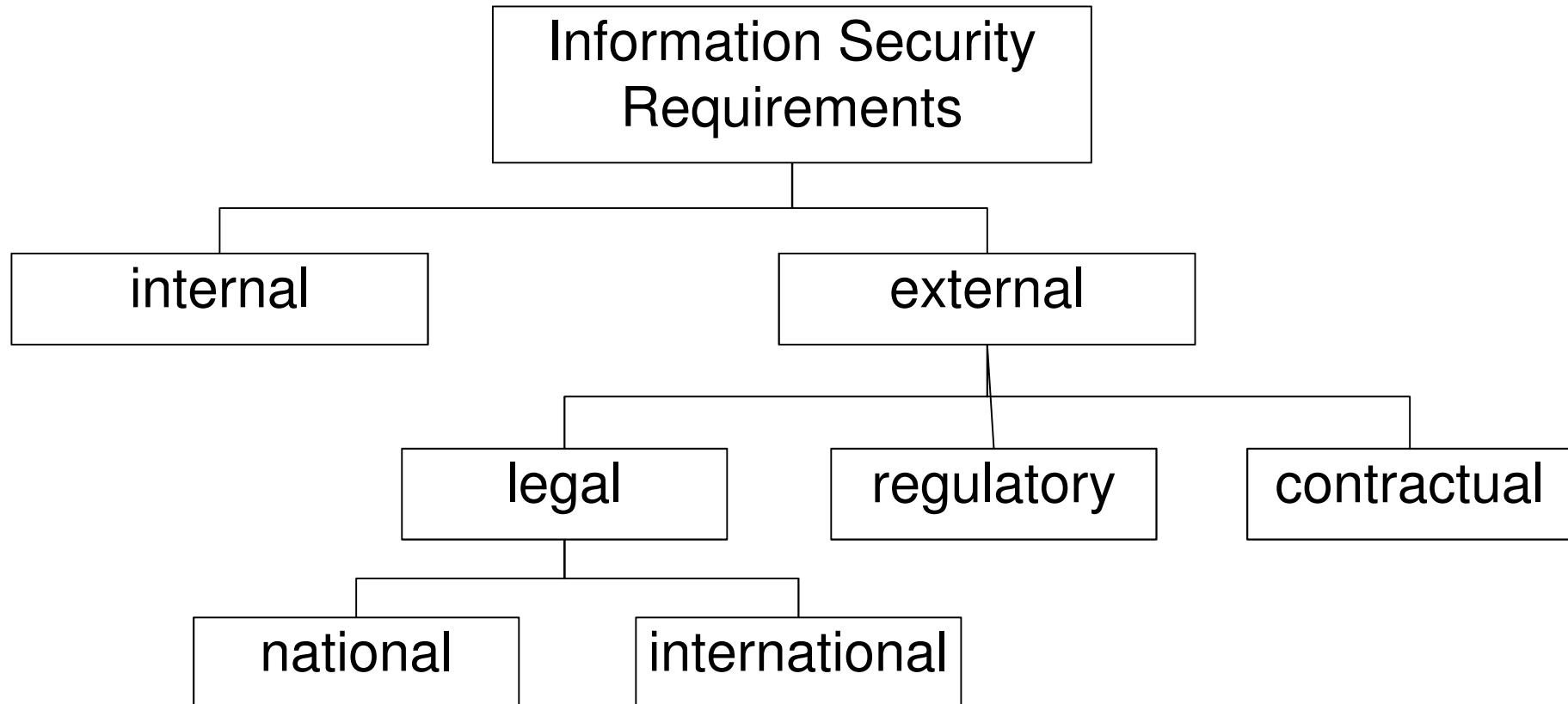


Security

Governance

Source: IT Compliance Institute

Requirements for IT Security



Based on: Compliance durch Standards für Informationssicherheit, Diplomarbeit S. Dummer, Univ. Regensburg, SS 2006

How are Standards Created?



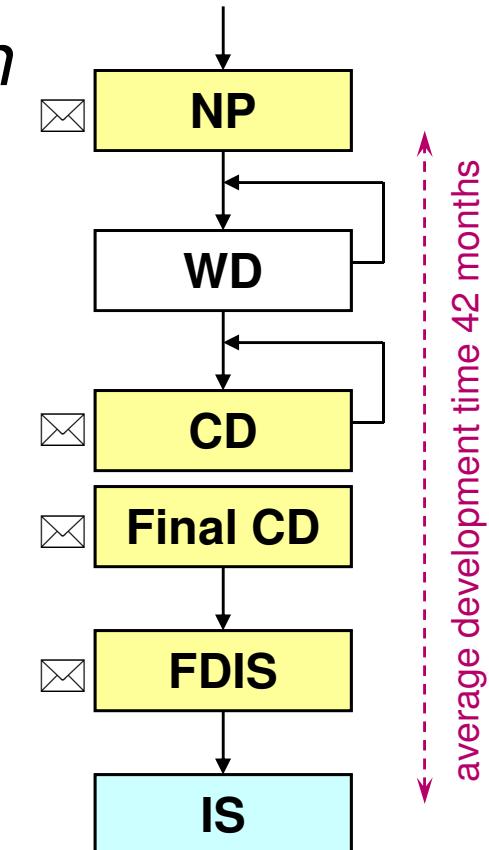
International Organization for Standardisation (ISO)

- Worldwide federation of national standards bodies from 146 countries, one from each country, e.g.,
 - DIN – Deutsches Institut für Normung ([DIN](#))
 - SNV – Schweizerische Normen-Vereinigung
- ISO was established in 1947 (www.iso.org)
- *Mission*
 - to promote the development of standardization and related activities in the world with a view to facilitating the international exchange of goods and services, and to developing cooperation in the spheres of intellectual, scientific, technological and economic activity.
- > 3000 technical bodies
 - ca. 200 technical committees (TCs)
 - ca. 600 subcommittees (SCs)
 - >> 2000 working groups (WGs)
- ISO's work results in international agreements which are published as International Standards (IS)
 - ca. 16'000 standards and standards-type documents
 - 1.247 (59.527 pages) published in 2004 alone

Source: Roadmap Sicherheitsmanagement-Standards der ISO, Walter Fumy, Siemens

ISO Standardization Process

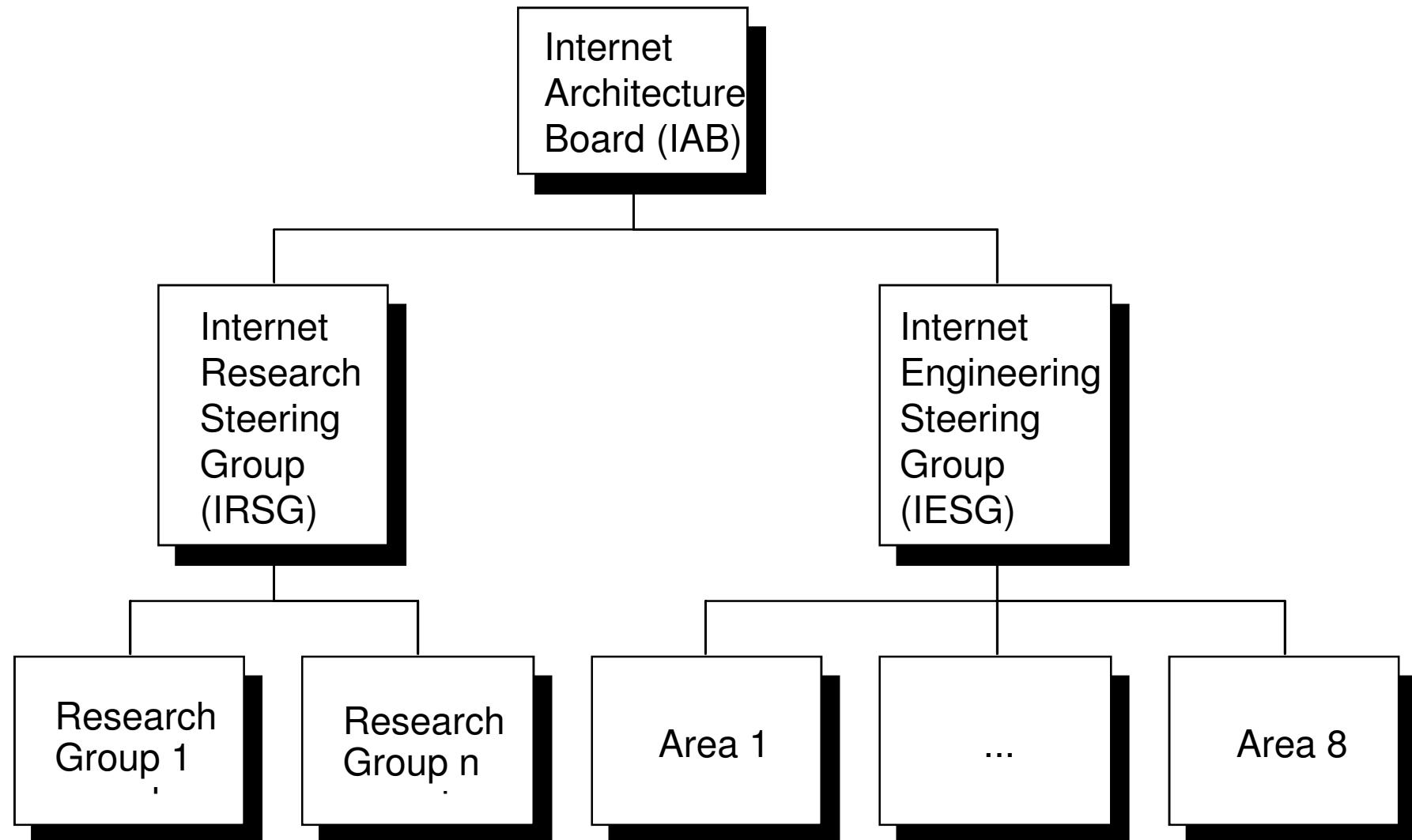
- *Maturity level / state of standardization*
 - Study Period / New Project (NP)
 - 2 month NP letter ballot*)
 - **Working Draft (WD)**
 - **Committee Draft (CD/FCD)**
 - 3 month CD ballot(s)
 - 4 month FCD ballot
 - **Draft International Standard (DIS/FDIS)**
 - 2 month FDIS ballot
 - no more comments at this stage
 - **International Standard (IS)**
 - review every 5 years
 - or after 'defect report'



*) one vote per P-member

Source: Roadmap Sicherheitsmanagement-Standards der ISO, Walter Fumy, Siemens

Internet Standardisation



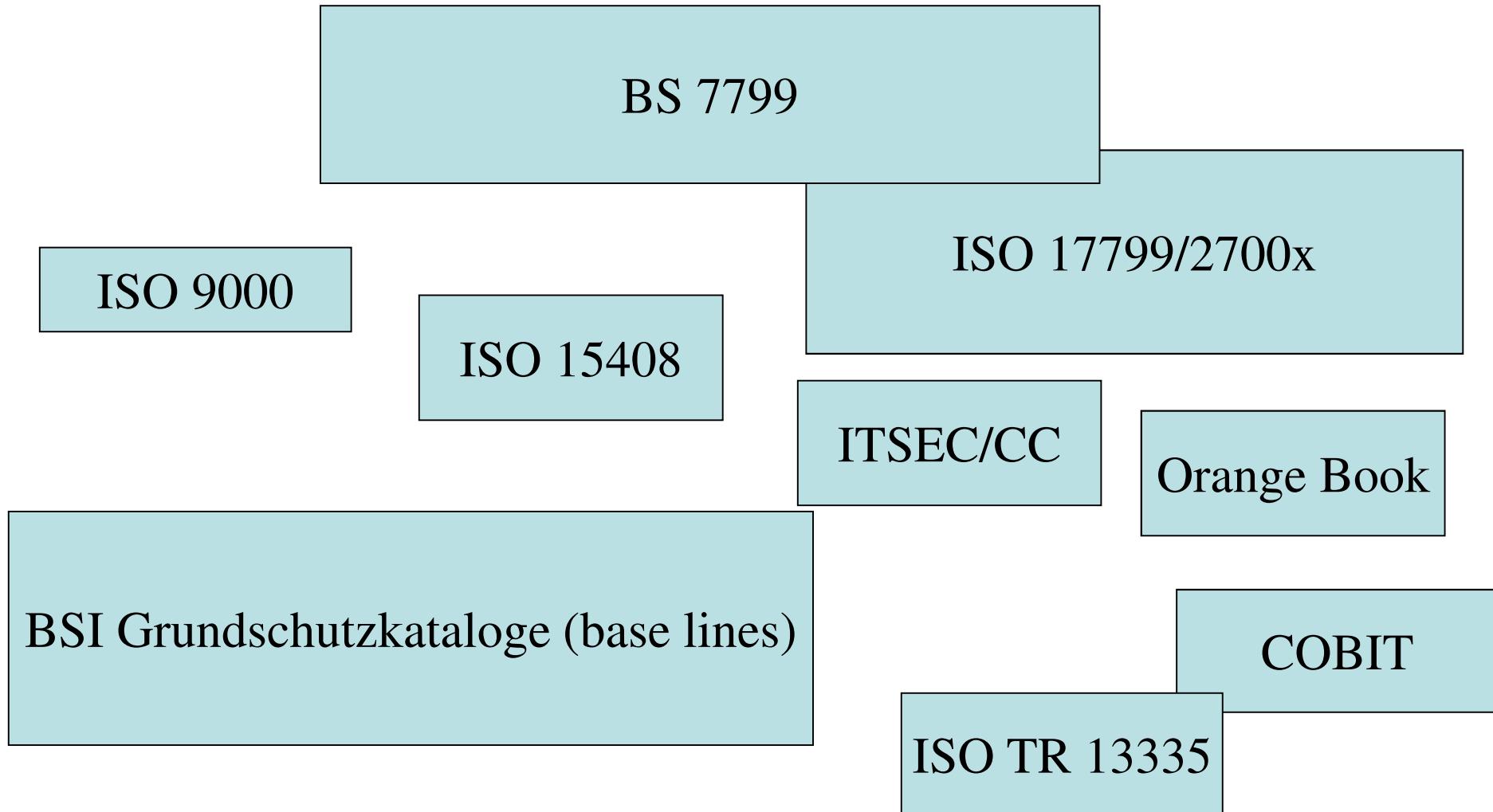
The Internet Standardisation Process

- Request for Comment (RFC): A series of electronically available publications, which describe various aspects of the Internet
- Earlier publications: Internet Engineering Notes (IEN)
- State of an Internet protocol:
 - Initial Protocol is candidate for a standard
 - Proposed Standard Protocol proposed as a standard; protocol is examined by IETF working groups)
 - Draft Standard examination result positive; at least two independent implementations are developed and examined
 - Standard protocol and implementations examination results are positive; becomes part of the TCP/IP protocol suite
 - Experimental protocol is used for experimental purposes only
 - Historic protocol is obsolete; no longer used

Which Standards Exist?

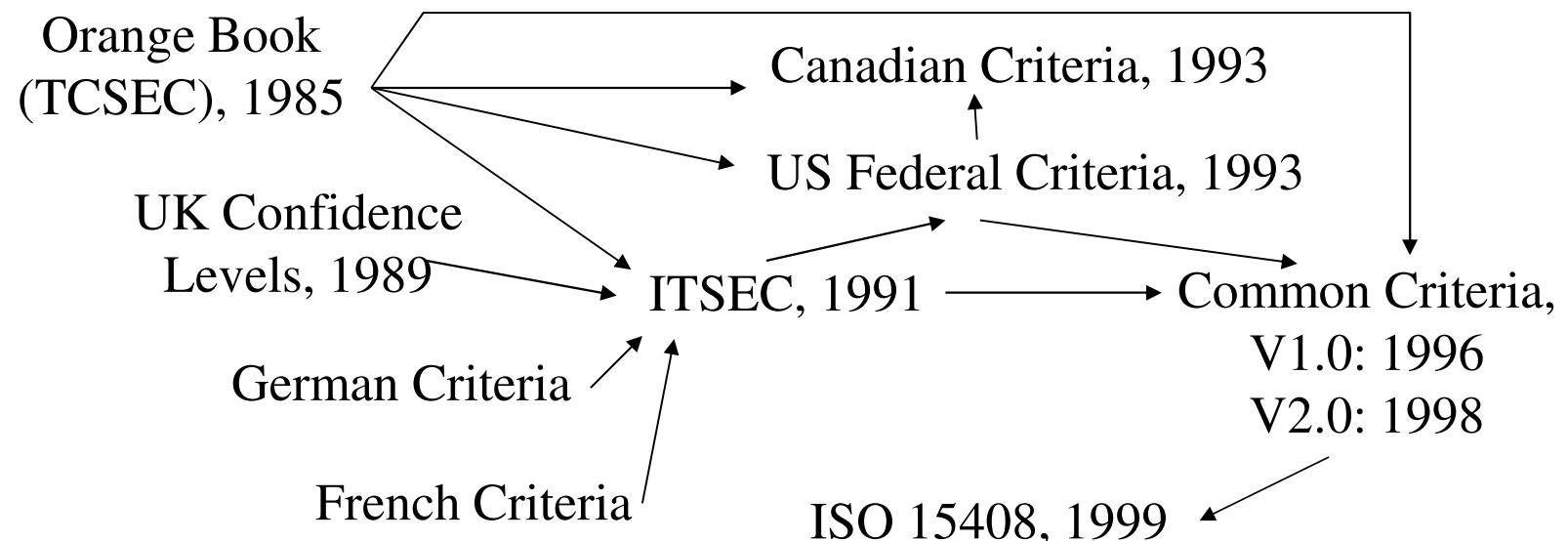


Security Standards: Overview



ITSEC/CC = ISO 15408:1999

- Evaluation of security properties of products (procurement)



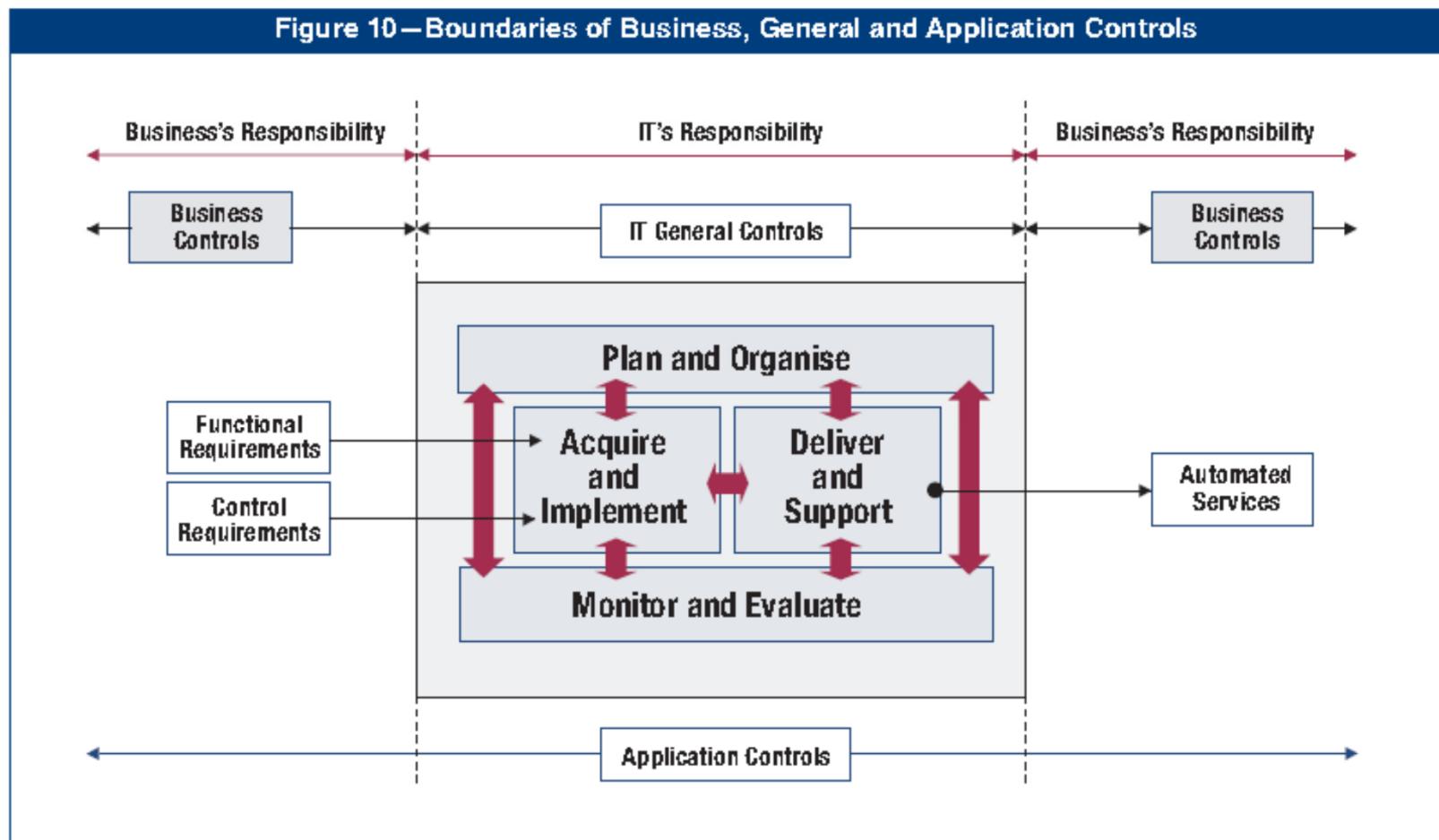
ISO 9000 / ISO TR 13335 / COBIT

- ISO 9000: Series of standards for planning and operating of a quality management system; Definition of verification / certification methods (service mgmt → ISO 20000)
- ISO 13335: 5 technical „best practice“ reports:
 - Concepts / models for IT Security: Processes
 - Management / planning of IT Security: ITSEC Process
 - Techniques for the management of IT Security: Methods
 - Selection of security criteria: Baseline Protection
 - Network security
- COBIT: Control Objectives for Information and Related Technology von ISACA (Information Systems Audit & Control Assoc.): Audit-oriented view of security

Pause



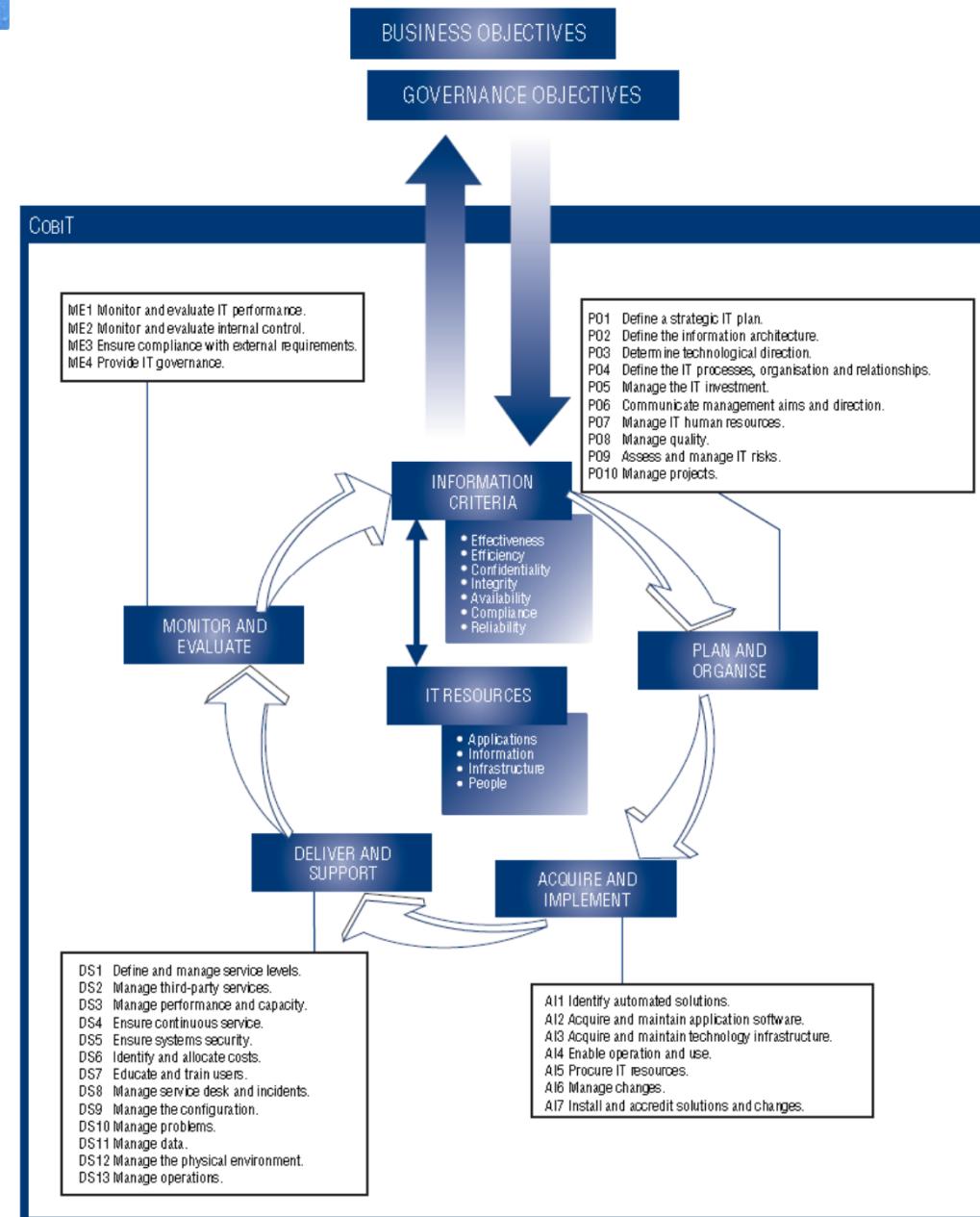
COBIT – Version 4.x



4 Domains - 34 Processes - 210 Control Objectives

COBIT

Figure 23—Overall COBIT Framework



COBIT

- DS5 (Ensure Systems Security) is the COBIT objective that relates specifically to internal security controls.

PLANNING AND ORGANISATION

- PO1** Define a Strategic IT Plan
- PO2** Define the Information Architecture
- PO3** Determine Technological Direction
- PO4** Define the IT Organisation and Relationships
- PO5** Manage the IT Investment
- PO6** Communicate Management Aims and Direction
- PO7** Manage Human Resources
- PO8** Ensure Compliance with External Requirements
- PO9** Assess Risks
- PO10** Manage Projects
- PO11** Manage Quality

ACQUISITION AND IMPLEMENTATION

- AI1** Identify Automated Solutions
- AI2** Acquire and Maintain Application Software
- AI3** Acquire and Maintain Technology Infrastructure
- AI4** Develop and Maintain Procedures
- AI5** Install and Accredite Systems
- AI6** Manage Changes

DELIVERY AND SUPPORT

- DS1** Define and Manage Service Levels
- DS2** Manage Third-Party Services
- DS3** Manage Performance and Capacity
- DS4** Ensure Continuous Service
- DS5** Ensure Systems Security
- DS6** Identify and Allocate Costs
- DS7** Educate and Train Users
- DS8** Assist and Advise Customers
- DS9** Manage the Configuration
- DS10** Manage Problems and Incidents
- DS11** Manage Data
- DS12** Manage Facilities
- DS13** Manage Operations

MONITORING

- M1** Monitor the Processes
- M2** Assess Internal Control Adequacy
- M3** Obtain Independent Assurance
- M4** Provide for Independent Audit

Source: CA Inc.

COBIT – Vers. 5 Came Out in Spring 2012

1. New Governance of Enterprise IT Principles
2. Increased Focus on Enablers
3. New Process Reference Model
4. New and Modified Processes
5. Practices and Activities
6. Goals and Metrics
7. Inputs and Outputs
8. RACI Charts
9. Process Capability Maturity Models and Assessments

COBIT 5 Process Reference Model

Processes for Governance of Enterprise IT

Evaluate, Direct and Monitor

EDM01 Ensure Governance Framework Setting and Maintenance

EDM02 Ensure Benefits Delivery

EDM03 Ensure Risk Optimisation

EDM04 Ensure Resource Optimisation

EDM05 Ensure Stakeholder Transparency

Align, Plan and Organise

AP001 Manage the IT Management Framework

AP002 Manage Strategy

AP003 Manage Enterprise Architecture

AP004 Manage Innovation

AP005 Manage Portfolio

AP006 Manage Budget and Costs

AP007 Manage Human Resources

AP008 Manage Relationships

AP009 Manage Service Agreements

AP010 Manage Suppliers

AP011 Manage Quality

AP012 Manage Risk

AP013 Manage Security

Build, Acquire and Implement

BAI01 Manage Programmes and Projects

BAI02 Manage Requirements Definition

BAI03 Manage Solutions Identification and Build

BAI04 Manage Availability and Capacity

BAI05 Manage Organisational Change Enablement

BAI06 Manage Changes

BAI07 Manage Change Acceptance and Transitioning

BAI08 Manage Knowledge

BAI09 Manage Assets

BAI10 Manage Configuration

Deliver, Service and Support

DSS01 Manage Operations

DSS02 Manage Service Requests and Incidents

DSS03 Manage Problems

DSS04 Manage Continuity

DSS05 Manage Security Services

DSS06 Manage Business Process Controls

Monitor, Evaluate and Assess

MEA01 Monitor, Evaluate and Assess Performance and Conformance

MEA02 Monitor, Evaluate and Assess the System of Internal Control

MEA03 Monitor, Evaluate and Assess Compliance With External Requirements

Processes for Management of Enterprise IT

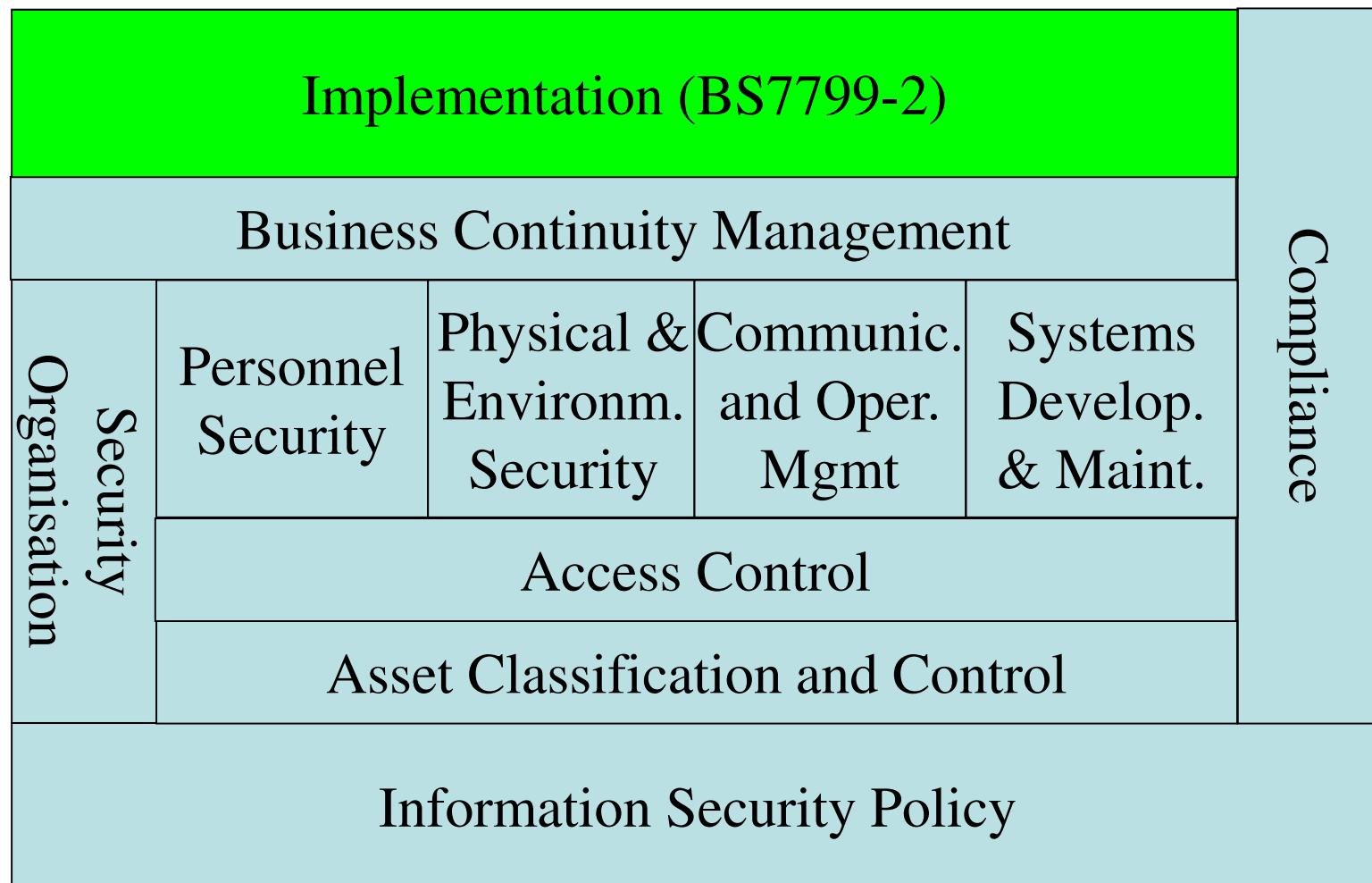
Source: COBIT® 5, figure 16. © 2012 ISACA®

BS 7799 / ISO 17799

- 1993: Code of Practice (UK DTI)
- 1995: BS 7799
- 1998: BS 7799 Part 2 (ISMS)
- 1999: Revision BS 7799 Parts 1 + 2
- 2000: ISO 17799 = BS7799 Part 1
- 2002: Adaptation of BS 7799-2 to ISO 9000

- ISO 17799:2000 = Code of Practice
- BS 7799-2:2002 = Basis for formal certification

Structure of ISO 17799



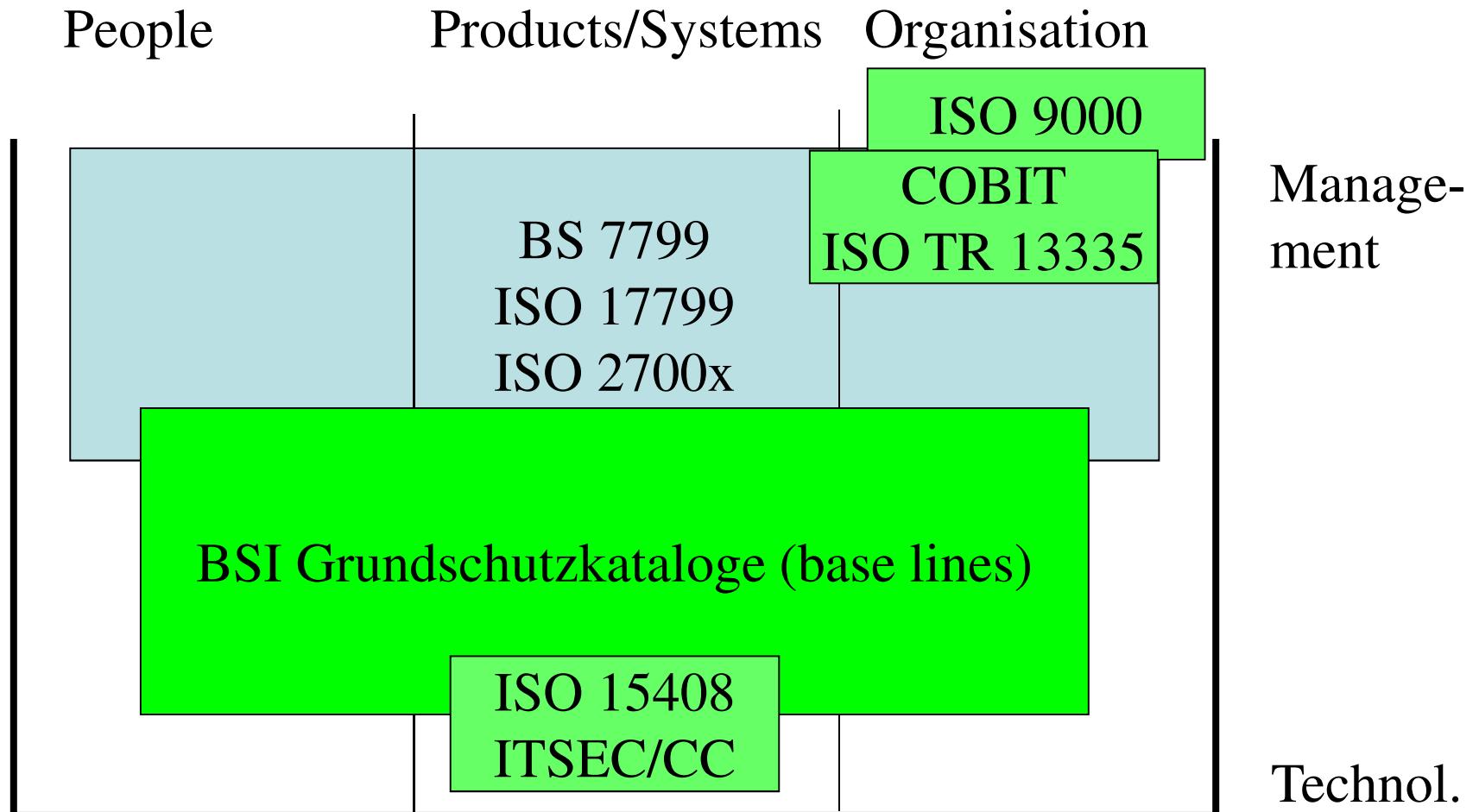


ISO 2700x Series

The new overall standard for „Information technology – Security techniques – Information security management system – Requirements, ISO 27000”, was published by ISO/IEC in 2005, replaces BS 7799-2. It forms the basis for a new ISO series of information security standards, including formal accreditation of certification authorities.

- ISO/IEC 27000: Basic Definitions (based on ISO 13335 MICTS part 1)
- ISO/IEC 27001: Requirements for an ISMS (based on BS 7799 part 2)
- ISO/IEC 27002: New name for ISO/IEC 17799
- ISO/IEC 27003: ISMS Implementation Guidelines (based on ISO 13335 MICTS part 1)
- ISO/IEC 27004: Metrics for Measuring Information Security and its Mgmt
- ISO/IEC 27005: ISMS Risk Mgmt (based on ISO 13335 MICTS part 2)
- ISO/IEC 27006: Instructions for an ISMS Accreditation of Certificate Authorities

Security Standards: Evaluation



Baseline Protection Model



BSI-Grundschutzhandbuch / GS-Kataloge

IT-Grundschutzhandbuch - Microsoft Internet Explorer provided by Computer Associates Int'l.

File Edit View Favorites Tools Help

Address https://www.bsi.bund.de/deutsch\menue.htm

BSI-Homepage

IT-Grundschutzhandbuch IT-Baseline Protection Manual IT-Grundschutz-Zertifikat

Aktuelles Kapitel des IT-GSHB

Bezugsquelle K 1 Wegweiser durch das IT-GSHB

FAQ K 2 Anwendung des IT-GSHB

Hotline K 3 Übergeordnete Komponenten

Hilfsmittel K 4 Infrastruktur

Inhaltsverzeichnis K 5 Nicht vernetzte Systeme

Index K 6 Vernetzte Systeme

Schichtenmodell K 7 Datenübertragungseinrichtung

Update Mai 2002 K 8 Telekommunikation

K 9 Sonstige IT-Komponenten

Massnahmenkataloge Gefährdungskataloge

M1 Infrastruktur G1 Höhere Gewalt

M2 Organisation G2 Organisat. Mängel

M3 Personal G3 Menschl. Fehlhandl.

M4 Hardware / Software G4 Techn. Versagen

M5 Kommunikation G5 Vorsätzl. Handlungen

M6 Notfallvorsorge

Avoids detailed analysis
Checklist-based
Certification through BSI (DE)

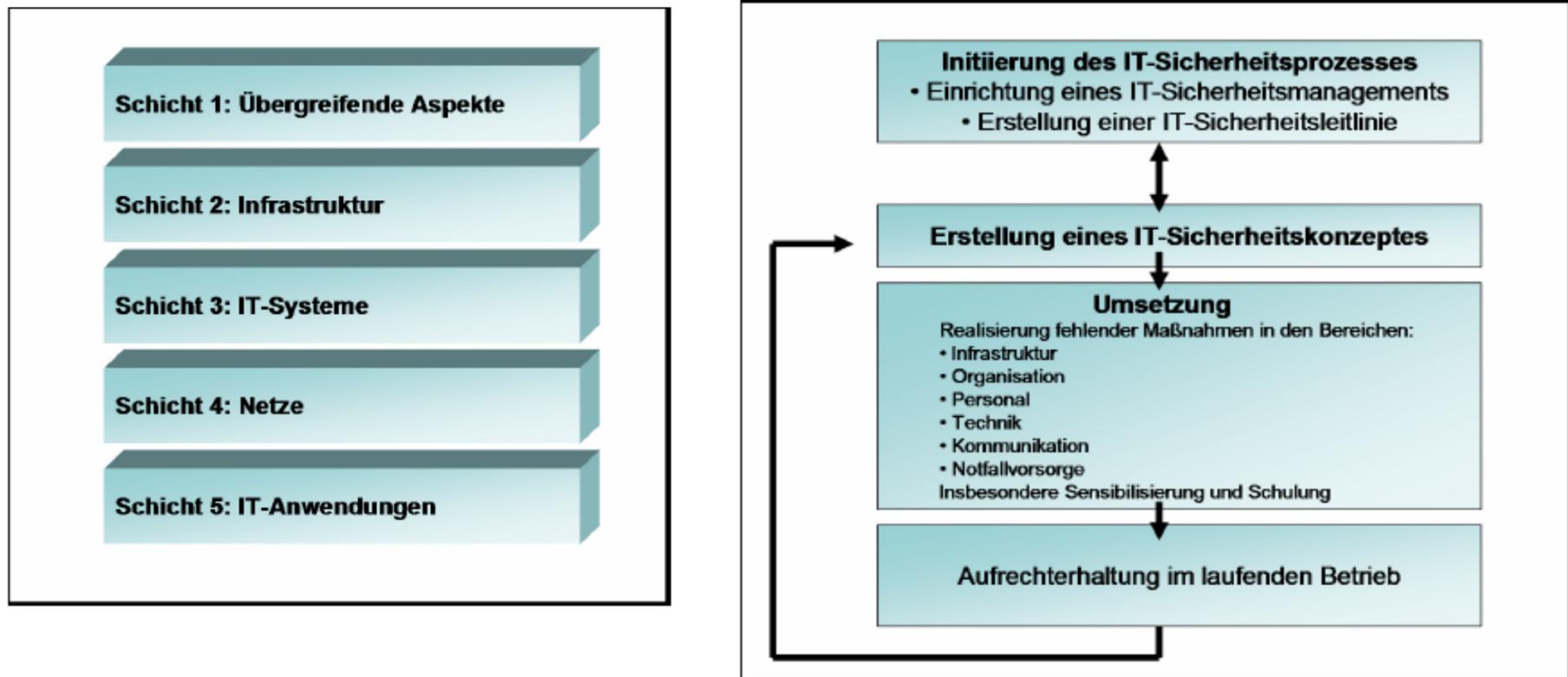
Navigator Inhaltsverzeichnis Index Ohne Frame

Hotline: gshb@bsi.bund.de Telefon: +49 (0) 1888 9582-369

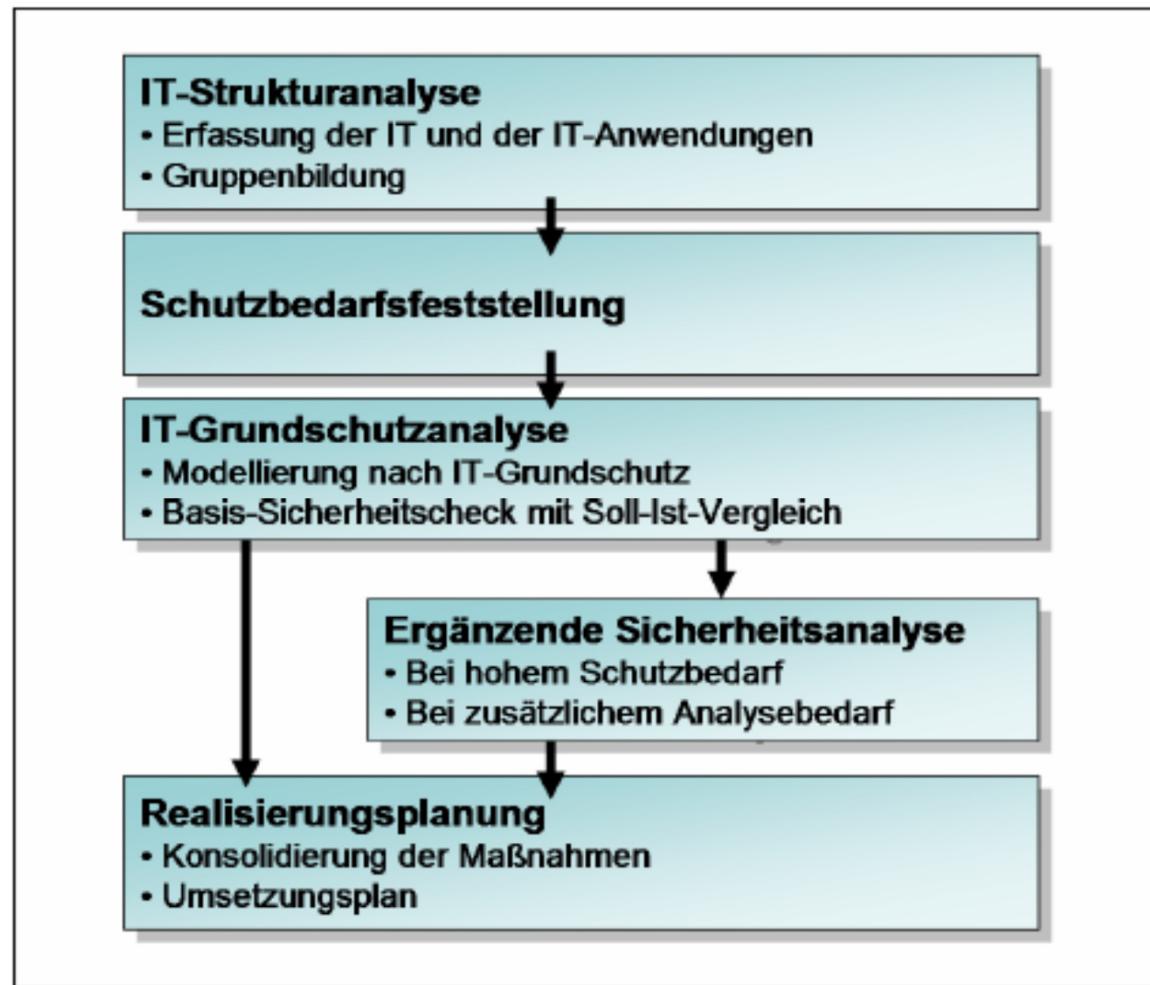
BSI-Homepage

My Computer

IT GSHB



IT GSHB





Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Best Practices



What is a “Best Practice”?

- Whatever fits the needs of a given organisation and situation.
- Is based on up-to-date information, standards, guidelines, and legal / regulatory requirements.
- Is process-oriented, repeatable and measurable.
- Should be both efficient and effective.
- Is transparent and adaptable to new situations.

Security “Best Practice” Examples

- Community collection of security “tips and tricks”,
e.g.:
 - <http://www.first.org/resources/guides/>
 - <http://www.switch.ch/de/cert/info/links.html>
- Vendor information on securing products, e.g.:
 - <http://www.hp.com/security/>
 - <http://www.redbooks.ibm.com/> → search for security
- Consultant information (see their home pages)
- Web pages, white papers and books, e.g.:
 - <http://www.csoonline.com/> (CSO Magazine)
 - <http://www.oreilly.com/> → search for security

Summary – Take Home Message

- There is one nice thing about standards: there are so many to chose from.
- ISO 2700x becomes the new, widely accepted series of security base standards.
- COBIT is a good extension to ISO 2700x with respect to security processes, and auditability.
- The BSI baseline concept (with or without formal certification) can complement ISO 2700x/COBIT.
- Best practices (in various domains) can be useful extensions of a formal security management system.

Introduction to the Lecture Project

Risk and Security Management – HS 2012

Detecon Consulting



Structure of an IT Security Architecture

Risk and Security Management – HS 2012

PD Dr. Hannes P. Lubich



Motivation



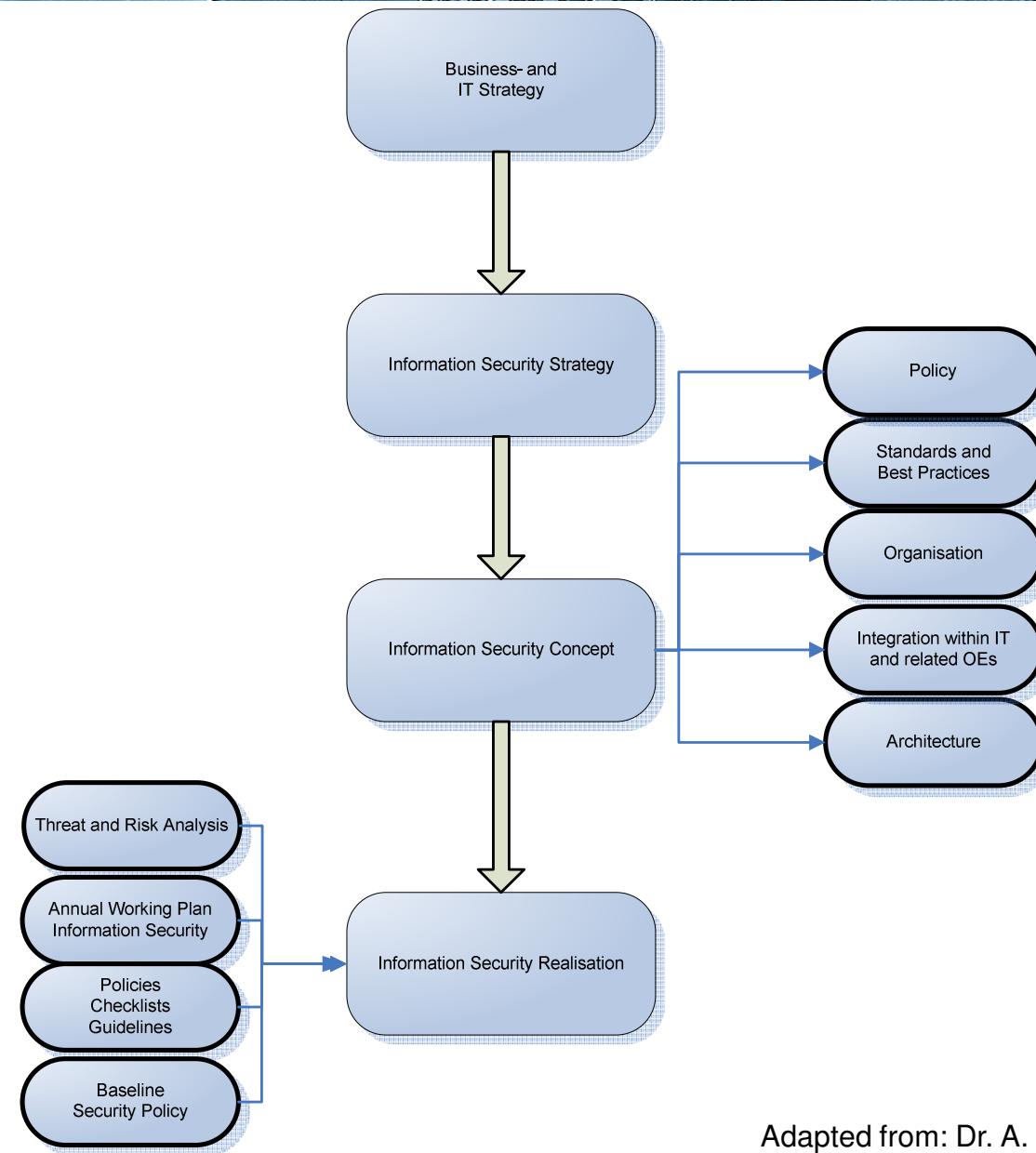
Outline

- A Layered Model of Security
- Architectural Elements of Security
 - Identity and Access Management
 - Threat Management
 - Security Information Management
- Interaction with other ICT Architectures

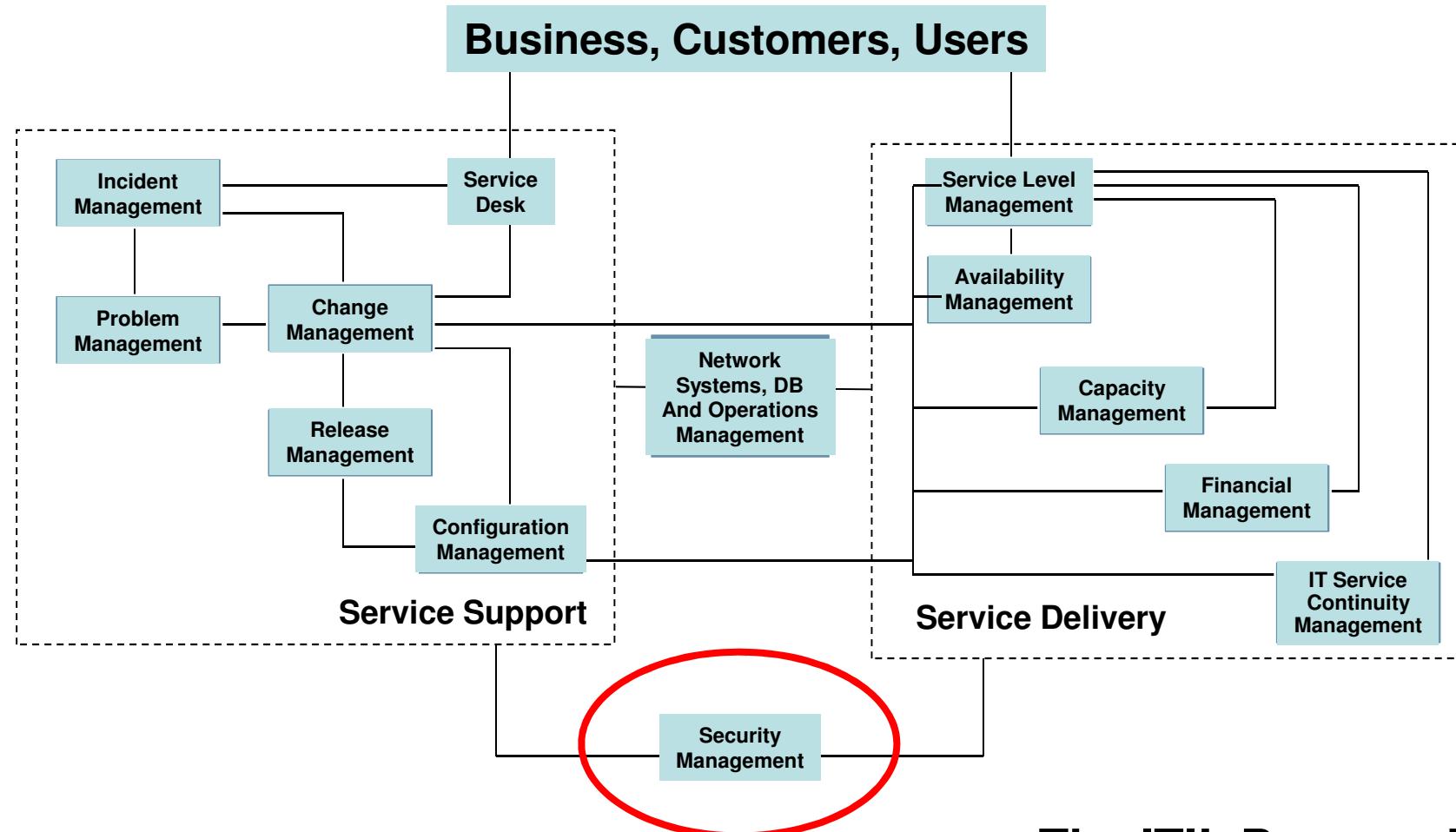
A Layered Model of Security



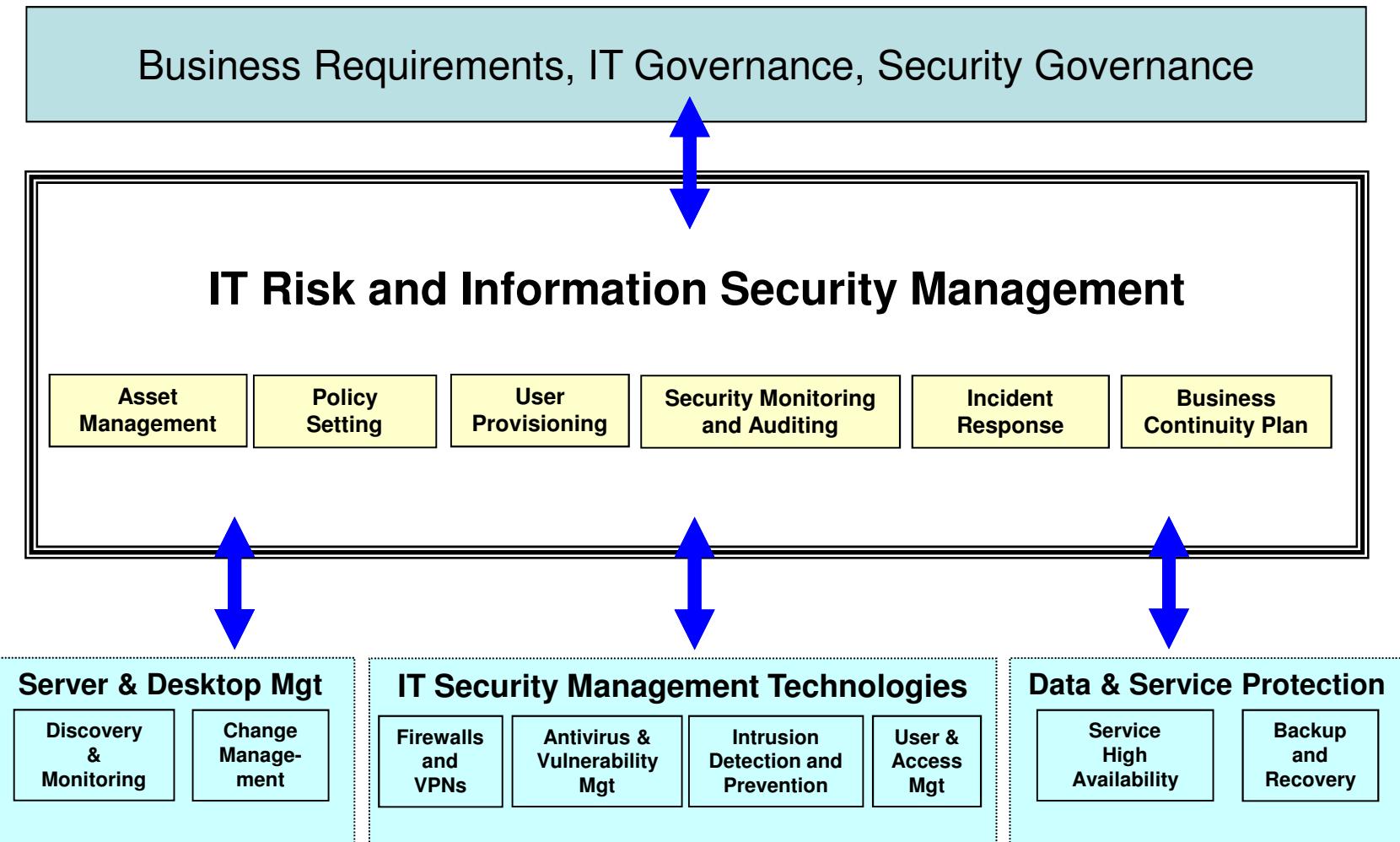
Overall Security Roadmap



Security is Part of Every IT Process

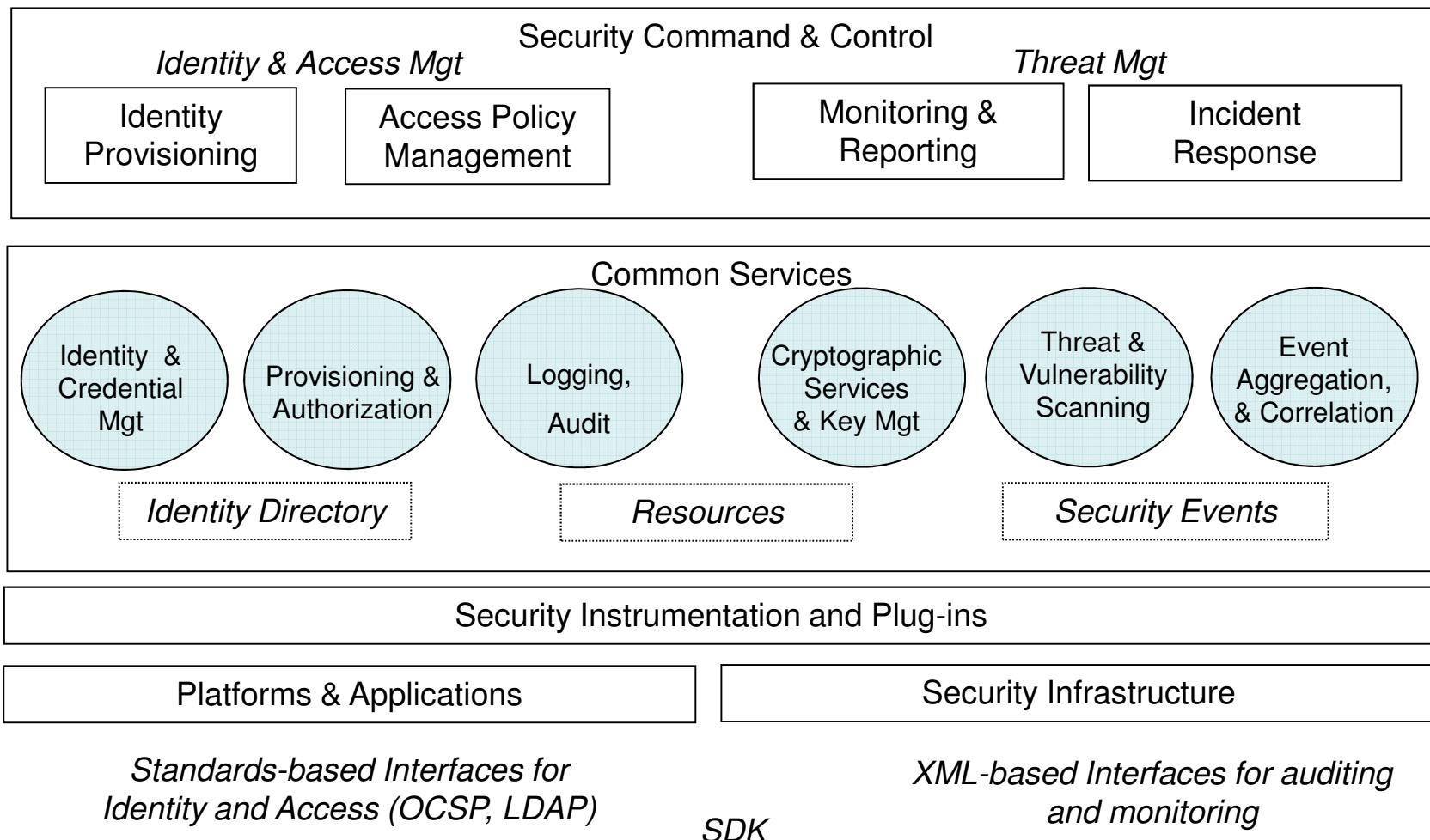


Overall Security Architecture

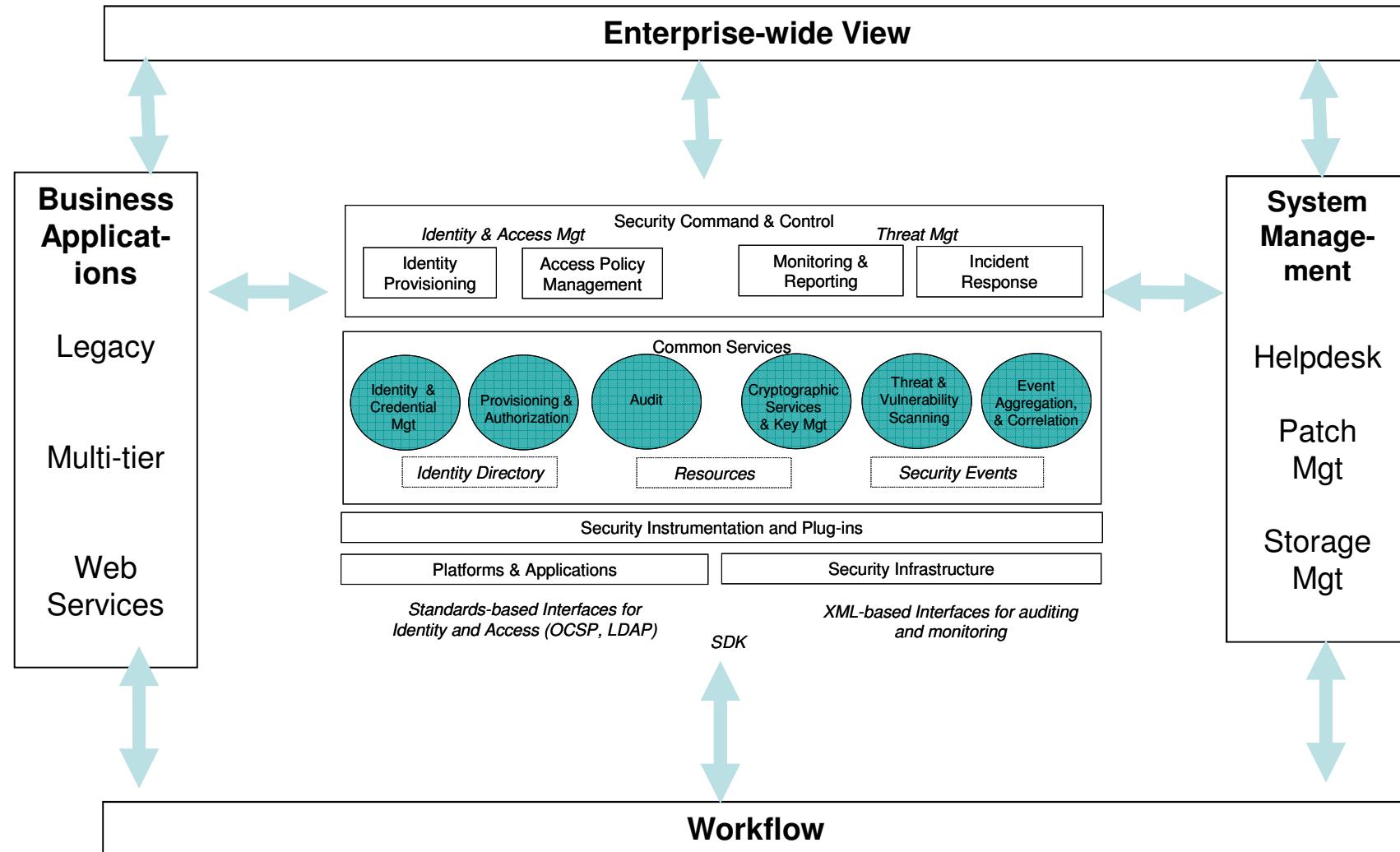


© Computer Associates

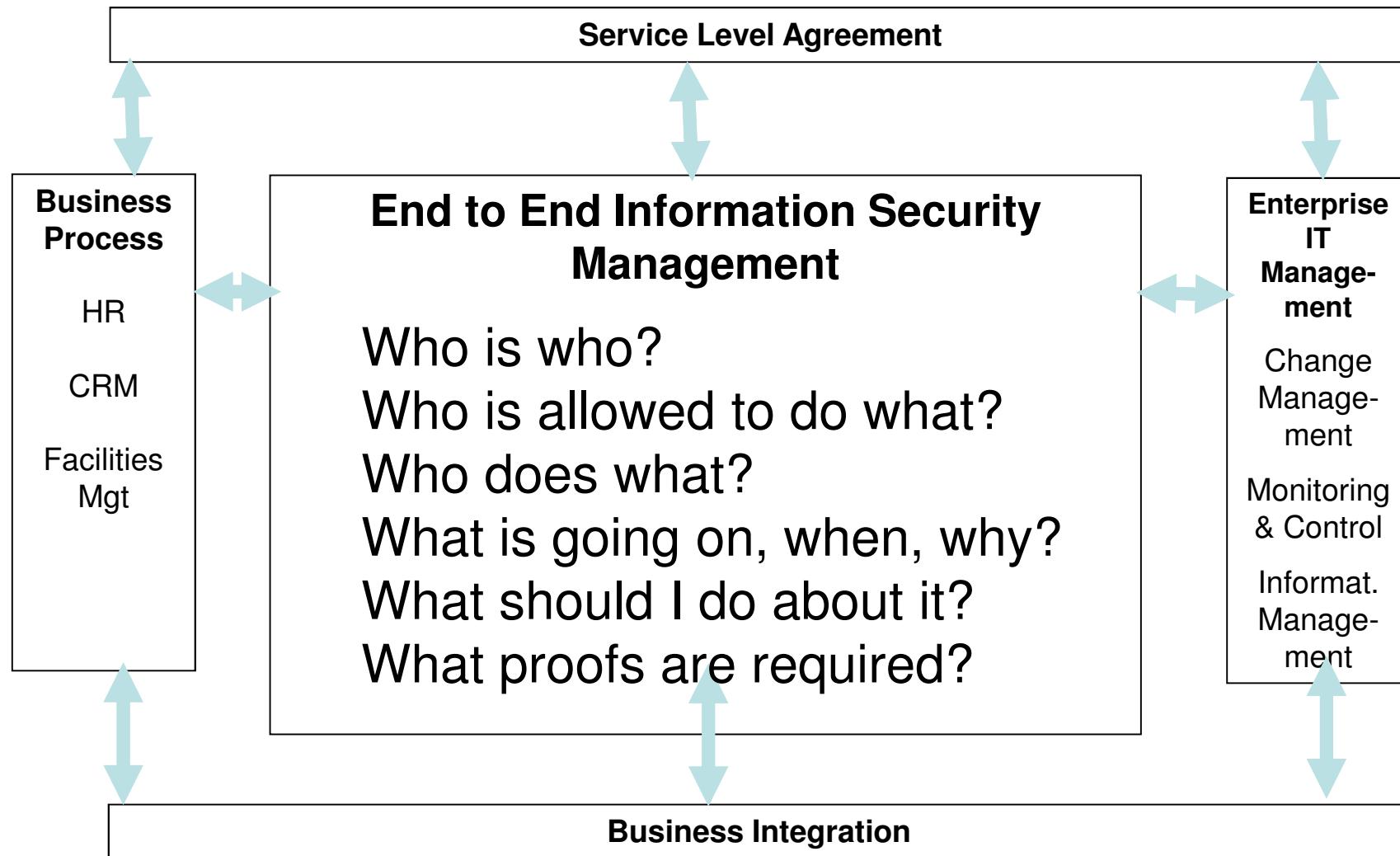
Security Architecture Modules



Integration into the Environment



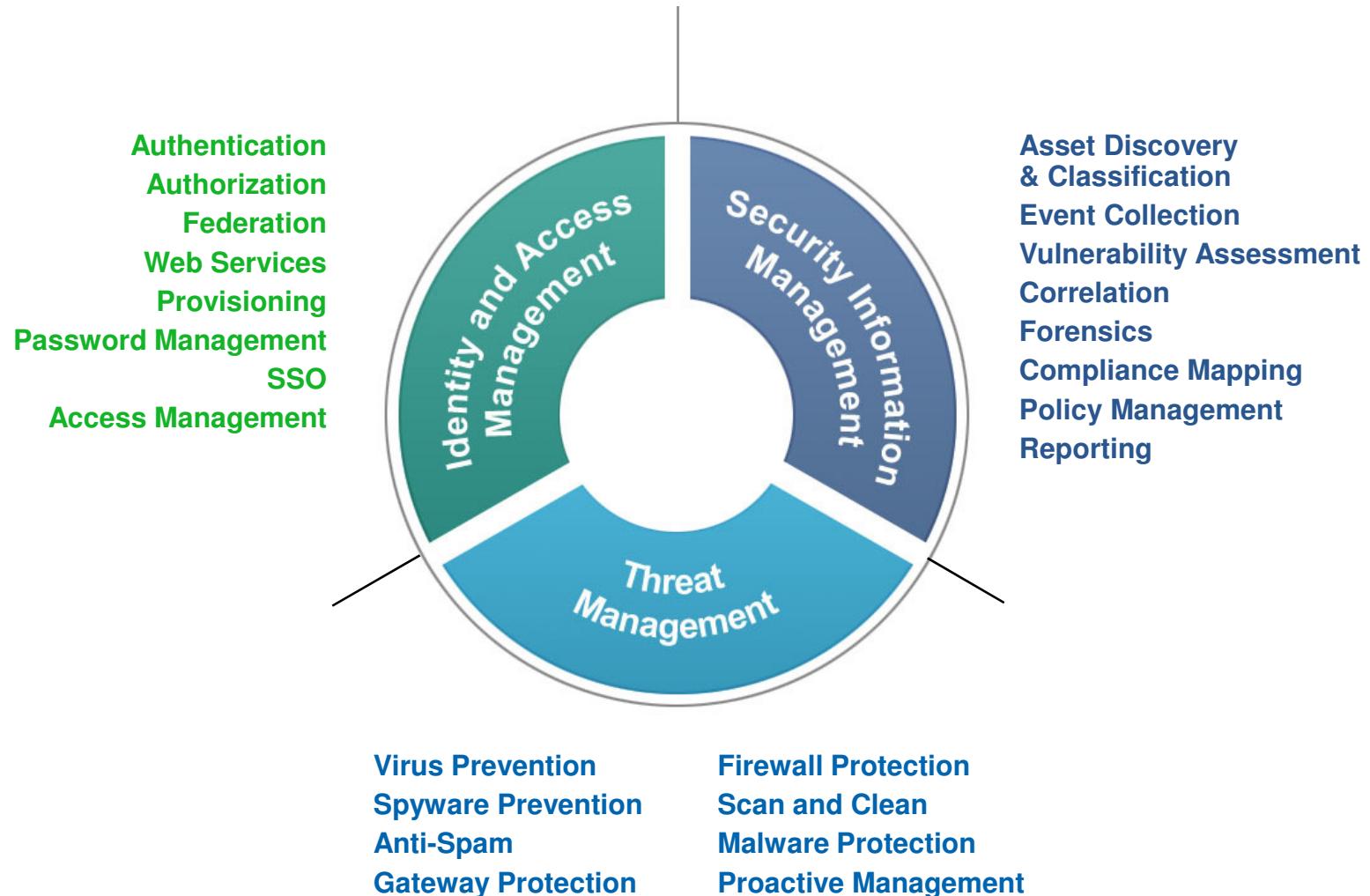
Integration into Business Applications



Architectural Elements of Security



Security Architecture Components

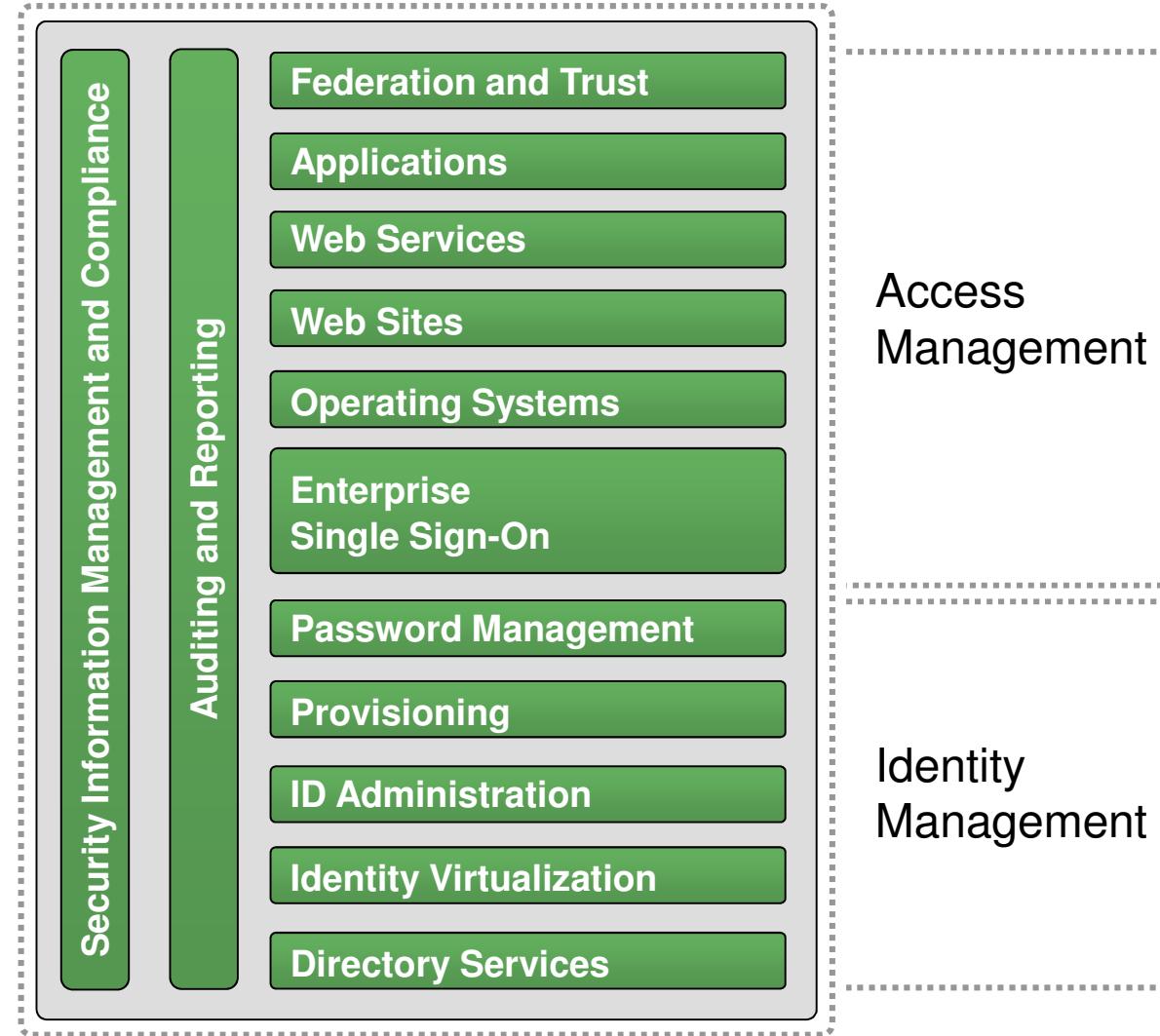


© Computer Associates

Pause

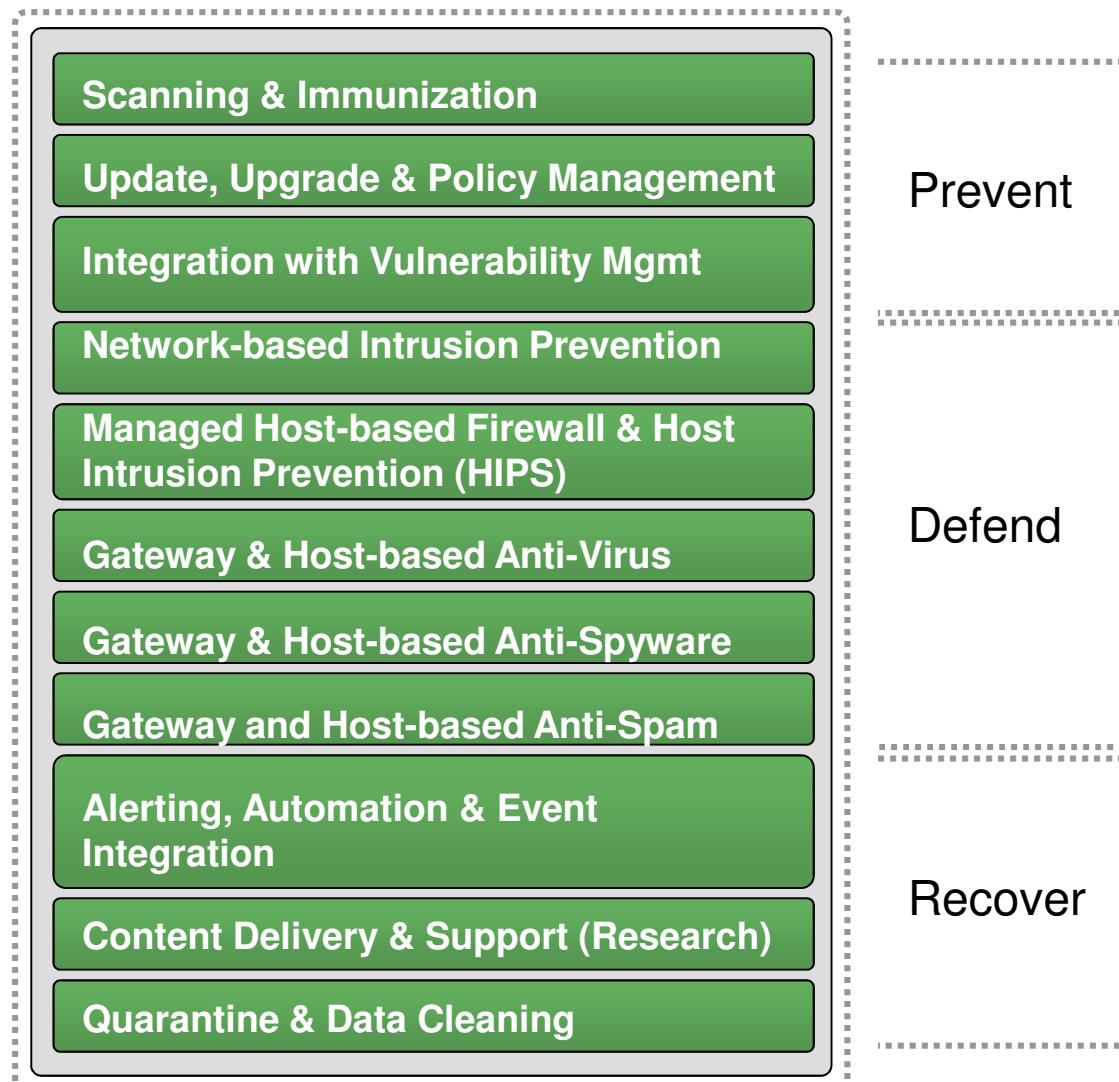


Identity and Access Mgmt Components



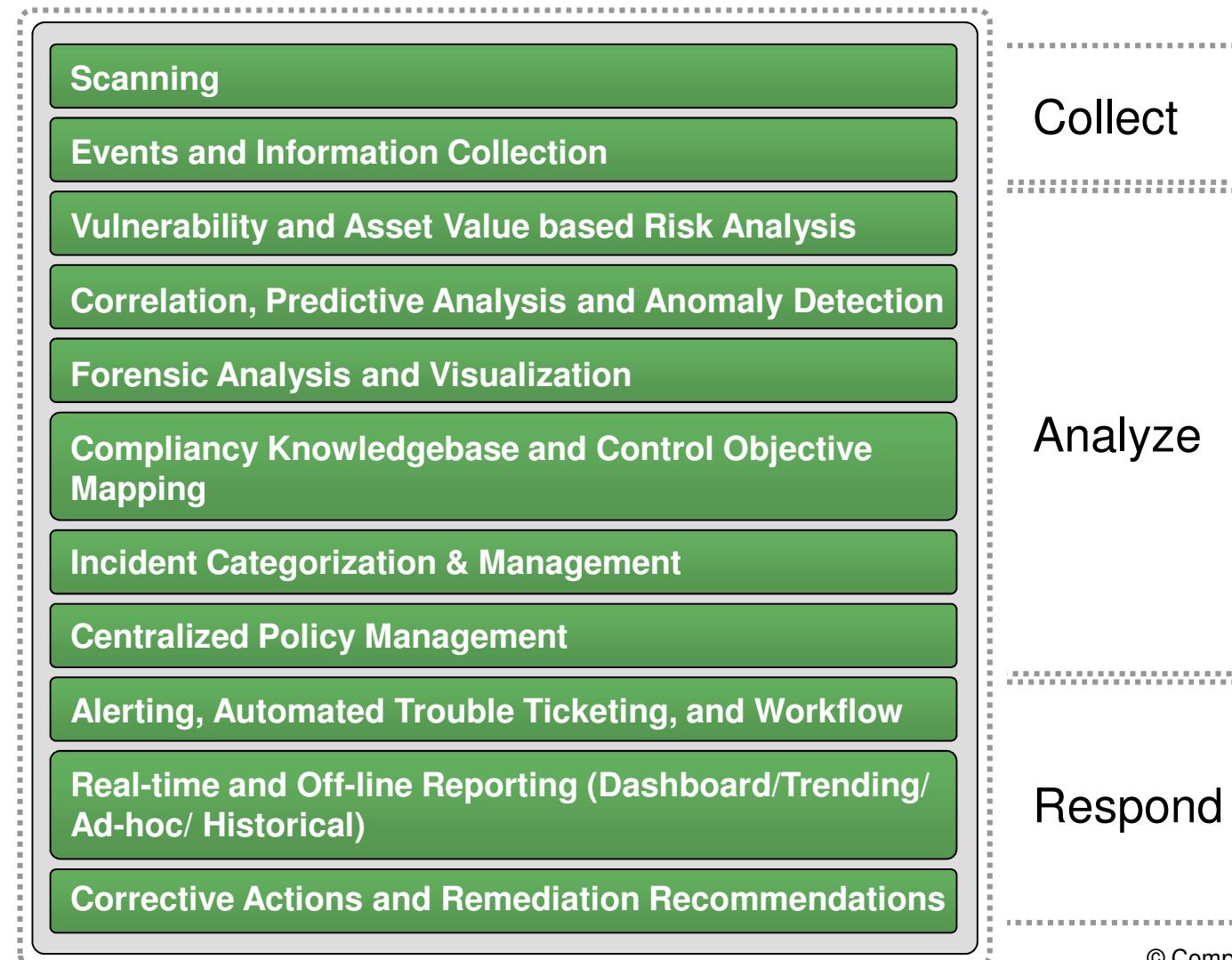
© Computer Associates

Threat Management Components



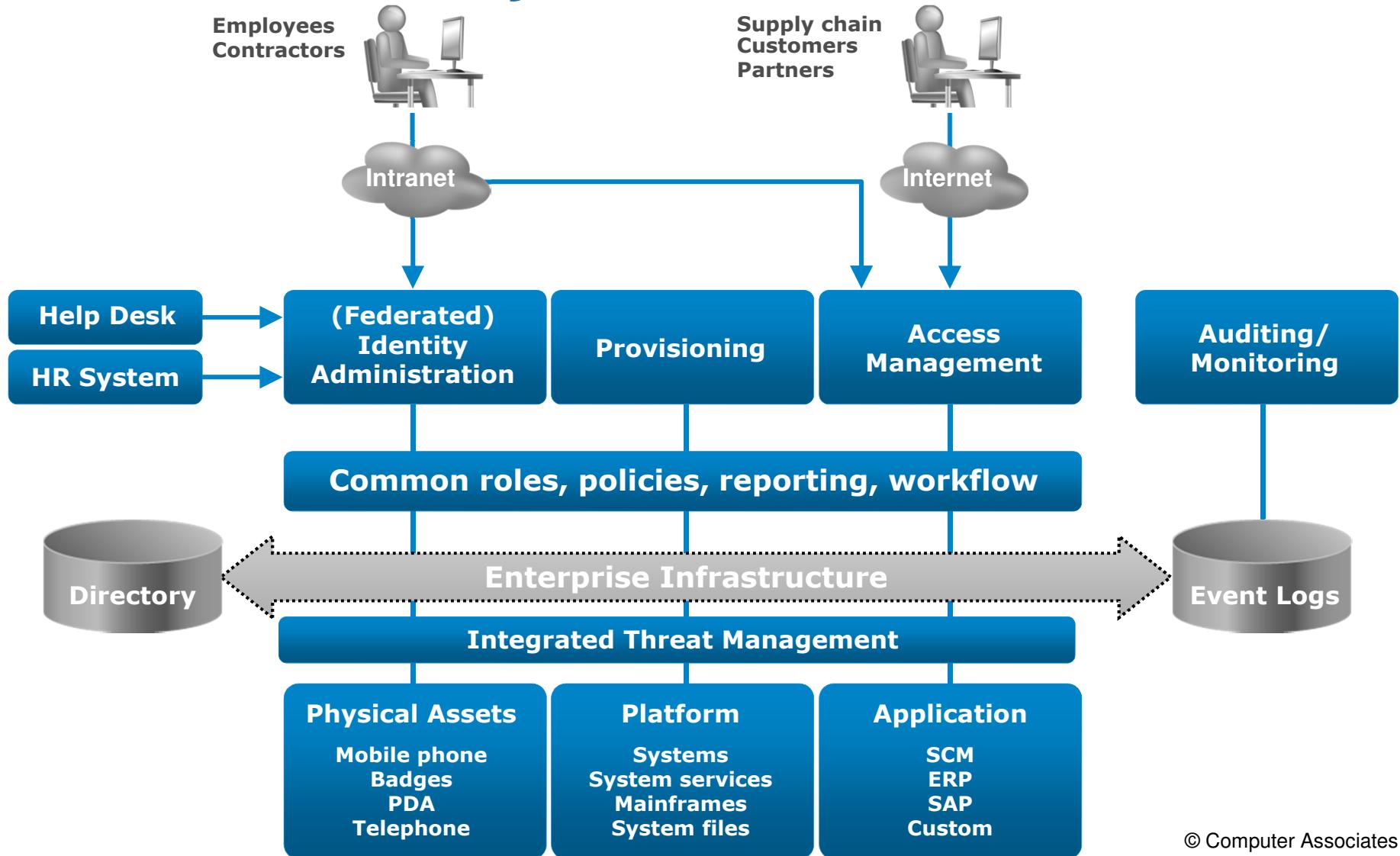
© Computer Associates

Security Information Mgmt Components



© Computer Associates

Overall Security Architecture



© Computer Associates

Interaction with other ICT Architectures



IT Architecture Building Blocks

- Hardware/Firmware
- **Operating Systems**
- **Networks**
- **Middleware Components**
- **Storage & Databases**
- **Information**
- **Applications**
- Integration
- User Interfaces
- **Development Environments**
- **Systems/Networks/Services Management**

Applications, Middleware, Databases

- Definition of a „secure enough“ base configuration
- Definition of process to harden the application (patches, configuration changes etc)
- Integration into surrounding security concept (ports, roles, rights, updates, monitoring etc)
- Security process for further development, maintenance and testing (esp. with third parties)
- Regular auditing of status, risks, activities etc.

Networks and Interfaces

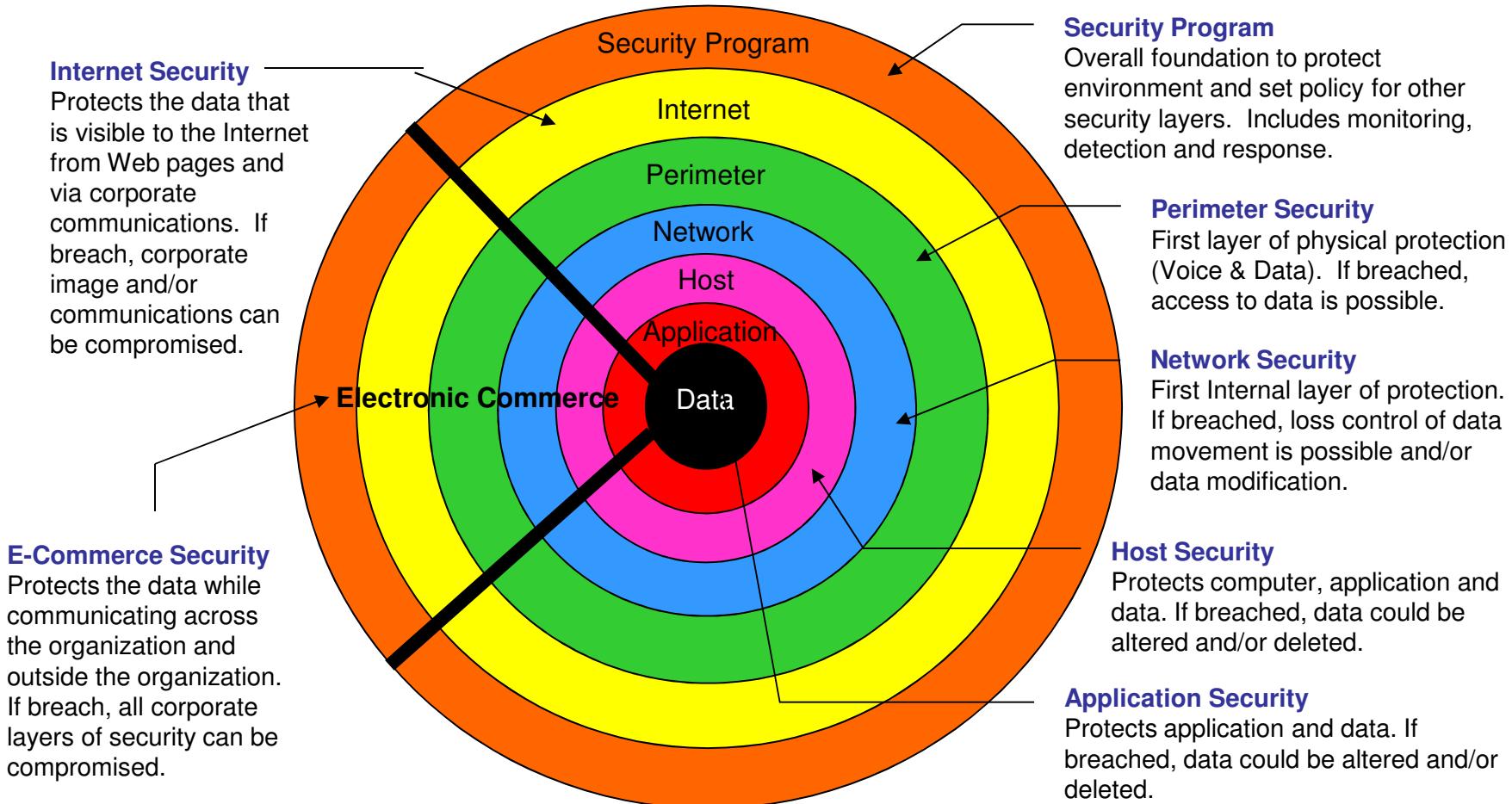
- Protection of physical / logical network access points
- Concept for secure wireless networks
- Self-protection of network (admission control, behaviour-based, NIDS, ...)
- Transition point protection (firewalls, packet inspection etc)
- Identification / Authentication of all network-based access
- Security concept for all external connectivity (e.g. vendors, maintenance), data feeds etc.
- Detection of attacks (from inside / outside) and automated countermeasures
- Embedding into IT asset mgmt and network management
- Regular reviews / audits of relevant log information

Systems and Platforms

- Definition of a „secure enough“ base configuration (including peripheral interfaces)
- Definition of process to harden the system / platform (patches, configuration changes etc), provision of system compartments where necessary
- Malware protection (local, and gateway-based)
- Host-based intrusion detection / prevention, if necessary
- Integration into IT asset management, systems and services management, change management
- Definition of local access rights, users etc., integration with directory services, SSO etc.
- Monitoring, reviews and audits
- Cleaning of systems before external use / return to vendor

Enterprise End-to-End Security

Corporate information protection is based on a multi-layered approach. The structure limits the exposure of any one security breach, however today, the Internet cuts across traditional layers and an unauthorized user could quickly exploit a weak layer.



Concept Jericho – Can we Drop Firewalls?

- Open Group concept Jericho:
 - Perimeter protection via firewalls is futile – too many applications and tunnels go trans-border already.
 - Strict authentication of communication partners
 - Strict segmentation within network
 - Well-defined, secured (encrypted) end-to-end communication channels
- Counter arguments:
 - Too complex / error-prone to administer
 - Firewalls are part of the overall security concept – nobody claims that they are perfect
- See: <https://collaboration.opengroup.org/jericho/>

Summary – Take Home Message

- An IT security architecture must be part of a larger IT security concept.
- Important elements of an IT security architecture are identity and access management, threat management, and security information mgmt.
- IT security also defines requirements for other elements of the overall IT architecture.
- IT security architectures support business risk mgmt.

Architecture Components – Identity and Access Management

Risk and Security Management – HS 2012

PD Dr. Hannes P. Lubich



Motivation



Identity Management Drivers

Business to Business

- Business transactions via web services
- Small # of users
- High # transactions
- Extremely high \$\$ value

of Users

B2C

Revenue

Enterprise

of Transactions

of Applications

Business to Customers

- Connecting customer to web apps
- Very high # of users
- Few applications
- High revenue potential

Enterprise Business

- Connecting users to applications
- Medium to large # users
- Many applications
- Productivity vs. revenue

IAM Challenges

	Drivers	Identity Problem	Access Problem
Enterprise Business	Connecting users to corporate applications	Too many platforms Who are my users? Manage passwords Manage identities	Manage User privilege Too many apps & hosts to manage Role Separation Regulatory Compliance What did they do? Who assigned the roles?
Business to Consumer	Connecting customers to web applications	Customer acquisition Scale Performance Reliability	Customer acquisition Web SSO Customer Information Privacy Server Hacking Prevention Regulatory Compliance
Business to Business	Connecting businesses through web services	Privacy Trust Accountability Certification	Access control enforcement of business layer agreements Content Access Entitlement Service Agreements

Outline

- What is an Identity?
- Provisioning
- Directories and Directory Services
- Single Sign-On
- Certificates and Public Key Infrastructures
- Access Control and Enforcement
- Case Study: SWITCHaai

What is an Identity?



Terminology and Basic Context

- **Identity**
 - Linking an actor to an evaluateable object though an attribute/value set
 - Valid within a defined context (country, company, ...)
 - Can be delegated to agents (third party, software, ...)
- **Building block of a security context for:**
 - Confidentiality
 - Integrity
 - Authenticity
 - Obligation

Identity-based Activities

- **Identification:** process of recognizing an entity based on the presented identification proof (attribute/value)
- **Authentication:** process of confirming that an entity is corresponding to the proposed identity, based on authentication information supplied by the sender
- **Authorisation:** process of providing or denying access to objects for a given entity
- **Provisioning:** process of allocating roles, access rights and resources to an identity

Requirement Analysis

- Legally binding, reproducible identification of an actor and its context exclusively for a pre-defined purpose
- Actor: person, software, third party, ...
- Context: private, employee, role (agent of authority)
- Purpose: internal / external, anonymous, protected, ...
- Legally binding: whole chain, end-to-end, individual step
- Reproducible: for whom?
- Usable in everyday life



Opportunities

- Legally binding, reproducible and protected process chains for B2B, B2C, P2P, G2C, ...
- Usage for everyone as a base technology / service
- Building block for more advanced business processes and usage models on a trustworthy basis

Risks

- Trustworthiness of all involved parties
 - Registration Authority
 - Certification Authority
 - Distribution- and Verification Path
 - Storage Method and Usage
- Interoperability
 - Technical: format, syntax, semantics
 - Organisational: timeframe, usage rules
 - Legal: acceptance, regulation, dispute settlement
- Misuse
 - Government: suppression, „Rasterfahndung“,
 - Business: unauthorised evaluation, transfer of information
 - Criminal: identity theft, blackmail
 - Societal: informational self-control / data protection / anonymity / pseudonymity versus „know your client“ requirements

Identity Management Architectures I

- **Centralised:** Provision of globally valid, unique identities.

Pro: central control/administration, common service model

Contra: too much central control, profiling/tracking is easy

Example: Microsoft Passport

- **Decentralised:** All participants define identities within their respective context(s)

Pro: simple realisation per application, distributed control over information and its dissemination by the owner, allows anonymity / pseudonymity, extensible

Contra: too many identities per user, potential loss of clearness of use/overview, danger of interoperability

Example: different ID's / passwords per supplier or personal identity manager (e.g. on a home PC, PDA or mobile phone)

Identity Management Architectures II

- **Federated:** no unique Identities, but network of linked identities

Pro: user retains control, no profiling possible, network can grow/shrink, market opportunity for identity service intermediaries

Contra: requires coordination / agreements on standards before service provision, inconsistencies between ID's possible, active role of user required

Example: Liberty Alliance „Circle of Trust“



Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

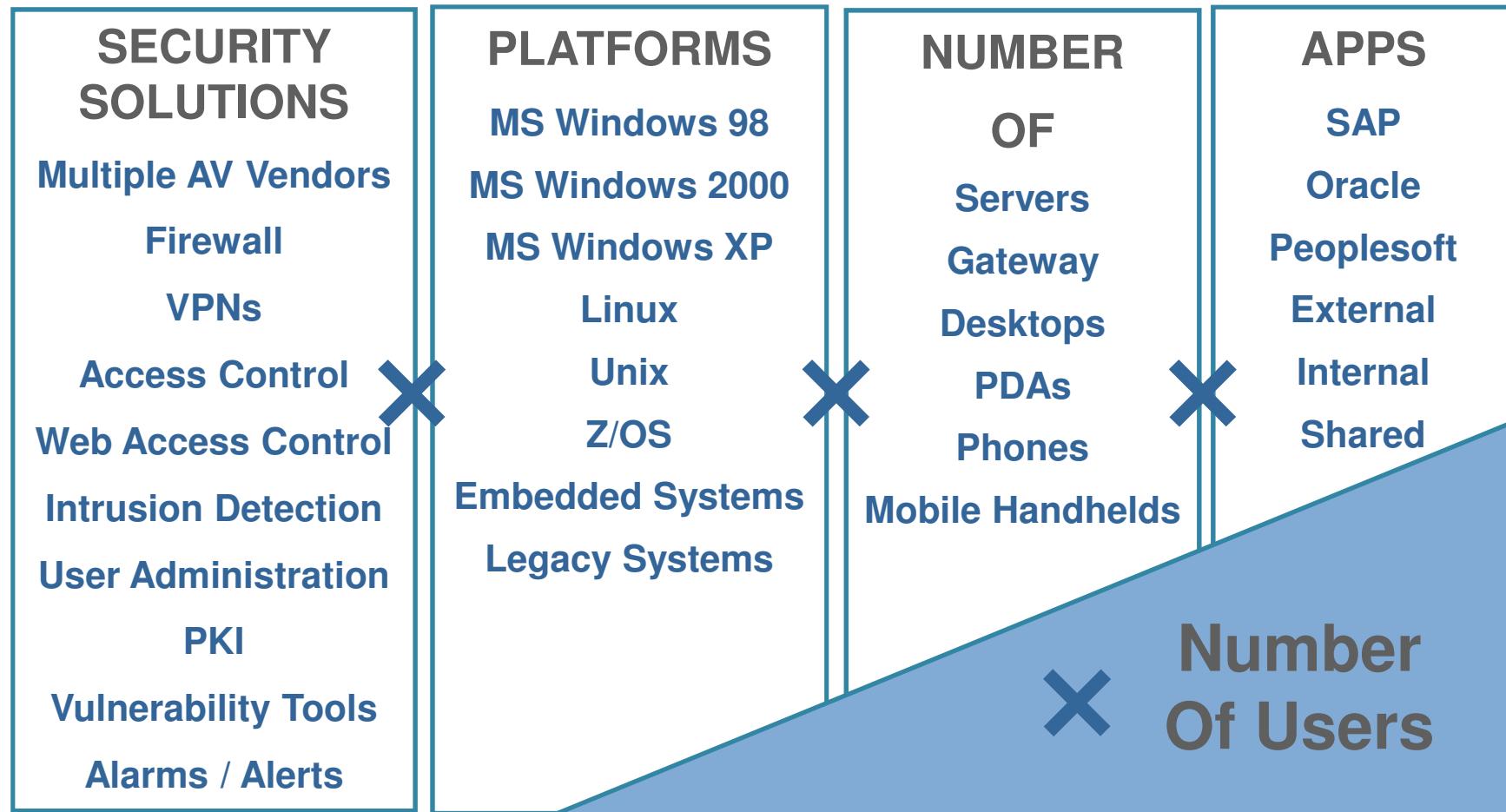
Provisioning



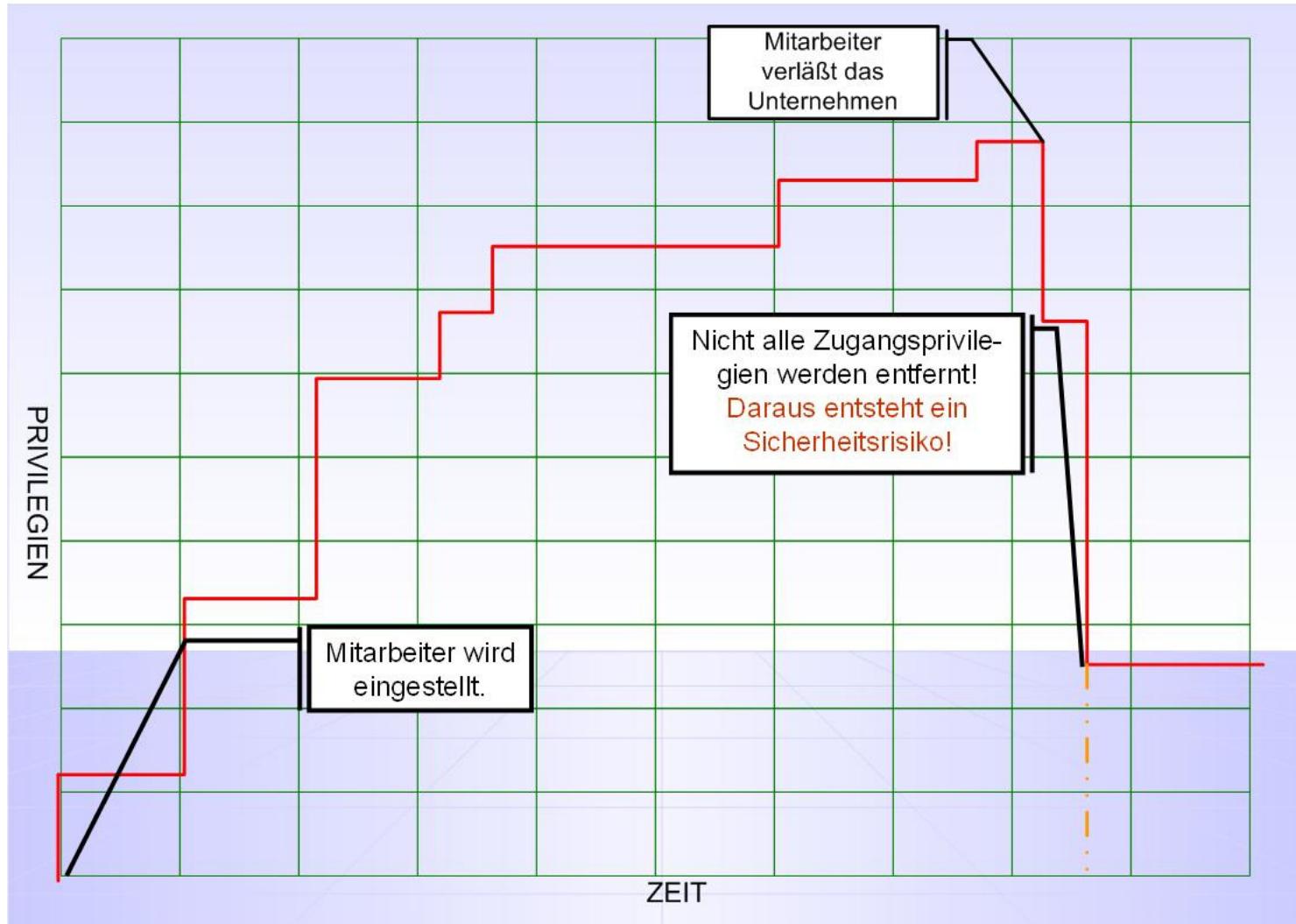
Provisioning Definition

- Provisioning is the automation of all processes and activities required for the administration (definition, modification, delegation, deletion etc.) of user or system access rights or related data pertaining to electronically controlled services (ranging from badge access to buildings to permission to modify data within an application or database).

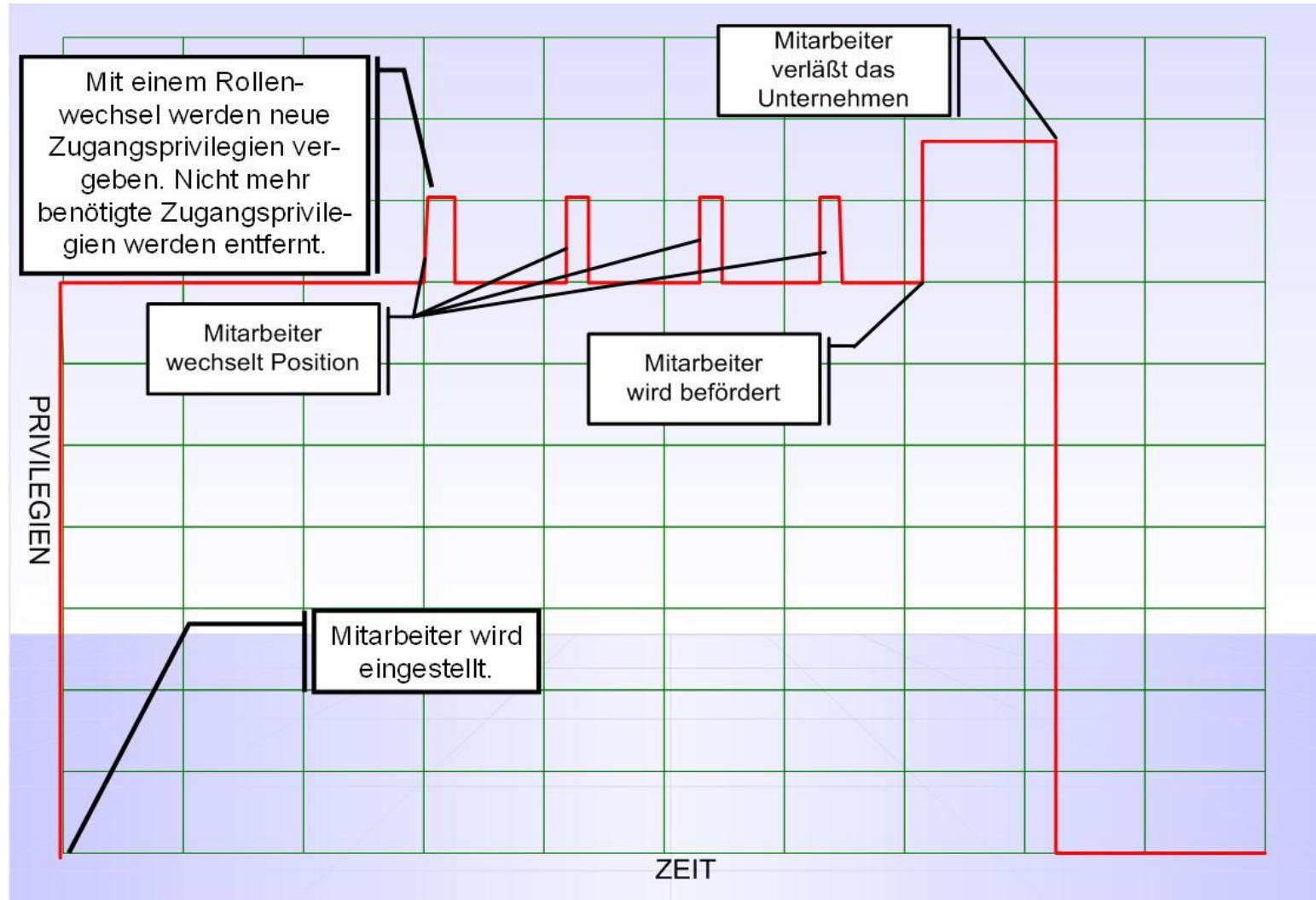
Dealing with large Numbers



Typical Provisioning Lifecycle



Optimised Provisioning Lifecycle



© Computer Associates

Pause



Directories and Directory Services



Identities Everywhere



HR Databases
SAP HR, SAP CO



O/S Directories
LDAP, ADS, NDS, UNIX



E-Mail Address Books
Lotus Notes, Exchange,
MEMO



Phone Directories
Nortel, Siemens,
Alcatel, Handy



Network Databases
NIS, DNS, DHCP, RADIUS



Database Applications
Oracle, DB2, SQL Server, SAP MM



**Access by Outsourcers,
Partners, Suppliers,
Service Providers**

Directory Services

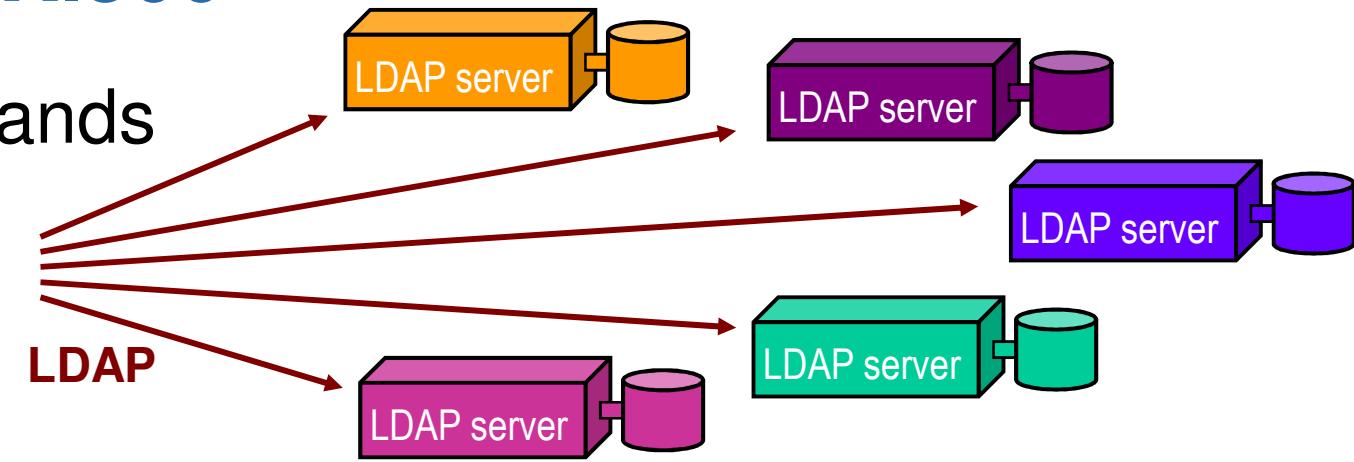
- A **directory** is a service providing a consistent way to name, describe, locate, manage and secure information about people, devices, systems and resources on a network.
- Directories provide many functions, including:
 - **Authentication**: validating users based on credentials
 - **Authorization**: checking entitlements to particular resources
 - **Publication**: searching and browsing for information
 - **Personalization**: storing user profiles and preferences
 - **PKI services**: managing X.509 certificates
- Directories are widely used for **identity management, security and administration**.

LDAP vs X.500

- LDAP Islands



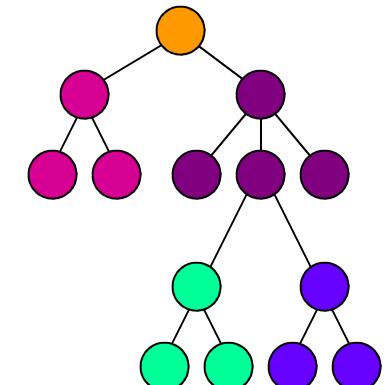
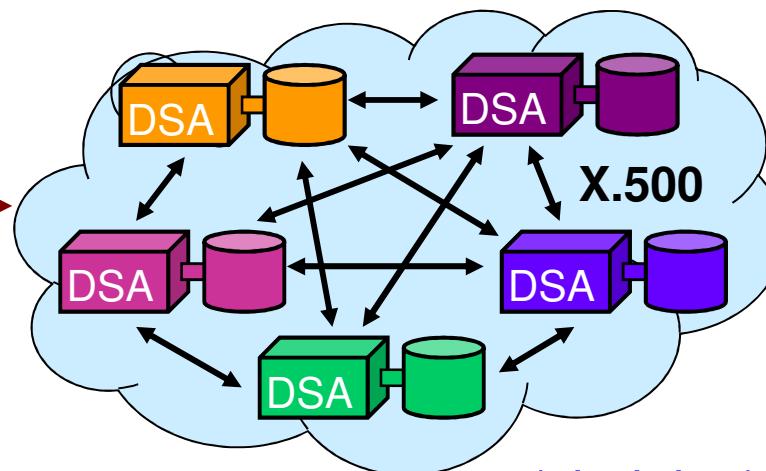
Client



- X.500 Backbone



LDAP
(DAP)
(DSML)

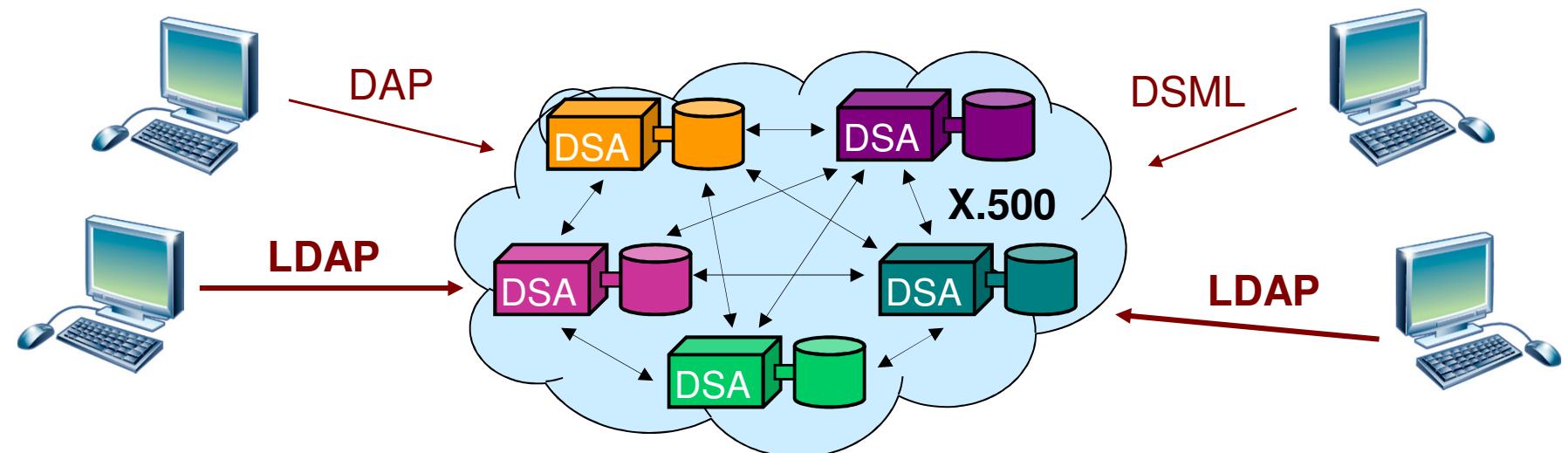


(chaining) server-server

© Computer Associates

LDAP vs X.500

- X.500 – international standard for directories
 - server → server communications
- LDAP – string based access protocol
 - client → server communications
- Almost all directories support both X.500 & LDAP



© Computer Associates

Integration Depth of Directories

- Use of a **common directory** service for different applications based on the same identification / authentication data.
- Use of a **meta-directory** service to synchronise information stored in different directories.
- Common **provisioning** in order to synchronise changes through several directory services.
- **Virtual directory** services that can combine information from several directories for one application.
- **Identity federation** as a dynamic process of transferring identity information between applications (e.g. in Web services).

Based on material by Kuppinger & Cole

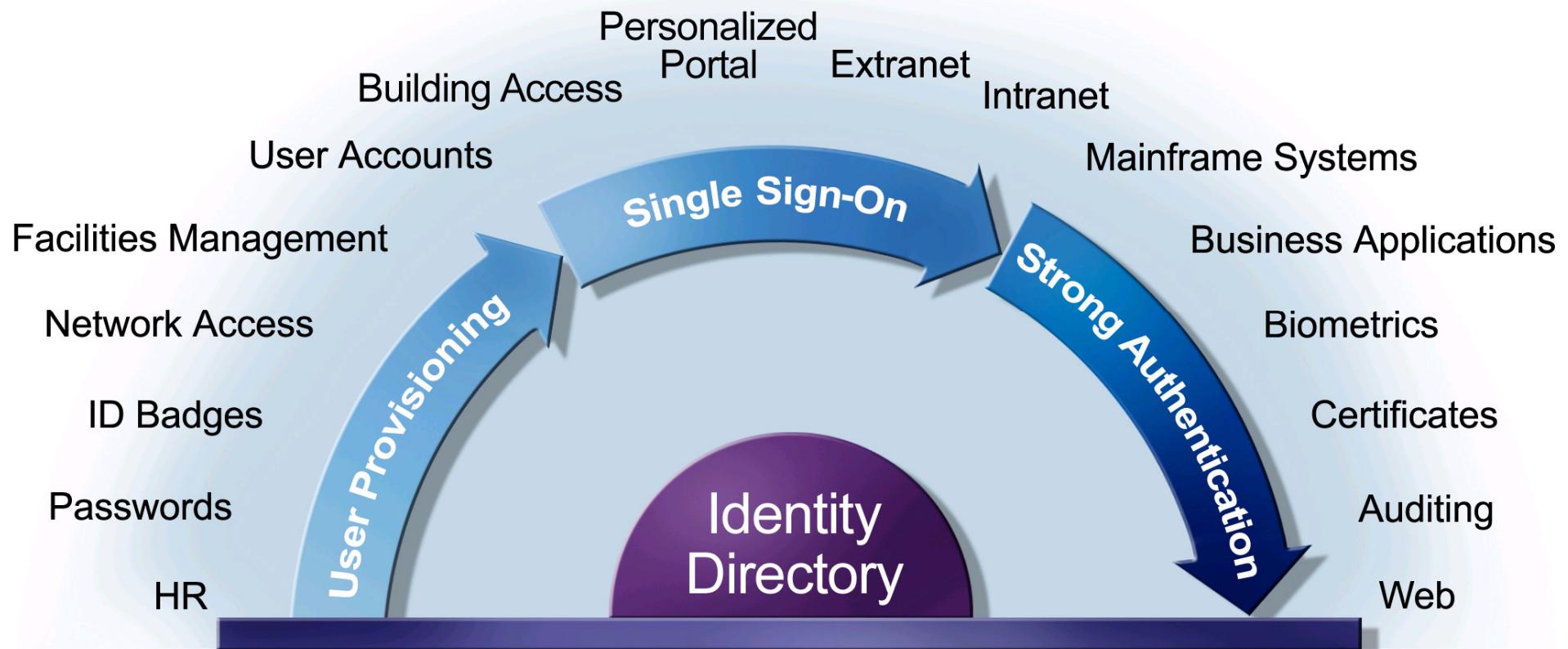


Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Single Sign-On



Single Sign-On Coverage



Single Sign-on Variants

- User-facing SSO: systems and applications still retain their individual IDs and credentials, but the user is able to control access via one “master” credential (e.g. passwords stored on a chip card)
- True SSO: ID, rights and role changes are automatically synchronised across all systems within the SSO domain
- Legacy Wrapping: strong identification and authentication around weak legacy systems

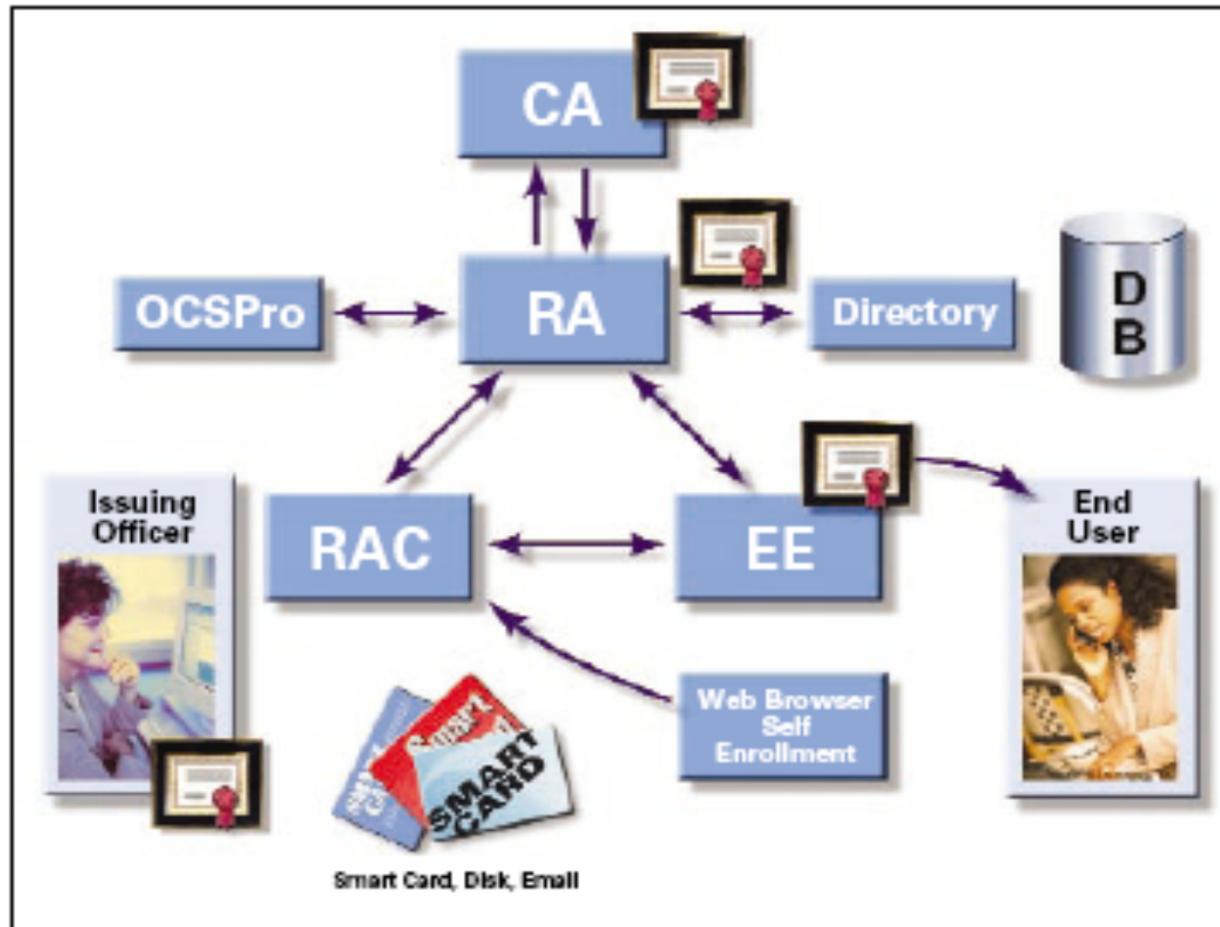
Certificates and Public Key Infrastructures



Definition

- A PKI enables users of a non-secured public network such as the Internet to securely and privately exchange information through the use of a public/private cryptographic key pair. The key pair or digital certificate based on the key pair is created, provided and shared through a trusted authority called a Certification Authority
- A PKI provides a digital certificate that can verify the identity of a user or an organization, and directory services that can store and, when necessary, revoke the certificates.
- A PKI may employ various Registration Authorities to provide secure and reliable primary identification of a user before issuing a certificate.

PKI Process and Core Functionality



RAC: Registration Authority Client
RA: Registration Authority
CA: Certification Authority
OCSP: Online Certificate Status Protocol
EE: End Entity

Access Control and Enforcement

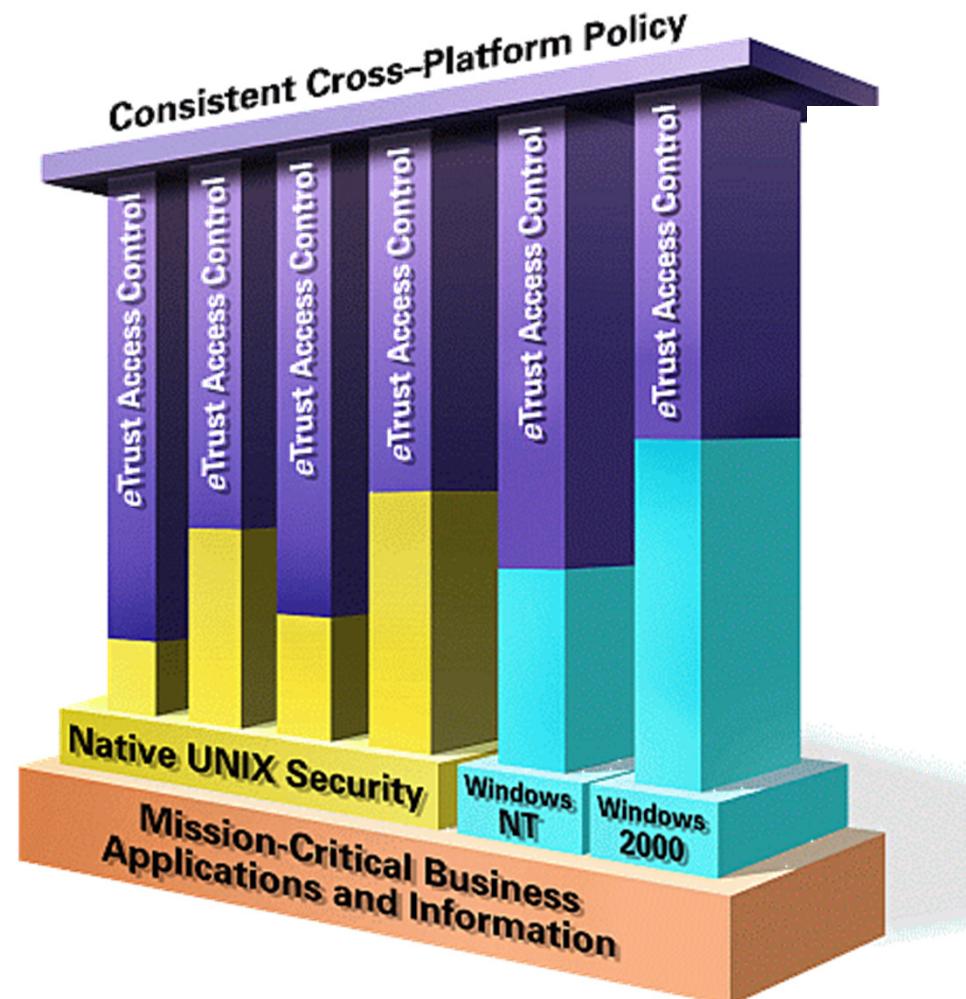


Access Enforcement Business Drivers

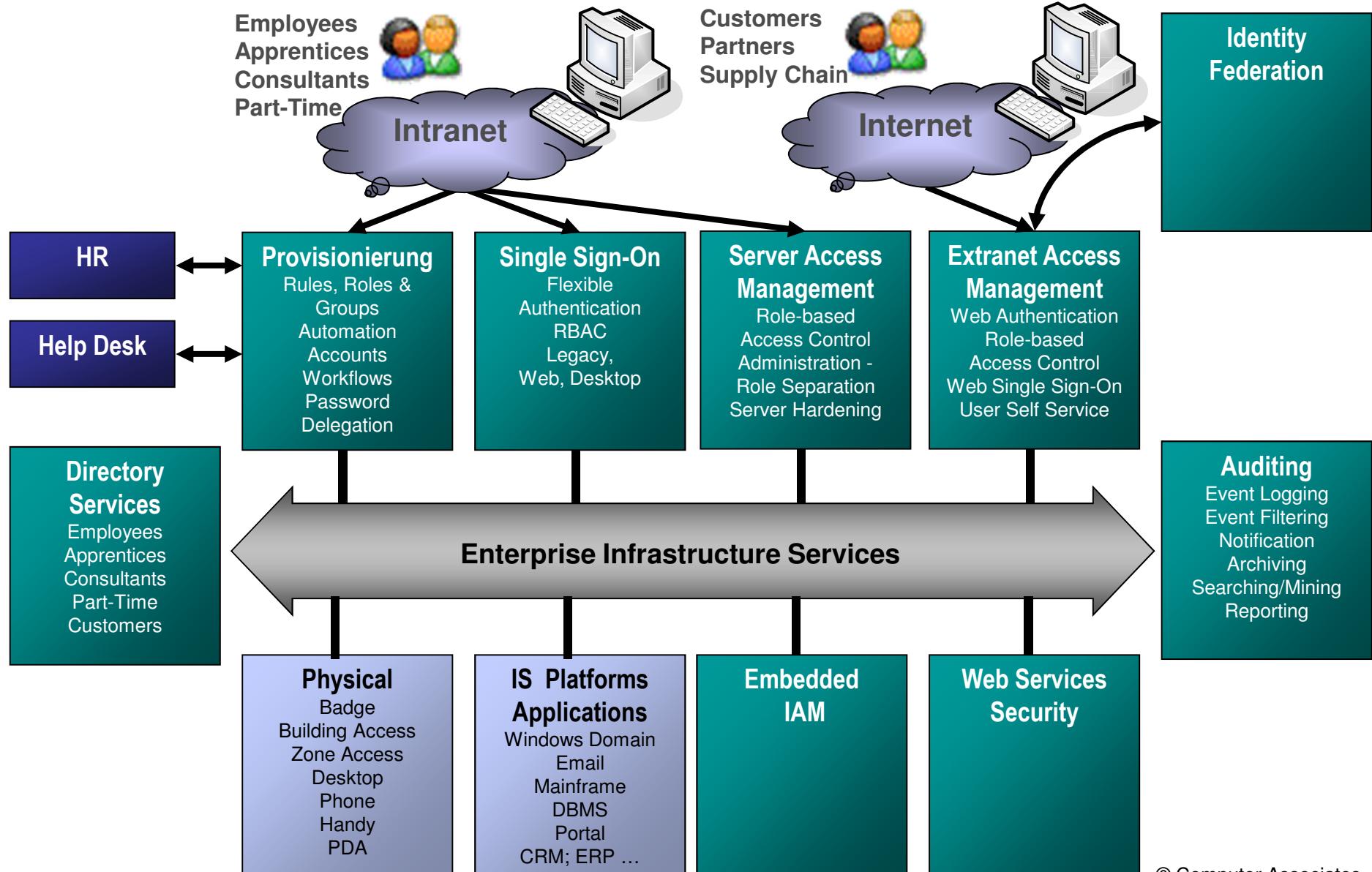
- **Regulatory Compliance and Policy Enforcement**
 - Industry and governmental regulations
 - Protect privacy & data Integrity
 - Proactive adoption of security measures
 - Internal auditing requirements
- **Risk Mitigation**
 - Enforce internal access policies
 - Eliminate redundant privileges to reduce risks
 - Track access usage
 - Protect assets (customer information and trust)
- **Business Continuity**
 - Ensure systems are not susceptible to hackers
 - Reduce impact of worms, prevent propagation
- **Operational Efficiencies**
 - Allow companies to do more with less
 - Eliminate access management inefficiencies
 - Reduce menial tasks – Reduce costs

Proprietary information theft resulted in the greatest financial loss (\$70,195,900 was lost among 530 surveyed companies, with the average reported loss being approximately \$2.7 million), which are mostly coming from internal unauthorized access. (CSI/FBI Reports)

Access Control Functional Elements



© Computer Associates

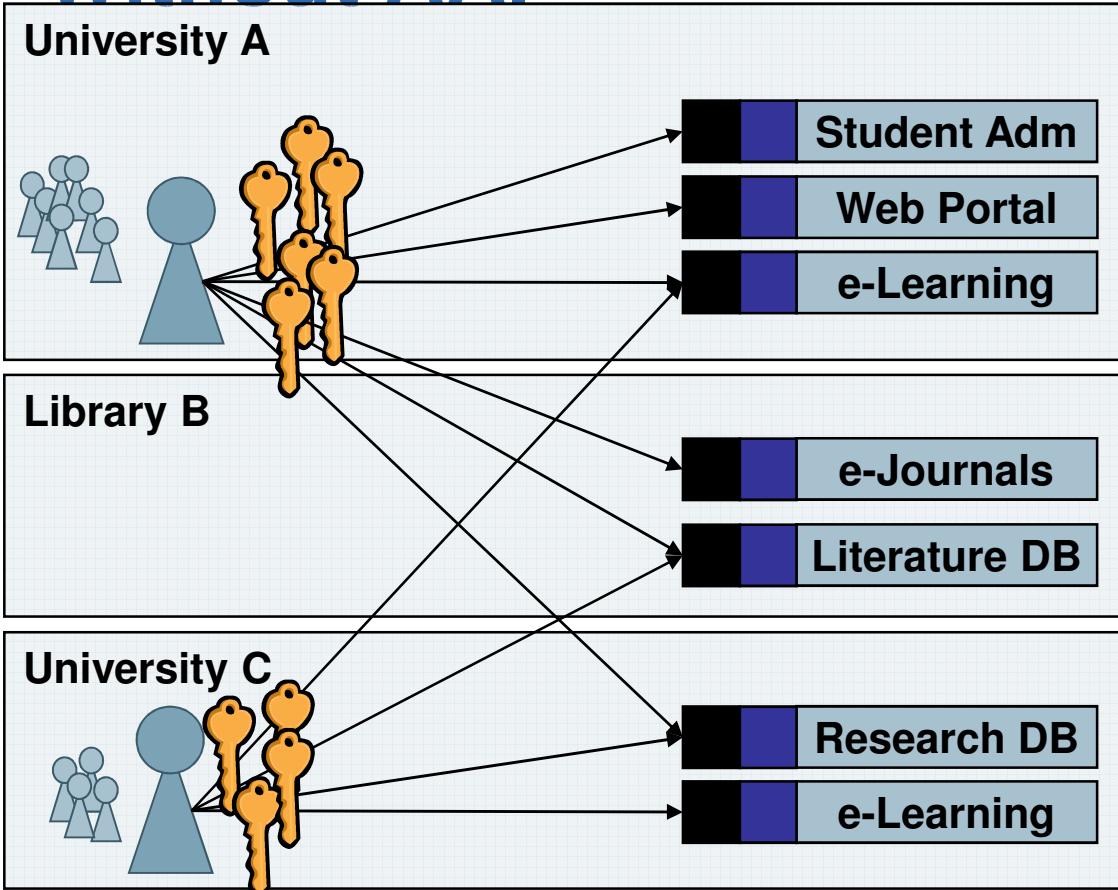


© Computer Associates

Case Study: SWITCHaai



Without AAI



- Tedious user registration at all resources
- Unreliable and outdated user data at resources
- Different login processes
- Many different passwords
- Many resources not protected due to difficulties
- Often IP-based authorization
- Costly implementation of inter-institutional access

User Administration
Authentication

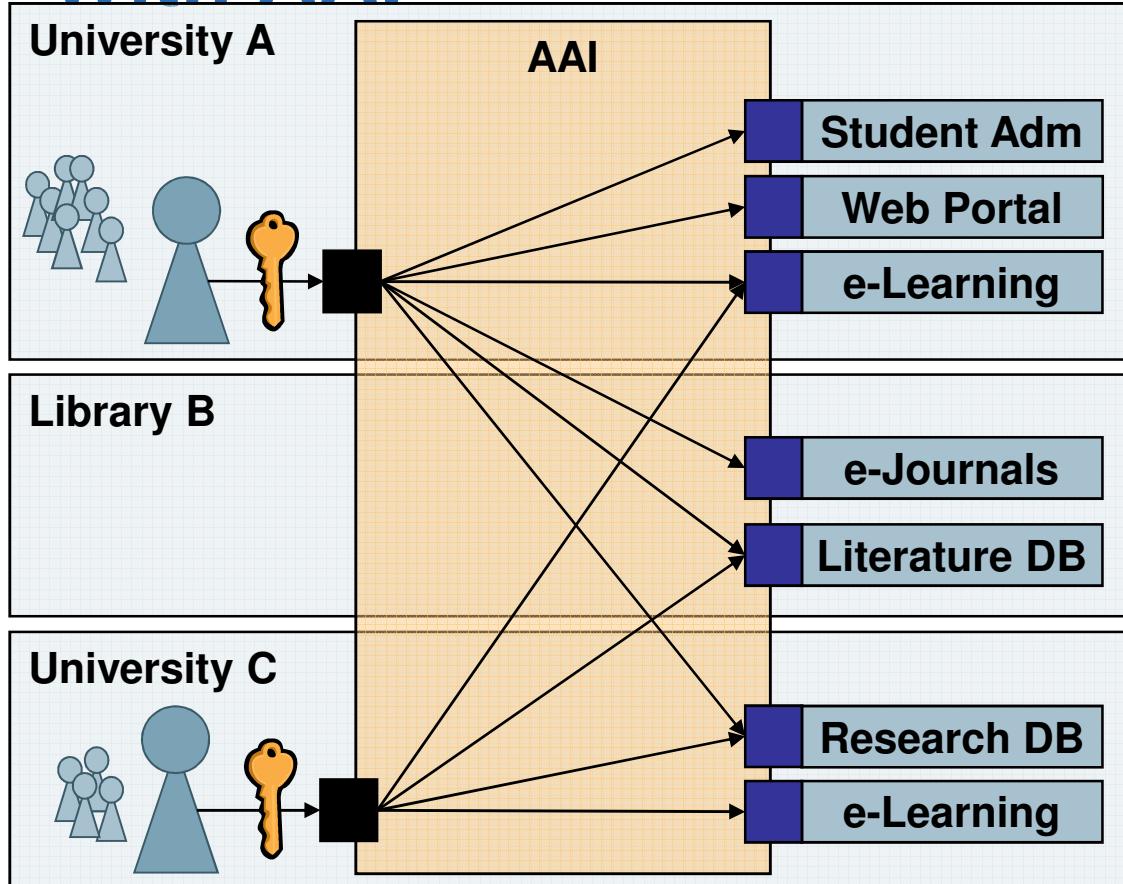
Authorization

Resource



© 2008 SWITCH

With AAI



- No user registration and user data maintenance at resource needed
- Single login process for the users
- Many new resources available for the users
- Authorization independent of location
- Efficient implementation of inter-institutional access

User Administration
Authentication

Authorization

Resource



© 2008 SWITCH

Links

- SWITCHaaI Federation
 - <http://www.switch.ch/aai>
- SAML - Open Standard from OASIS
 - <http://saml.xml.org>
- Shibboleth - Open Source Software from Internet2
 - <http://shibboleth.net/>

© 2008 SWITCH

Summary – Take Home Message

- Identities are the most important element of security.
- Identities need to be provisioned with roles, rights, objects etc.
- The provisioned identities must be published via corresponding PKI's and directory services.
- Access control and monitoring indicate how identities and rights are used / mis-used.

Architecture Components – Threat Mgmt

Risk and Security Management – HS 2012

PD Dr. Hannes P. Lubich



Motivation



Outline

- Vulnerabilities
- Fighting Threats:
 - Viruses
 - Worms
 - Spam
 - Spyware
 - Trojans
- Layered Defense:
 - Secure Content Management
 - Packet Filters and Firewalls
 - Intrusion Detection and Prevention

Vulnerabilities



Vulnerabilities

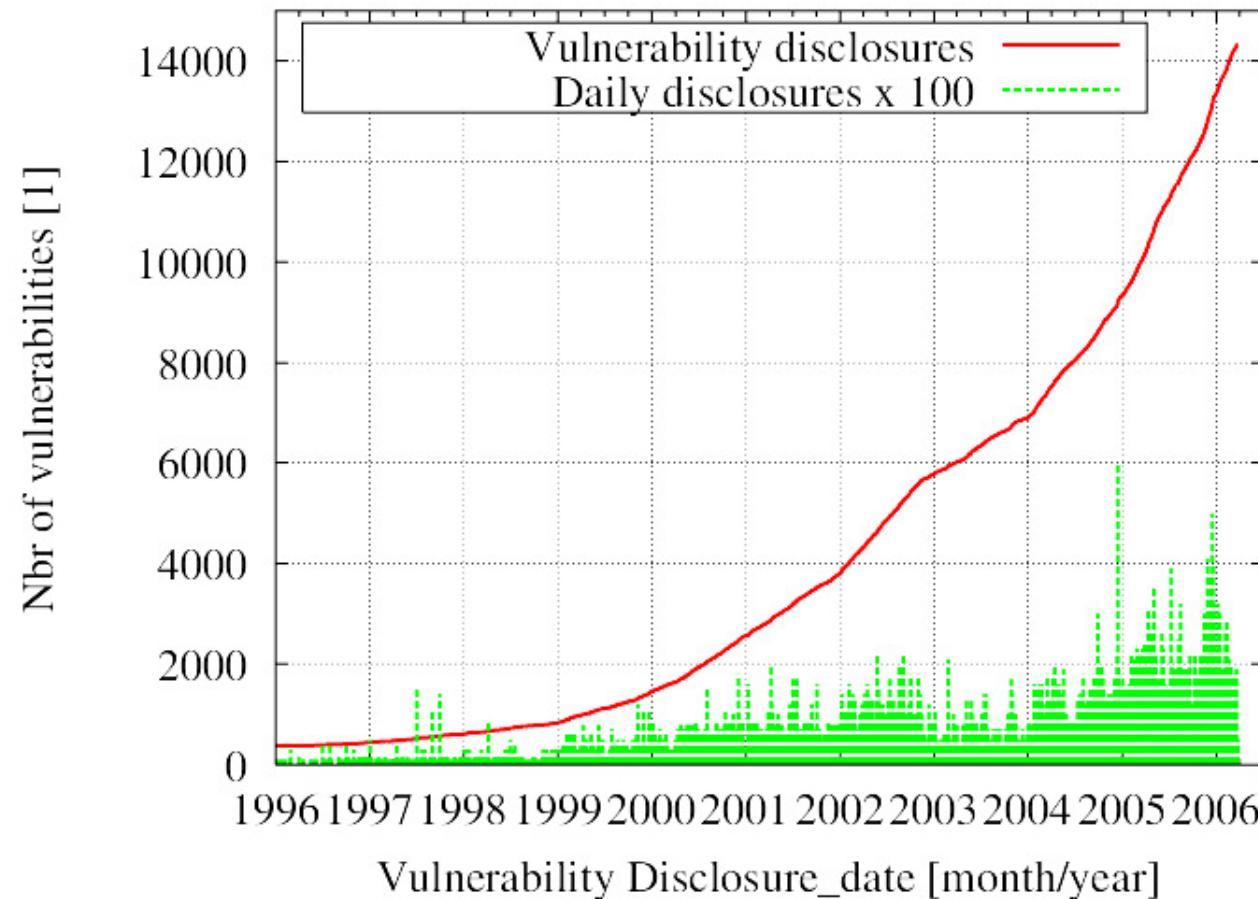
- **Security vulnerability**
 - “refers to a weakness in a system allowing an attacker to violate the confidentiality, integrity, availability of the system or the data and applications it hosts.”
 - no commonly accepted definition exists
 - the security landscape is defined by vulnerabilities.
- **What is a vulnerability?**
 - “it’s a feature, not a vulnerability”, says vendor X
 - CVE Common Vulnerability Exposure¹

1) <http://cve.mitre.org>

Source: Stefan Frei, Network Security - WS 2006/07

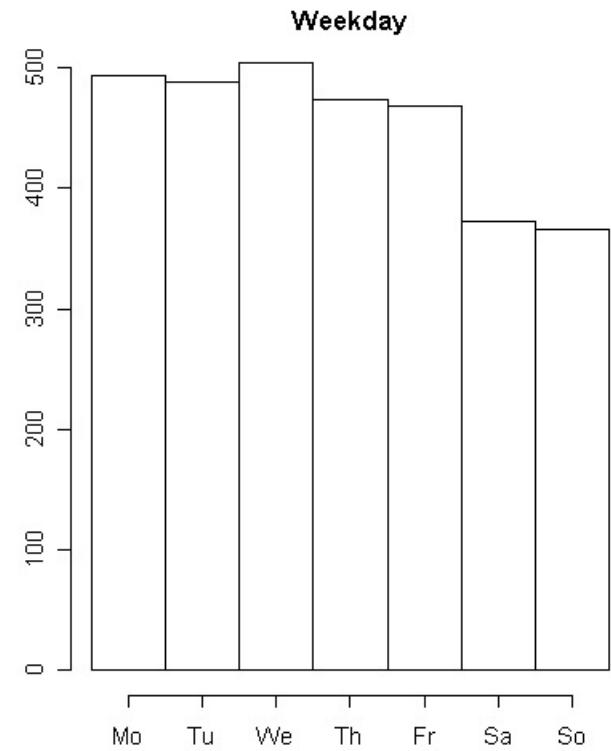
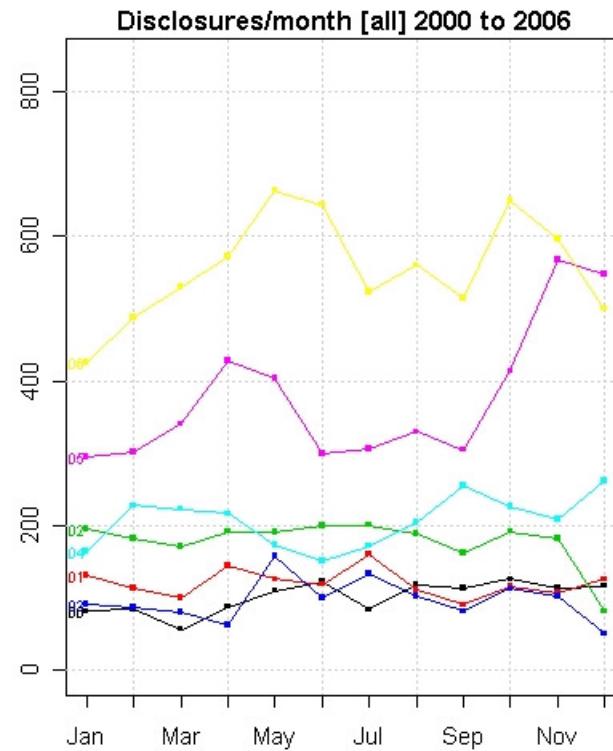
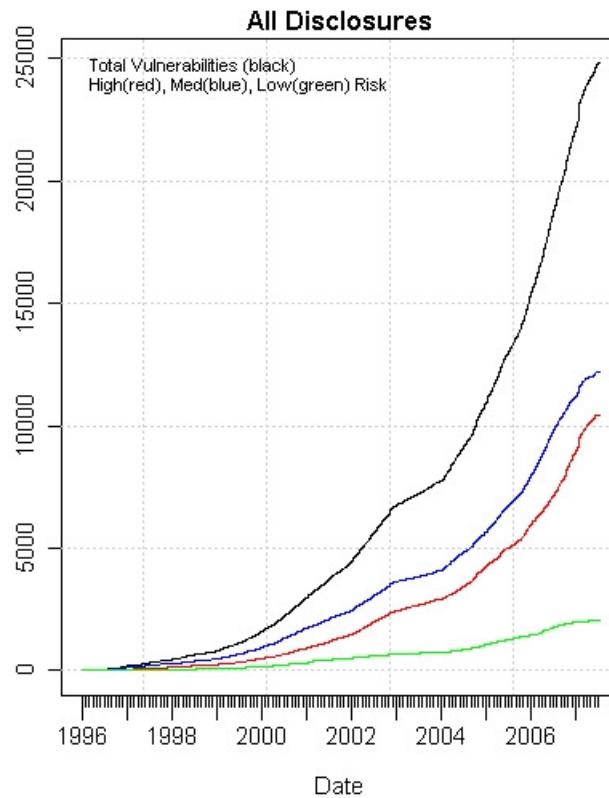
Disclosed Vulnerabilities

- Cumulated number of disclosed vulnerabilities



Source: Stefan Frei, Network Security - WS 2006/07

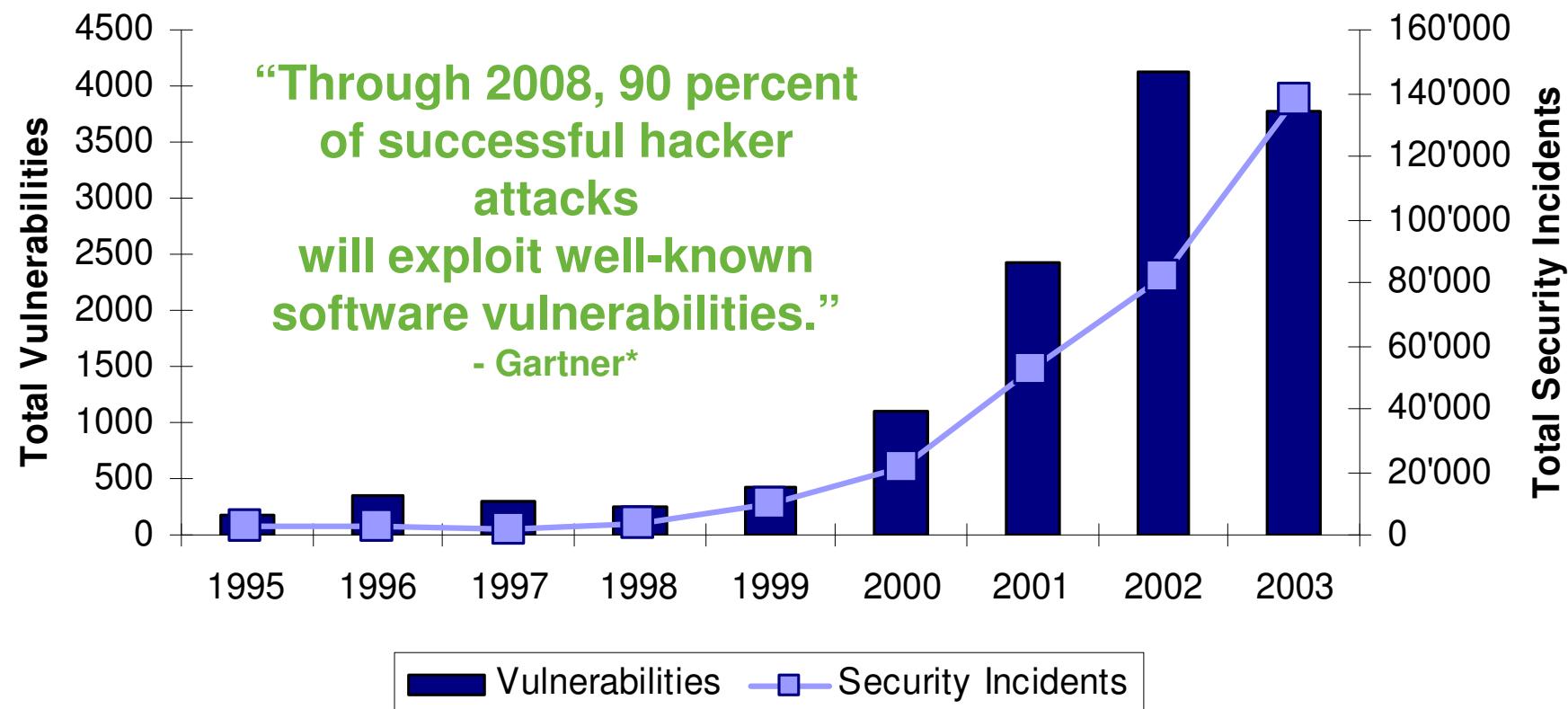
Disclosed Vulnerabilities



Source: Stefan Frei, ETHZ

The Problem is Growing

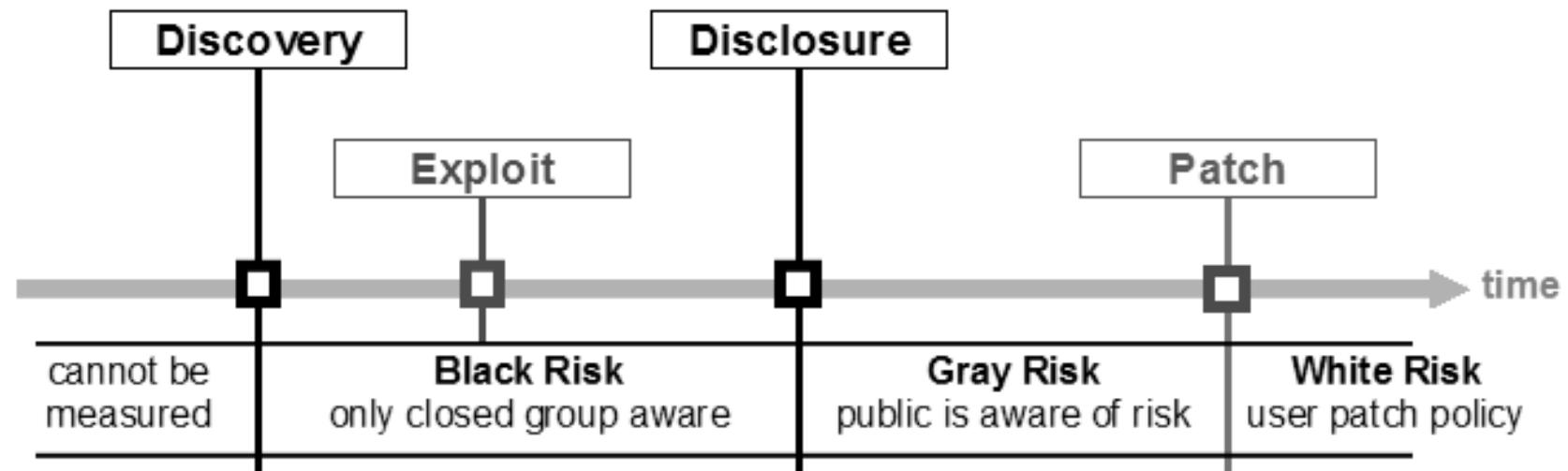
Incidents and Vulnerabilities Reported to CERT/CC



* Gartner "CIO Alert: Follow Gartner's Guidelines for Updating Security on Internet Servers, Reduce Risks." J. Pescatore, February 2003

© Computer Associates

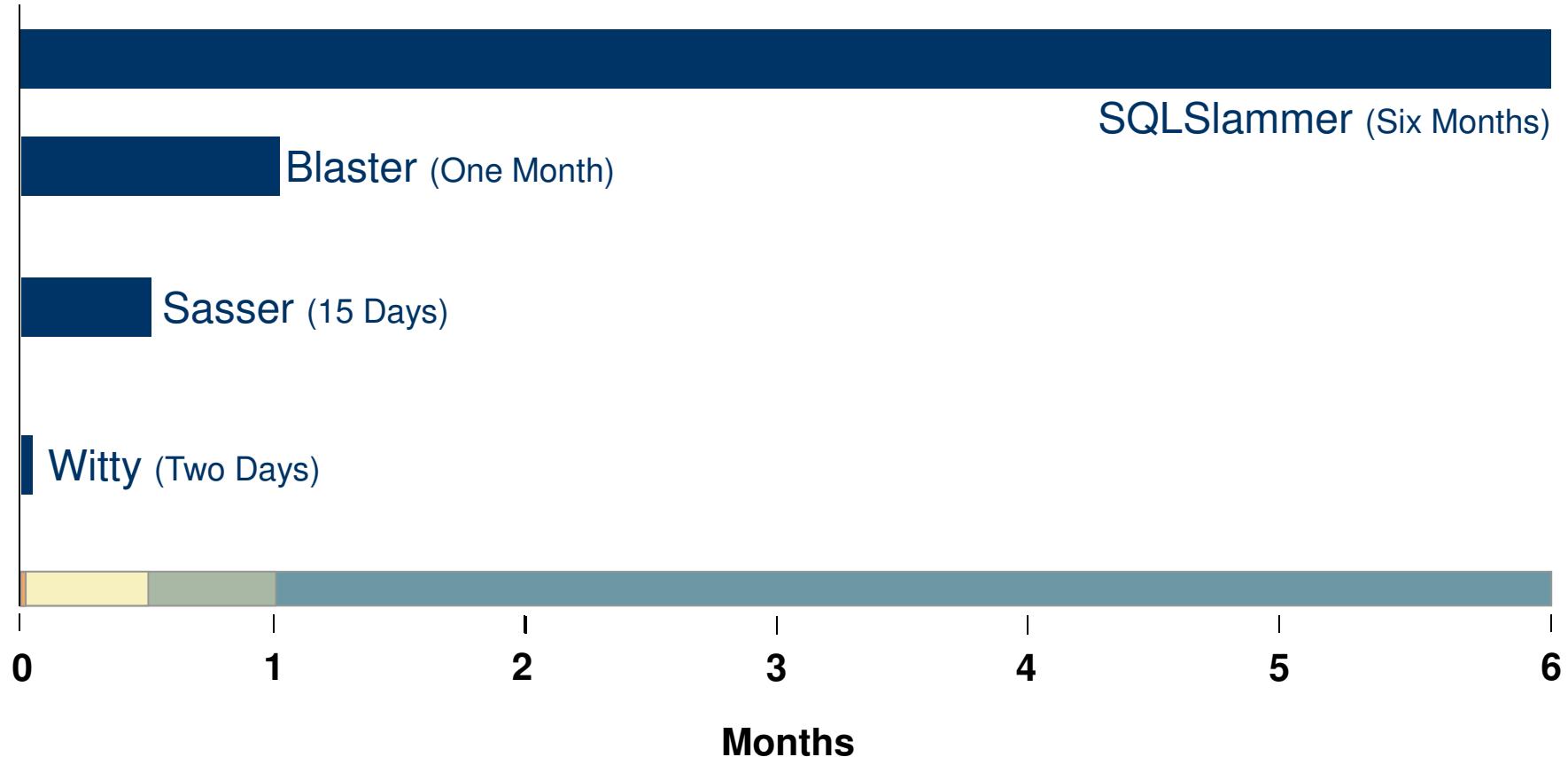
Vulnerability Lifecycle



- **Timing**
 - the relation between the times determines the risk exposure, or **window of exposure**

Source: Stefan Frei, Network Security - WS 2006/07

Window to Exploit is Shrinking



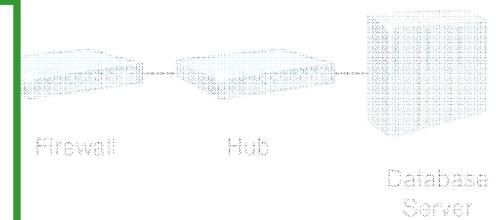
Managing Your Assets' Vulnerabilities

On average, it will take **43 staff hours** to manually address 170 vulnerabilities for 4 technologies.*

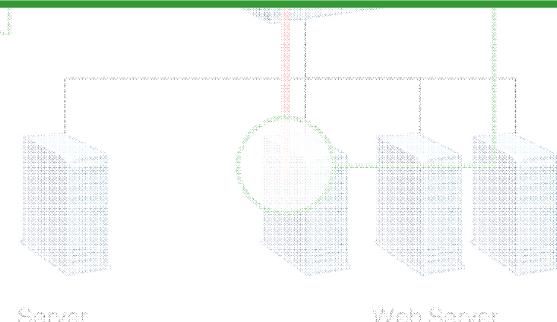
* **Source:** Based on a study conducted by a third-party consultant.

Technology	Vulnerabilities
Cisco Router IOS 12	56

Technology	Vulnerabilities
Cisco PIX 6.2	14



Technology	Vulnerabilities
Win2K Server sp4 IIS 5.1	32



Vulnerabilities, Patches, Configurations

Depending on the technology, patches correct only a portion of the vulnerabilities

Technology	Number of Vulnerabilities	Number of Vulnerabilities Fixed by Patches	Number of Vulnerabilities Fixed by Configuration
Internet Explorer 6.0 SP1 <ul style="list-style-type: none">▪ 30% of the vulnerabilities can be addressed by a patch▪ 70% need to be addressed by changing a system configuration	70	21	49
Windows XP Professional SP1 <ul style="list-style-type: none">▪ 50% of the vulnerabilities can be addressed by a patch▪ 50% need to be addressed by changing a system configuration	54	27	27
SUSE Linux 9.0* <ul style="list-style-type: none">▪ 85% of the vulnerabilities can be addressed by a patch▪ 12% need to be addressed by changing a system configuration	66	56	8

Data based on eTrust™ Security Advisory Team research, March 2004.

*SUSE Linux 9.0 has two vulnerabilities for which no fixes exist.

© Computer Associates

Automated Vulnerability & Config Mgmt

LHW2KS01

Vulnerability Task Search

State: Open
Risk: High

Results per page: 90

System Summary

You are logged in as: Kim, Paul
Last Login Date: 8/19/04 11:30:00 AM

Messages:

System:
eTrust VM Version: 8.0
Content Source: CA
Content Interval: Hourly
Content Time: 48 minute(s) after the hour
Last Content Update: 8/19/04 11:30:00 AM
Next Maintenance: 8/19/04 2:00:00 PM
License Expiration: 8/19/05 10:00:00 AM
Maximum Assets Allowed: 10000

Apply an Action:
Save as Personal

Global Notes: Global Notes apply to all selected tasks and can be applied without applying a Remediation. Clicking Save will apply the action and append the note.

System Summary

You are logged in as: Kim, Paul
Last Login Date: 8/19/04 11:30:00 AM

Messages:

System:
eTrust VM Version: 8.0
Content Source: CA
Content Interval: Hourly
Content Time: 48 minute(s) after the hour
Last Content Update: 8/19/04 11:30:00 AM
Next Maintenance: 8/19/04 2:00:00 PM
License Expiration: 8/19/05 10:00:00 AM
Maximum Assets Allowed: 10000

Deployment Queue

Showing Results: 1 to 2 of 2

Select All	Date / Submitted by	Rank	Name / Components	Affected Assets	Asset Groups
<input type="checkbox"/>	Thu Aug 19 11:30:00 CDT 2004 pkim03	69	Q319733 • Q319733	1	IT Services
<input type="checkbox"/>	Thu Aug 19 11:30:00 CDT 2004 mallen01	7	WindowsXP-KB826939-x86-ENU • WindowsXP-KB826939-x86-ENU	1	Personnel

Showing Results: 1 to 2 of 2

Remove selected items from deployment queue

Copyright © 2004 Computer Associates International, Inc. All rights reserved.
Browser requirements are Internet Explorer 6.0 and higher or Mozilla 1.4 and higher.

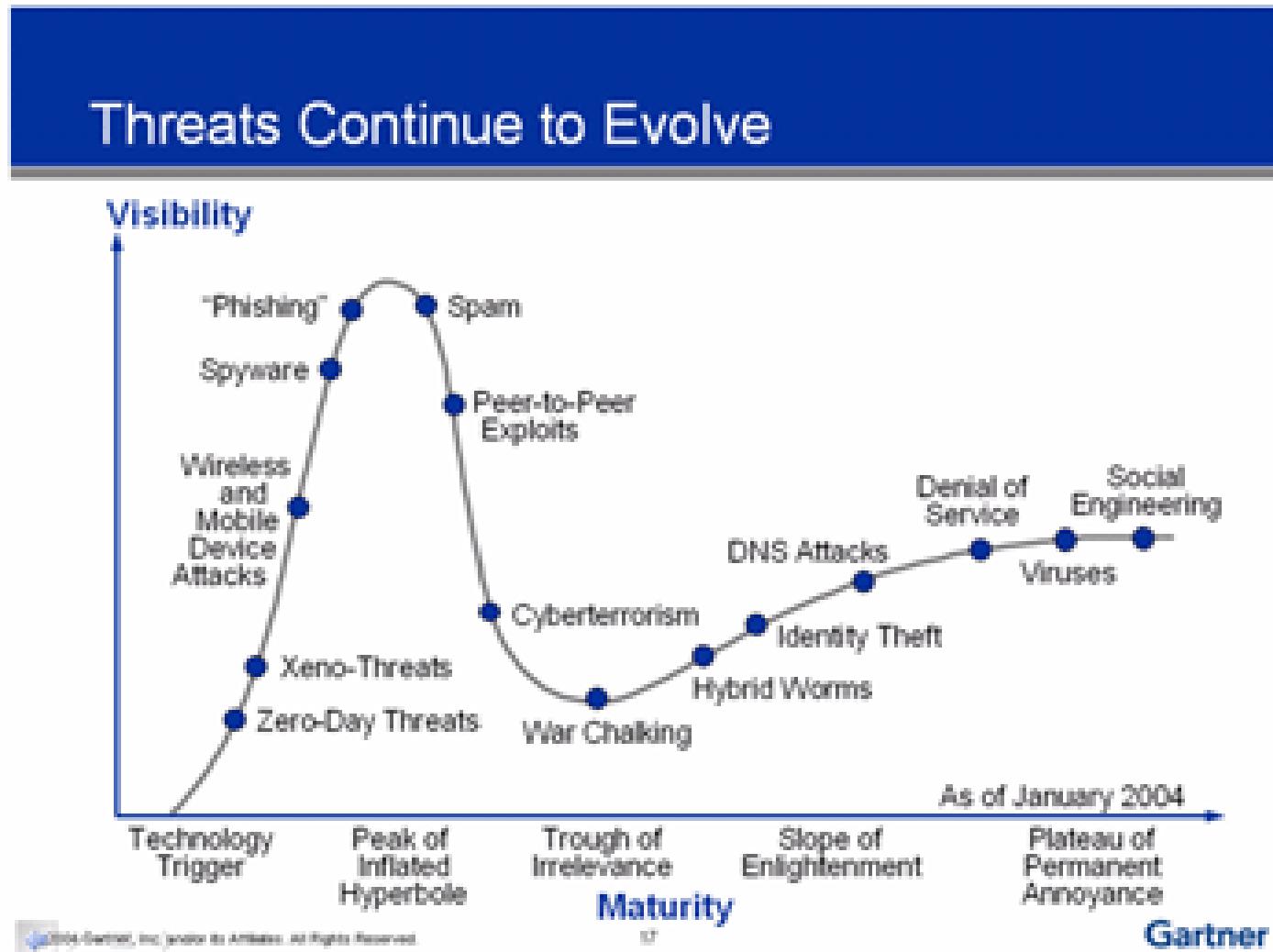
Computer Associates®

Copyright © 2004 Computer Associates International, Inc. All rights reserved.
Browser requirements are Internet Explorer 6.0 and higher or Mozilla 1.4 and higher.

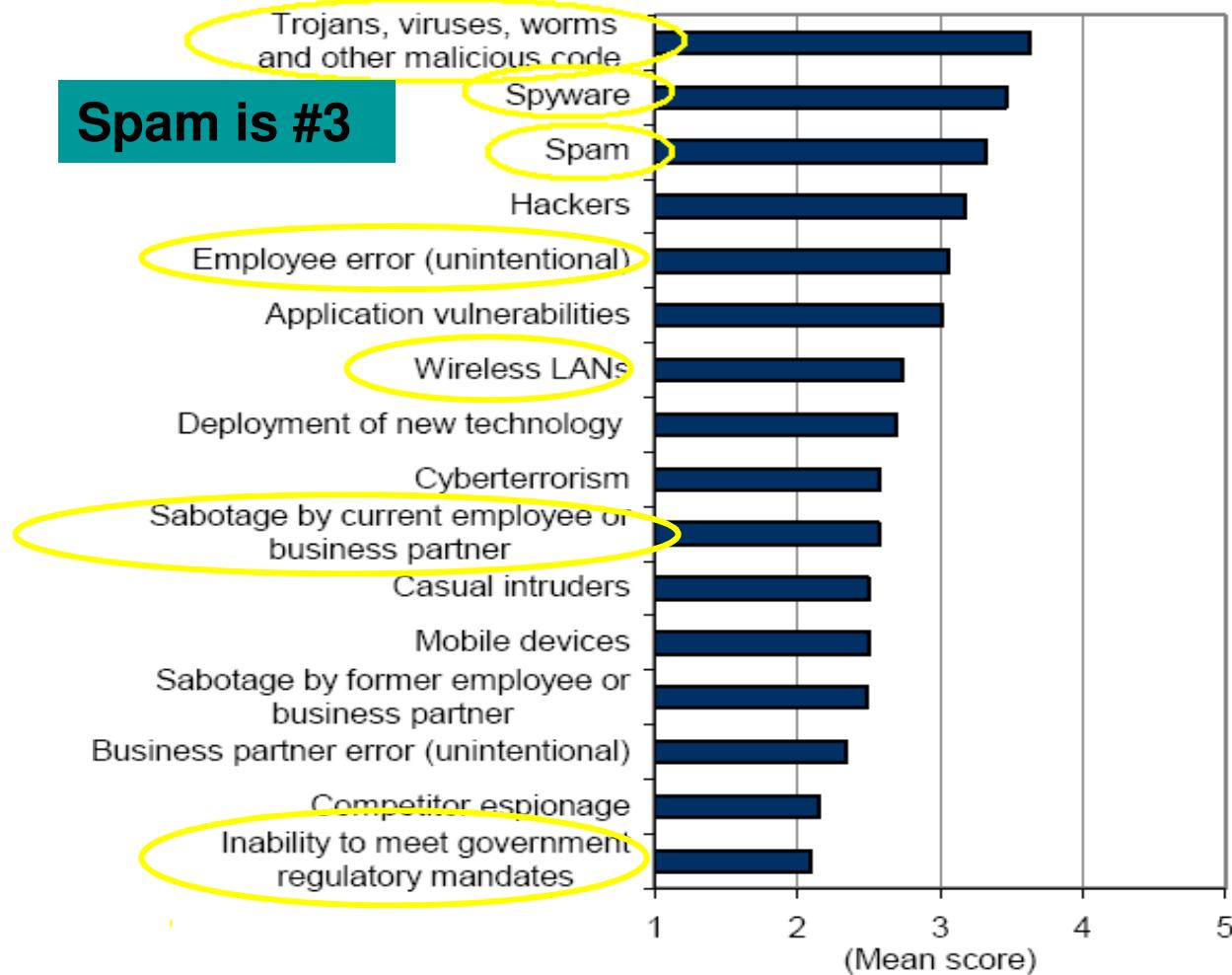
Fighting Threats



Gartner Hype Cycle on Threats



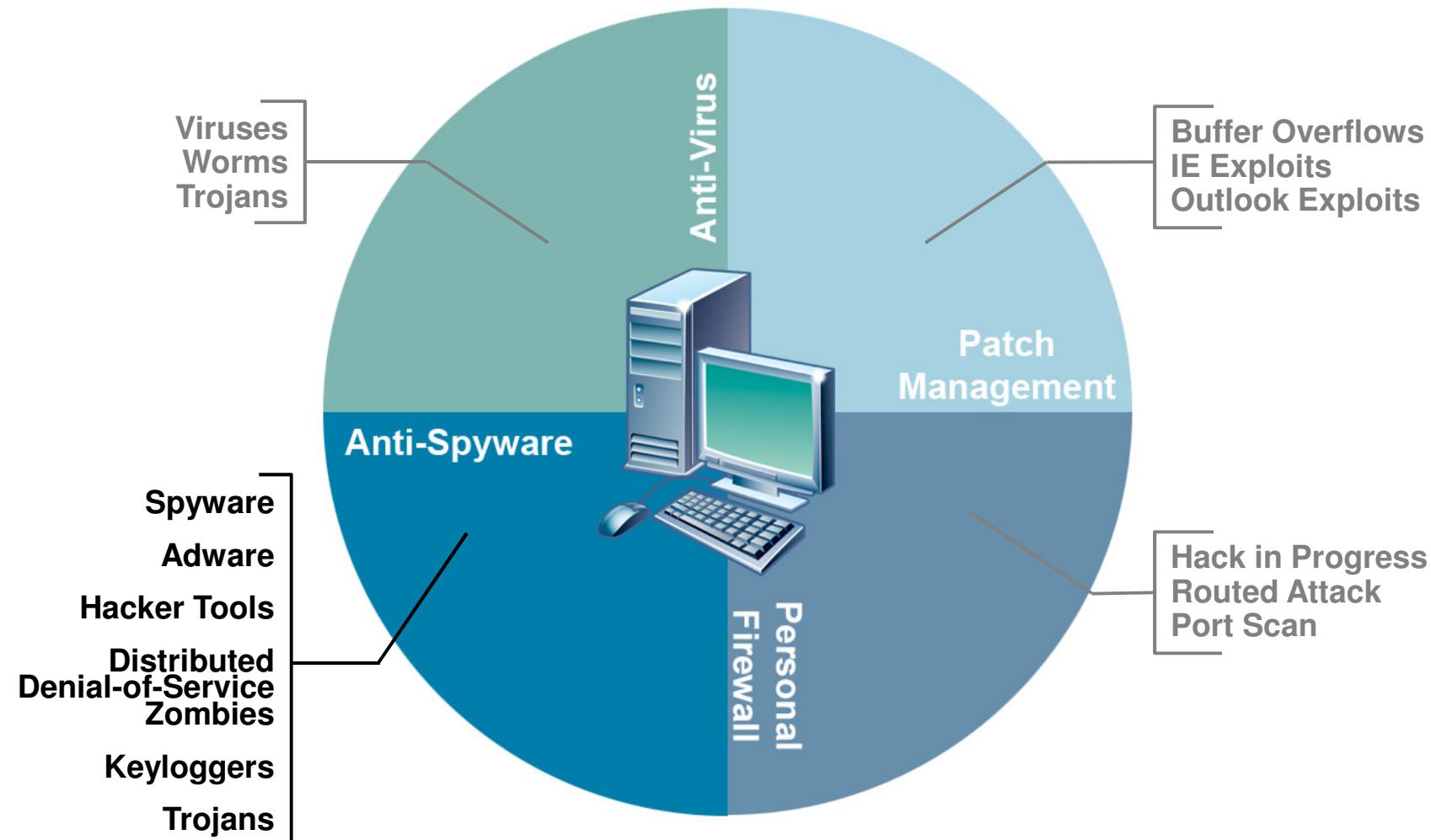
Threats Aren't Going Away



IDC, "Worldwide Secure Content Management 2005-2009 Forecast Update and 2004 Vendor Shares: Spyware, Spam, and Malicious Code Continue to Wreak Havoc," #34023 – November, 2005

© Computer Associates

Threat Defense



© Computer Associates

Future Threats

- „More of the same“: large numbers = complexity
 - „The Fast and the Furious“: quick & dangerous
 - „I'll be back“: Malware as „door opener“ for more
 - „Die hard“: Malware is trying to protect itself against countermeasures (counterattack)
- Anticipation / agility (quick detection & response)

Layered Defense: Secure Content Management



Distributed Architecture

- Either master/slave or distributed multi-tier architecture
- A “Control Center” concentrates all the data flow from and to the different SCM components
- We can separate SCM into “**Engine**” and “**Management**” components

Typical Engine Components:

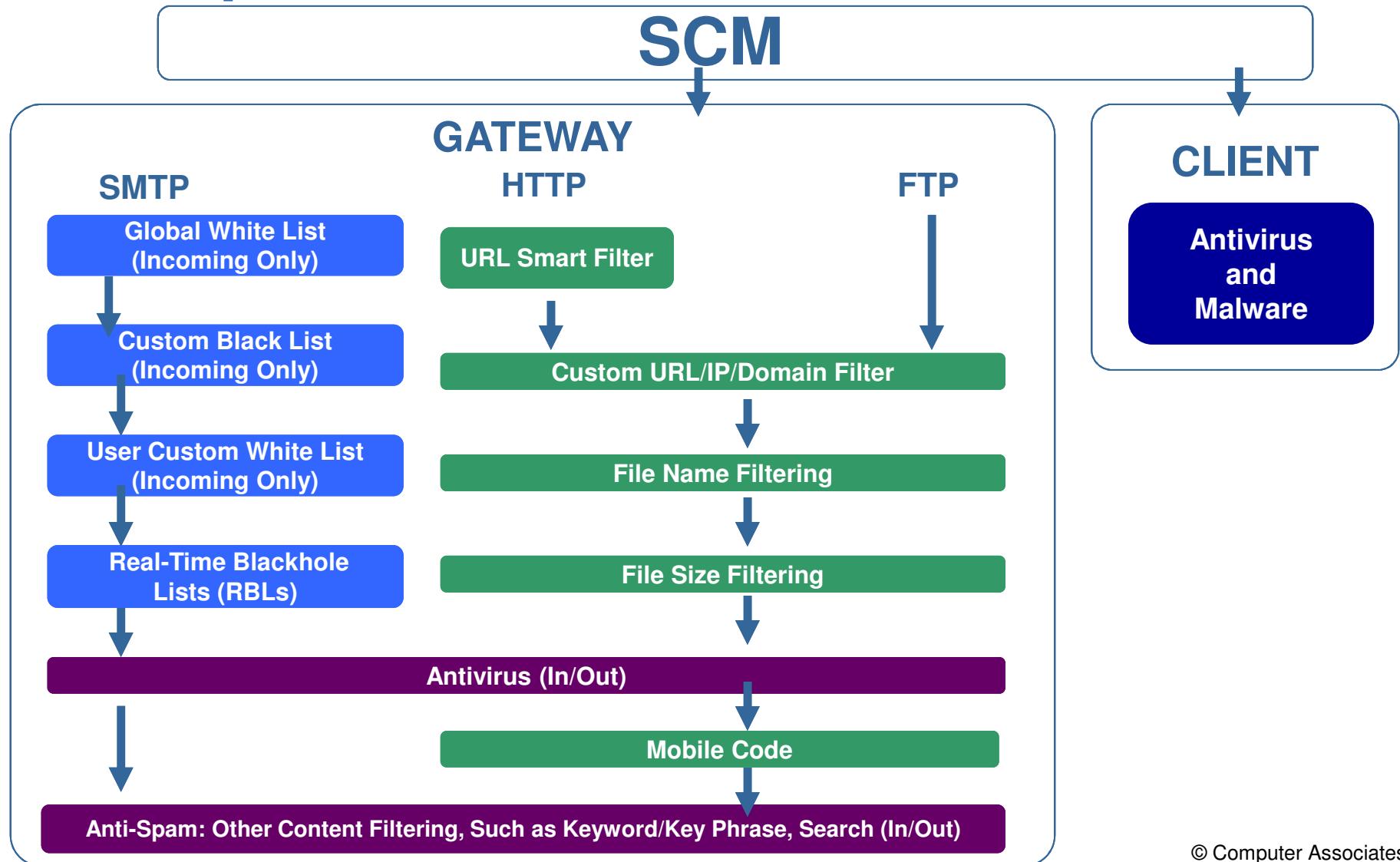
- HTTP/FTP Content Engine – Performs analysis of web content, FTP over the HTTP proxy, and URL Filtering
- SMTP Content Engine – Performs analysis of SMTP content and spam filtering

Distributed Architecture

Typical Management Components:

- **Control Center** — The main management service which concentrates data, distributes policies, and provides connectivity between all eTrust SCM components. Typically, there should be a single instance of the Control Center in an environment.
- **Quarantine Manager** — A tool and service which manage messages that were quarantined based on the SMTP Content Engine's analysis. There should be a single instance of the Quarantine Manager in an environment.
- **Central Reporter** — A tool and service which provide over time reporting based on data collected by the Content Engines. There should be a single instance of the Central Reporter in an environment.
- **Manager Console** — The main management user interface, which connects to the Control Center and allows policy and environment settings to be configured on the Content Engines, and real-time monitoring of Engines and Enterprise activities.

Example Architecture



Pause



Layered Defense: Packet Filters and Firewalls



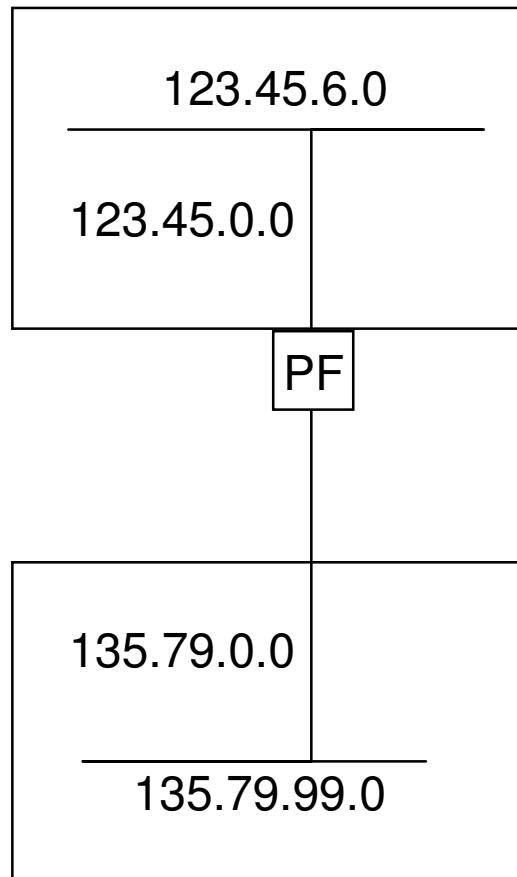
Firewall Principles

- Design
 - Stateless
 - Stateful
- Deployment:
 - local (personal firewall)
 - Gateway (at organisational or org. unit border)
 - Combination
 - Redundancy
- Operation
- Integration (esp. with end-to-end security / VPN)

Stateless Packet Filters

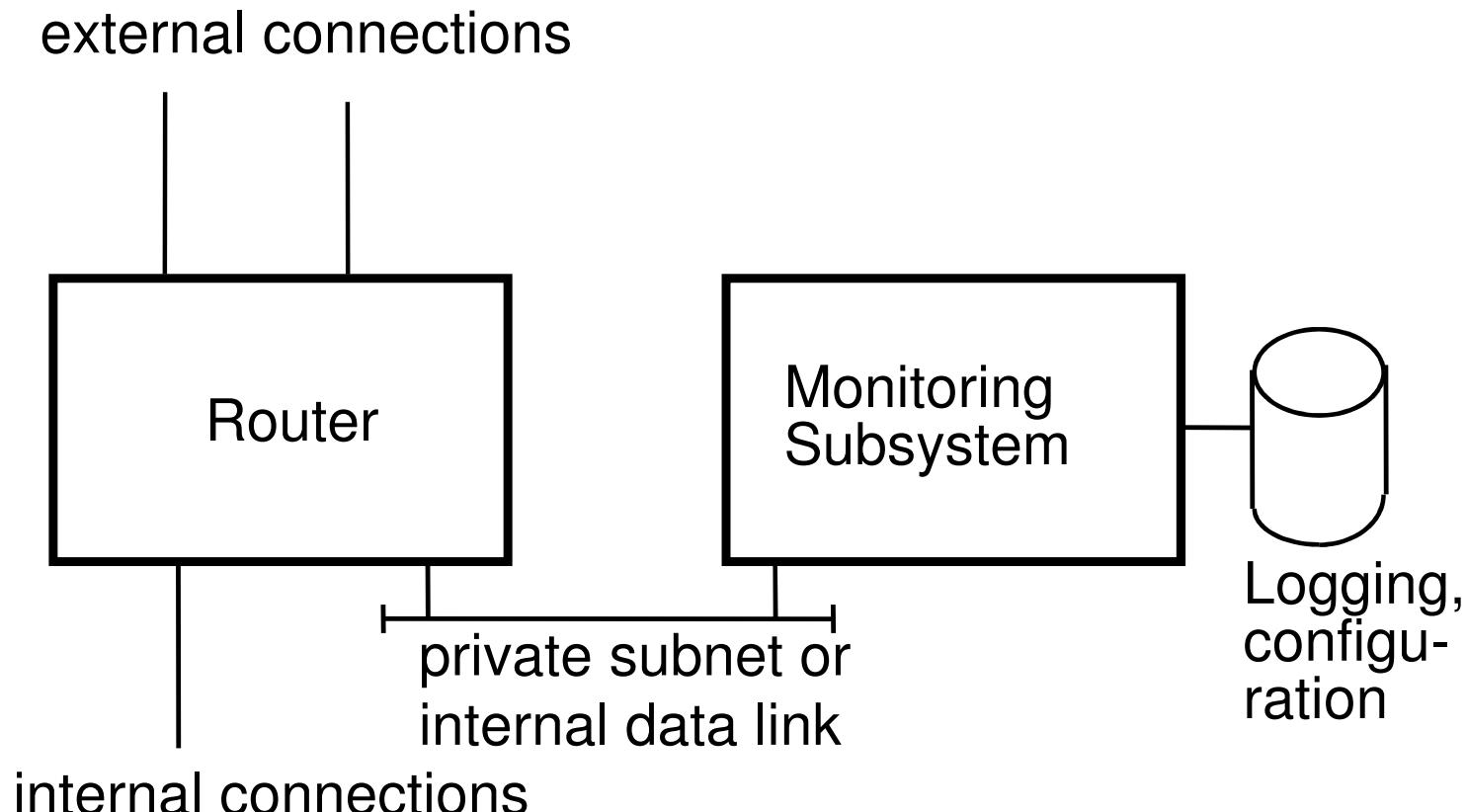
- Network layer functionality
- Information used for filtering:
 - IP-Address of senders
 - IP-Address of recipient
 - Port number of recipient
 - possibly port number of sender
 - Responsible transport protocol
- Filter rules (static or dynamic/timing-based)
- Limited authentication (e.g. through “port knocking”, see fwknop)
- Deficiencies of packet filters

Filter Rules: Simple Example



Rule	Source	Destination	Action
A	135.79.0.0/16	123.45.6.0/24	Permit
B	135.79.99.0/24	123.45.0.0/16	Deny
C	0.0.0.0/0	0.0.0.0/0	Deny

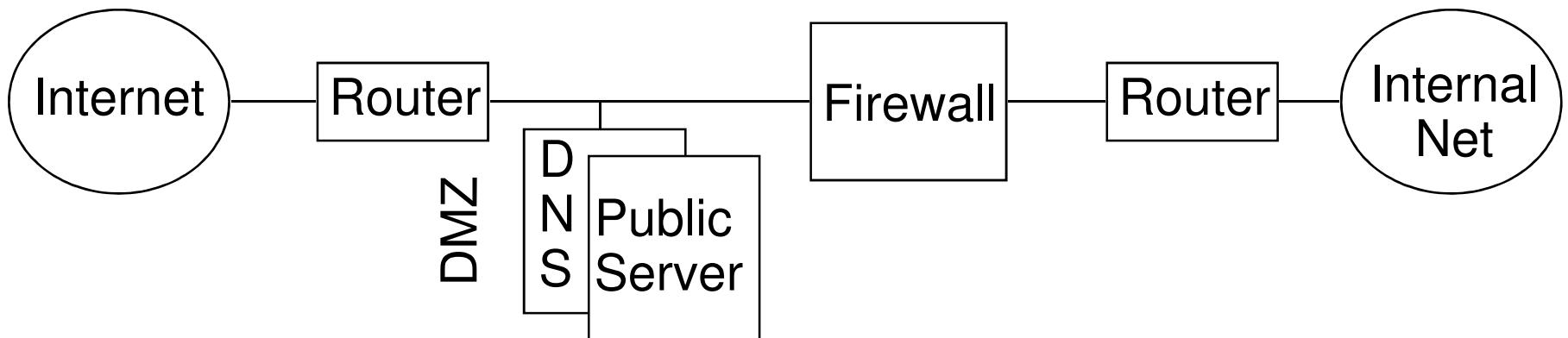
Extended Packet Filter



Controversy: stateless versus stateful filtering/packet inspection

Application Level Firewall

- Terminates all “store-and-forward” services (DNS, SMTP, ...), possibly through semi-public servers in one or more DMZ
- Authentication of users/processes requesting access (both ways)
- Logging and alarming
- Selective forwarding of application connections
- Rewriting / hiding of internal IP addresses (NAT) etc.
- Carries out actions on behalf of a user / program (proxy)
- Acts as a VPN endpoint



Operation of Firewalls

- With today's network security mechanisms, organisations can provide controlled access from/to public networks such as the Internet, however performance and functionality are limited.
- Configuration, daily operation and administration of access control mechanisms should not be coupled closely with the normal IT operation processes.
- Instead, installation and operation of a secure network access system should be the responsibility of a security operations group, with corresponding know-how, resources and empowerment.
- An up-to-date and accepted security policy and operations guide as well as proper education of all parties involved are more important than investments in "technology-only" security mechanisms.

Layered Defense: Intrusion Detection / Prevention



What is an “Attack”?

- Obvious:
 - Port Scan
 - “delete all files on fileserver”
- Less Obvious:
 - Slow/Random Scan
 - Irregular Login Times & Patterns
- Not Obvious:
 - Too many “regular” users (DDoS)
 - Covert Channels

How to Recognise an Intention?

- Log and evaluate patterns of “normal” use for a long time → profiling per unit (user, department, customer segment,)
 - Define “need to know / have” policy & rules and log all violations
 - Systematic evaluation of profiles against usage logs of software and users
- All deviations indicate a potential risk

Intrusion Detection System

- Intrusion Detection
 - monitor network / system to detect intrusions
 - traffic compared to signature database of known attacks (1'000+)
 - various detection methods and techniques
 - customized through security policy (what to detect, how to react)
- Output
 - Alerts (.. many of them)
 - Action (block)
 - Reporting, Analysis

Source: Stefan Frei, Network Security - WS 2006/07

Lots of events ..

The screenshot shows the RealSecure SiteProtector software interface. The window title is "RealSecure SiteProtector - swordfish.iss.net". The menu bar includes Connection, Window, More Info, SF Console, Edit, Grouping, Analysis, Asset, Sensor, Tools. The main area has tabs for Asset, Sensor, and Sensor Analysis, with Sensor Analysis selected. On the left, there's a tree view under "Enterprise Groups" for "SWORDFISH" with nodes like "SWORDFISH (0:0)", "LONDON (0:0)", "Testing (0:0)", and "Ungrouped Assets". The main pane displays a table of events with columns: Tag Name, Status, Severity, Event Count, Source Count, Target Count, Object Count, Earliest Event, and Latest Event. The table lists numerous entries, such as "http-dotdot" with 181 events, "http-cgi-vuln" with 4 events, and "synflood" with 73750 events. Most entries have a red or yellow severity indicator.

Tag Name	Status	Severity	Event Count	Source Count	Target Count	Object Count	Earliest Event	Latest Event
http-dotdot	Not Applicable	High	181 (+133)	9 (+7)	15 (+11)	1	2002-04-17 21:00:00 EDT	2002-04-18 06:00:01
http-cgi-vuln	Not Applicable	High	4	2	2	1	2002-04-18 00:00:00 EDT	2002-04-18 00:00:01
synflood	Not Applicable	Medium	73750 (+20)	1	27679 (+8)	25	2002-04-13 19:00:00 EDT	2002-04-18 05:00:01
smurf	Not Applicable	Medium	1	1	1	1	2002-04-18 01:00:00 EDT	2002-04-18 01:00:01
ip-halfscan	Not Applicable	Low	27799 (+6)	2 (+1)	27793	2	2002-04-15 14:00:00 EDT	2002-04-18 06:00:01
ip-unknown	Not Applicable	Low	105 (+37)	17 (+1)	18 (+5)	1	2002-04-15 15:00:00 EDT	2002-04-18 06:00:01
decod-nmap	Not Applicable	Low	1	1	1	1	2002-04-18 06:00:00 EDT	2002-04-18 06:00:01
traceroute	Not Applicable	Low	10354 (+3717)	4701 (+1648)	56 (+10)	541	2002-04-13 19:00:00 EDT	2002-04-18 06:00:01
ip-dup	Not Applicable	Low	16 (+7)	5 (+1)	4 (+1)	1	2002-04-16 15:00:00 EDT	2002-04-18 03:00:01
decod-ftp-syst	Not Applicable	Low	7 (+3)	3 (+1)	3 (+1)	1	2002-04-17 15:00:00 EDT	2002-04-18 01:00:01
decod-ssh	Not Applicable	Low	84	57	4	70	2002-04-16 20:00:00 EDT	2002-04-18 00:00:01
dhcp-ack	Not Applicable	Low	1307	2	1	1	2002-04-17 14:00:00 EDT	2002-04-18 00:00:01
decod-dns-zone	Not Applicable	Low	1	1	1	1	2002-04-18 00:00:00 EDT	2002-04-18 00:00:01
rs-kill	Not Applicable	Low	9	3	4	4	2002-04-14 02:00:00 EDT	2002-04-17 20:00:01
dhcp-request	Not Applicable	Low	63	1	1	1	2002-04-17 14:00:00 EDT	2002-04-17 19:00:01
dhcp-discover	Not Applicable	Low	44	3	1	1	2002-04-17 14:00:00 EDT	2002-04-17 18:00:01
ping-flood	Not Applicable	Low	22	1	1	1	2002-04-17 15:00:00 EDT	2002-04-17 15:00:01
snmp-suspicious-get	Not Applicable	Low	6	2	1	1	2002-04-17 14:00:00 EDT	2002-04-17 14:00:01
sensor-info	Not Applicable	Low	4	1	1	1	2002-04-15 15:00:00 EDT	2002-04-15 15:00:01

Source: Stefan Frei, Network Security - WS 2006/07

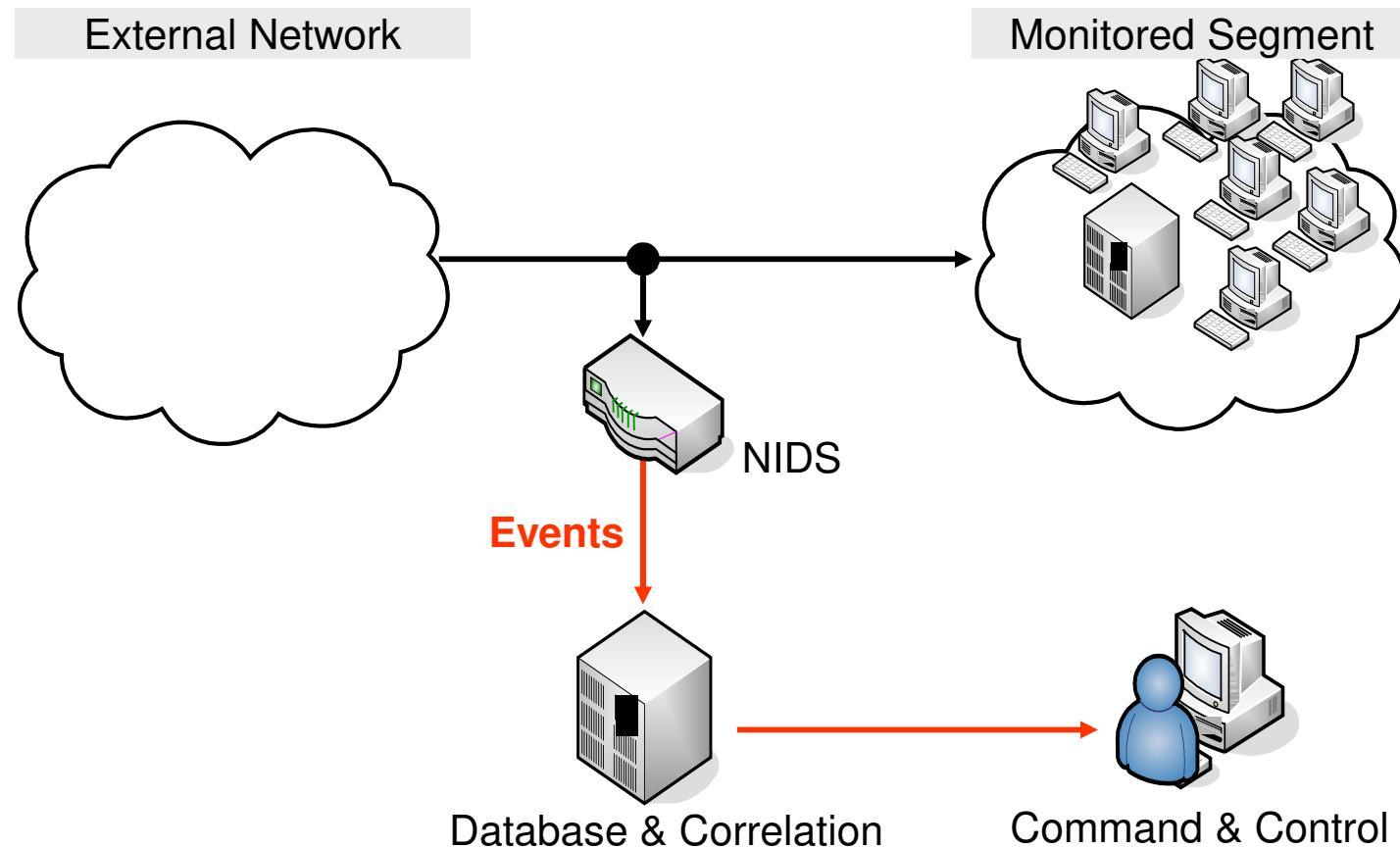
Intrusion Detection System

- Challenges
 - false alarms (false positives, false negatives)
 - cope with network speed (true GB monitoring)
 - sensor management
 - signature distribution
 - policy management
 - intervention
 - 24x7 monitoring needs people!
- IDS is a complex business
 - outsourcing
 - managed security services (MSS)

Source: Stefan Frei, Network Security - WS 2006/07

Network IDS - NIDS

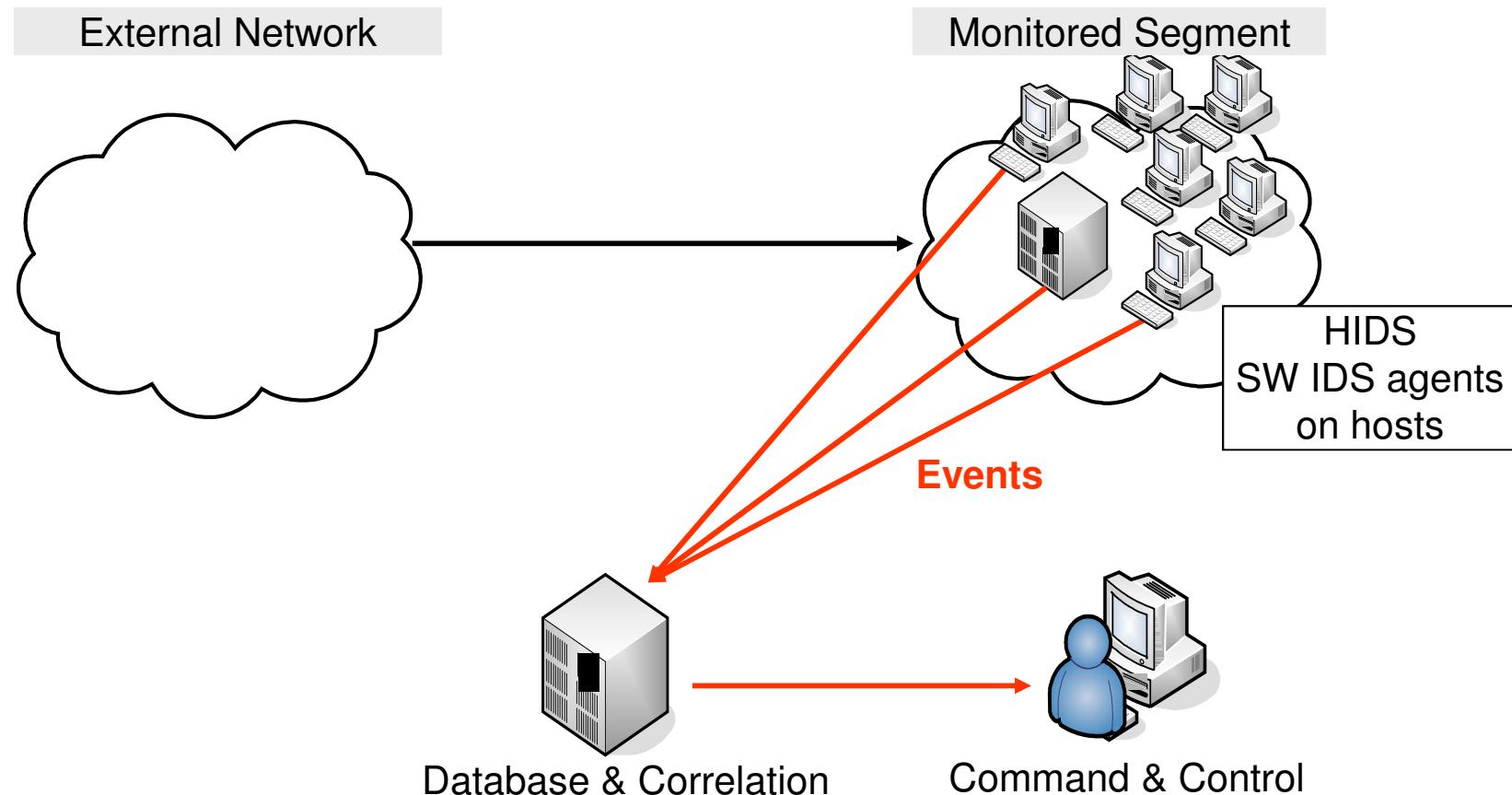
- Monitoring networks, segments, ..



Source: Stefan Frei, Network Security - WS 2006/07

Host-based IDS - HIDS

- Monitoring individual hosts



Source: Stefan Frei, Network Security - WS 2006/07

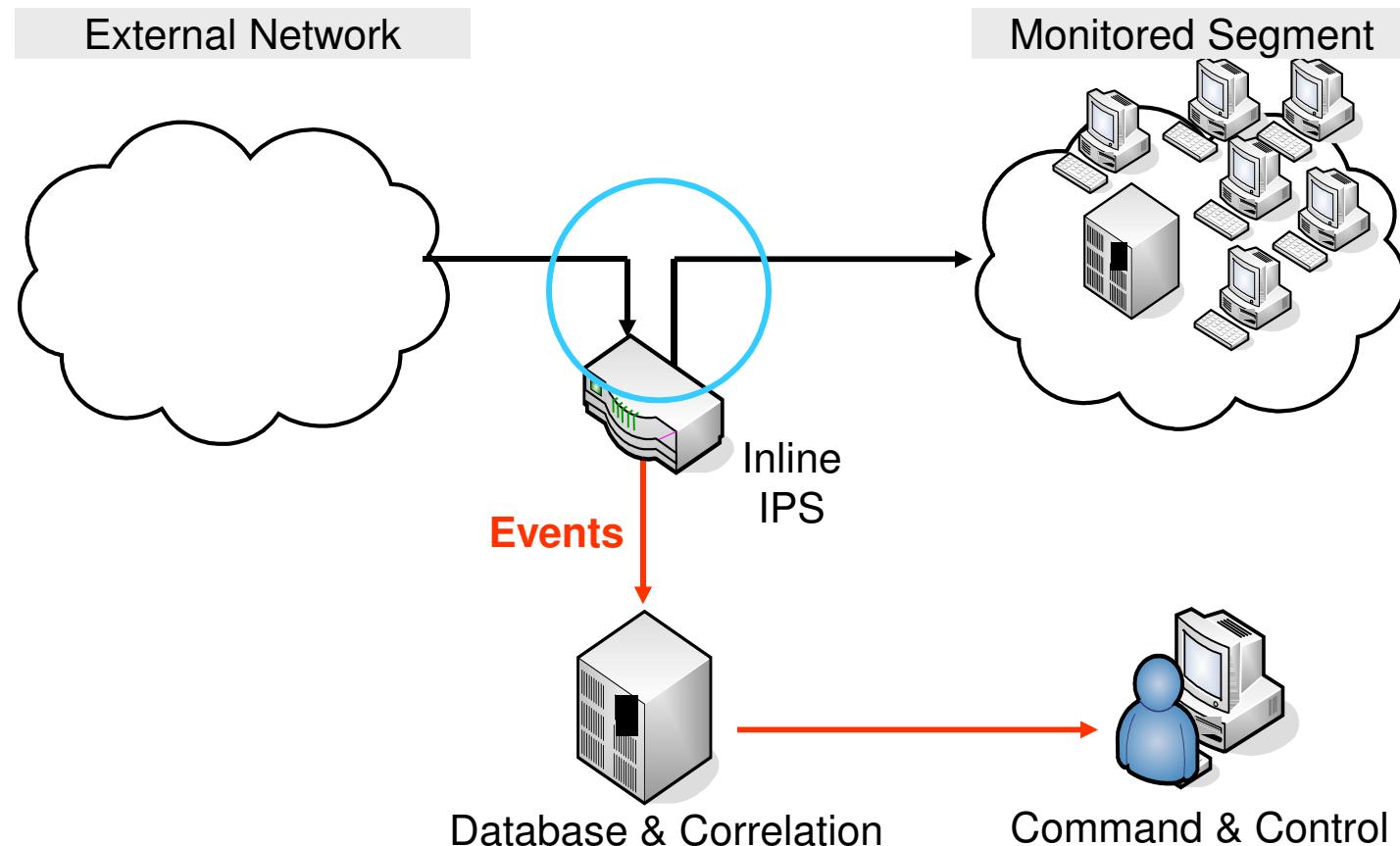
Intrusion Prevention System

- In-line device
 - traffic flows through, not past the sensor
 - failed-open or failed-close mode?
 - a false positive automatically becomes a “network problem”
 - resource intensive (CPU, Memory)
 - can protect against single-packet attacks
- Operation
 - normalize (reassemble, decode and store) traffic
 - inspect traffic
 - forward to output if OK

Source: Stefan Frei, Network Security - WS 2006/07

Network IPS

- Intrusion Protection/Prevention System



Source: Stefan Frei, Network Security - WS 2006/07

Market Overview (Gartner Magic Quadrant)

Figure 1. Magic Quadrant for Network Intrusion Prevention !



As of December 2010

Source: Gartner (December 2010)

Pattern Recognition and Intelligence

- Problems with “classic” IDS approach:
 - Pattern recognition requires significant learning / training phase (else too many false positives/negatives)
 - Very restrictive: everything which is not explicitly allowed, is suspicious / forbidden
 - Very resource-consuming: everything which is allowed must be explicitly granted / codified in rule sets
 - You can only sanction what you already know

- “Self learning” strategies, intelligent recognition of usage patterns, correlation analysis

Malware Communities (personal pick)

The screenshot shows a Firefox browser window with the following details:

- Title Bar:** Firefox
- Address Bar:** www.finjan.com/SecurityLab.aspx?id=547
- Page Header:**
 - finjan® Vital Security™
 - securing your web
 - Home | Contact us | Site Map | RSS | Follow us | Search
 - M86 SECURITY logo
- Page Content:**
 - Left Sidebar:** Overview, Latest Web Vulnerabilities, "In the Wild" Audit Results, URL Analysis, Info Center, Cybercrime Intelligence, Test Your Vital Security Policy, Code Obfuscation, Glossary, MCRC Blog.
 - Main Content Area:**
 - Section:** Malicious Code Research Center (MCRC)
 - Description:** Finjan's Malicious Code Research Center specializes in the detection, analysis and research of web threats, including Crimeware, Web 2.0 attacks, Trojans and other forms of malware. Our goal is to be steps ahead of hackers and cybercriminals, who are attempting to exploit flaws in computer platforms and applications for their profit. In order to protect our customers from the next Crimeware wave and emerging malware and attack vectors, MCRC is a driving force behind the development of Finjan's next generation of security technologies used in our Secure Web Gateway solutions.
 - Section:** Latest Web Vulnerabilities
 - Table:**

Name of the Vulnerability	Publish Date	Severity
Registry OCX ActiveX Vulnerability	Jul 15, 2010	■
Cisco Secure Desktop CSDWebInstaller ActiveX Vulnerability	Jul 15, 2010	■
Microsoft Internet Explorer Transfer Of Control Vulnerability	Jul 15, 2010	■
 - Threat Alerts:**
 - Worm.Win32.Skipi.a
 - Trojan.Win32.StartPage.au
 - Email-Worm.VBS.Small.n
 - W32/Sohana-AM
 - Troj/Agent-GEP
 - Troj/IRCBot-YQ
 - Malicious Page of the Month:**

Malicious Page of the Month	Date
Malicious Page of the Month	10/2008
Malicious Page of the Month	09/2008
Malicious Page of the Month	05/2008
Malicious Page of the Month	04/2008
Malicious Page of the Month	02/2008
Malicious Page of the Month	01/2008

Summary – Take Home Message

- Vulnerabilities are (and will remain) a fact of life, due to complexity and “time to market”.
- Corresponding malware, partially driven by criminal and commercial motives, will continue to prosper.
- Defense needs to be layered, cooperative, and needs to „look both ways“.
- Providing sufficient service, even under attack.

Architecture Components – Security Information Mgmt, Correlation, Forensics

Risk and Security Management – HS 2012

PD Dr. Hannes P. Lubich



Motivation

“Wenn das technische Personal gewusst hätte, wo es hinschauen muss, und hätte es die wichtigen Fehlermeldungen erkannt – dann wäre das Schlimmste vermeidbar gewesen.”

Hansjörg Hess, Chef SBB-Infrastruktur
(Tages Anzeiger, 2. Juli 2005)



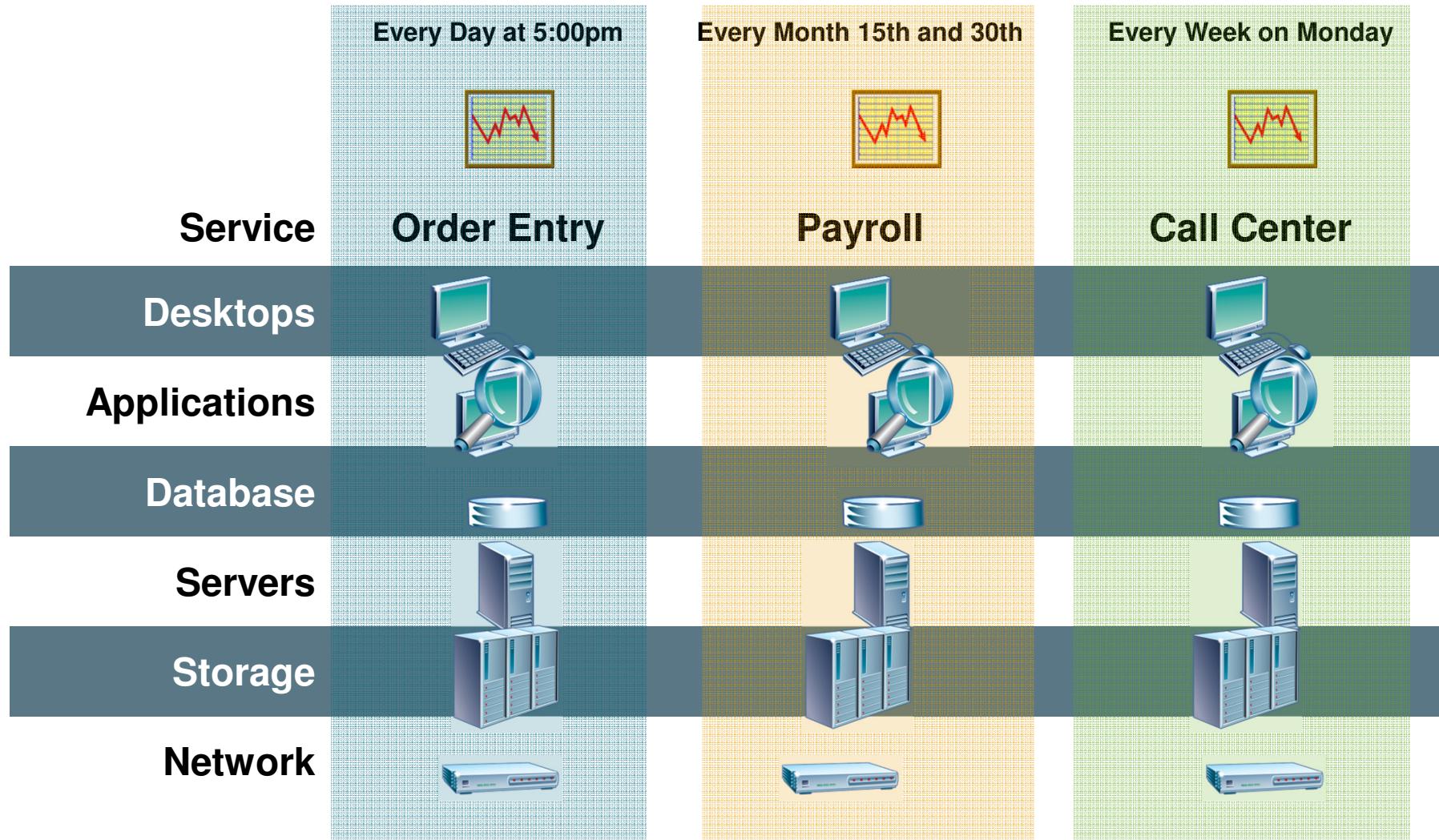
Outline

- Security Information Management
 - Collection
 - Normalisation
 - Archiving
 - Correlation
 - Reporting & Escalation
- Interfaces with other IT Management Systems
- Forensic Analysis
- Integration with Enterprise IT Management

Security Information Management Requirements



IT is Still Managed in Silos



© Computer Associates

Legal / Regulatory Requirements

- Non delegateable responsibility for proper IT operation as part of responsibility for proper job execution (Sorgfaltspflicht) and possibly product liability (Produkt-Haftpflicht).
- Internal & external audits of IT service availability, functionality, performance and security (ICS).
- Proof of ability for systematic risk management (e.g. providers and users of financial services, medical / life sciences etc).
- Reliable and reproducible calculation of risks, effects and countermeasures, e.g. as part of service level agreements (internal / outsourced).

Business / Organisational Requirements

- „Doing more with less“ – no additional resources
- Need to adapt to frequently changing business requirements
- Consideration of new / additional attacker profiles and motivations
- Migration from technical IT security towards a consistent, company (IT) risk management

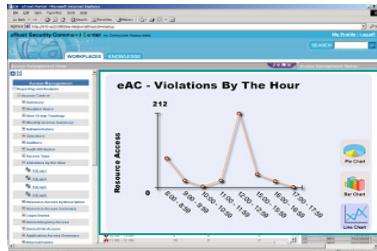
Technical / Operational Requirements

- Mature standards and „best practices“ available
- (Too) large choice of solution components
- Retain (normal) service level, even under an on-going threat or attack
- Outsourcing / out-tasking of IT services while retaining IT governance responsibility and execution

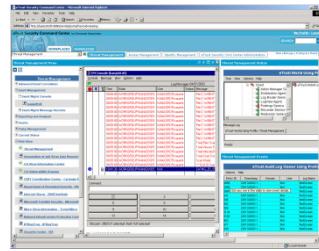
Security Information Management Functionality



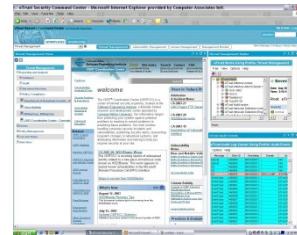
Security Director



Security Administrator



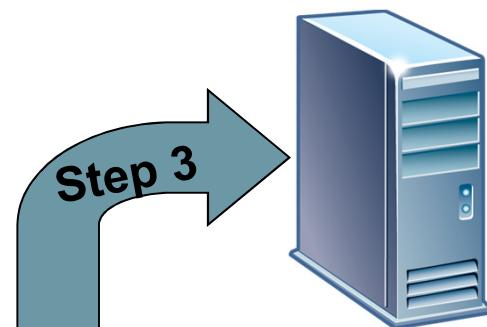
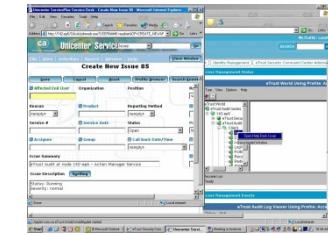
Antivirus Administrator



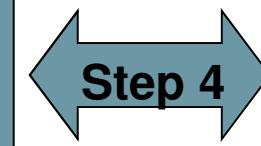
CSO



Help Desk



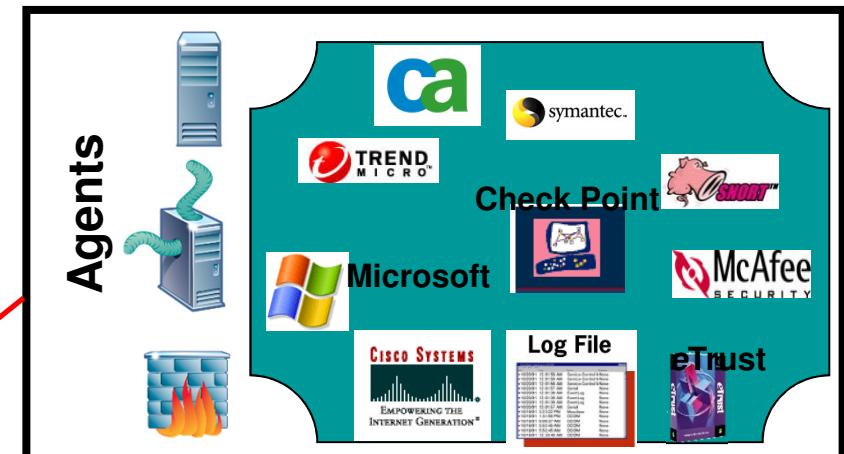
**Security Command Center:
Advanced Correlation, Reporting,
Action and Remediation**



**Event
Management
System**

**Step 2: Local
Reduction/Correlation of Security
Events (Hundreds)**

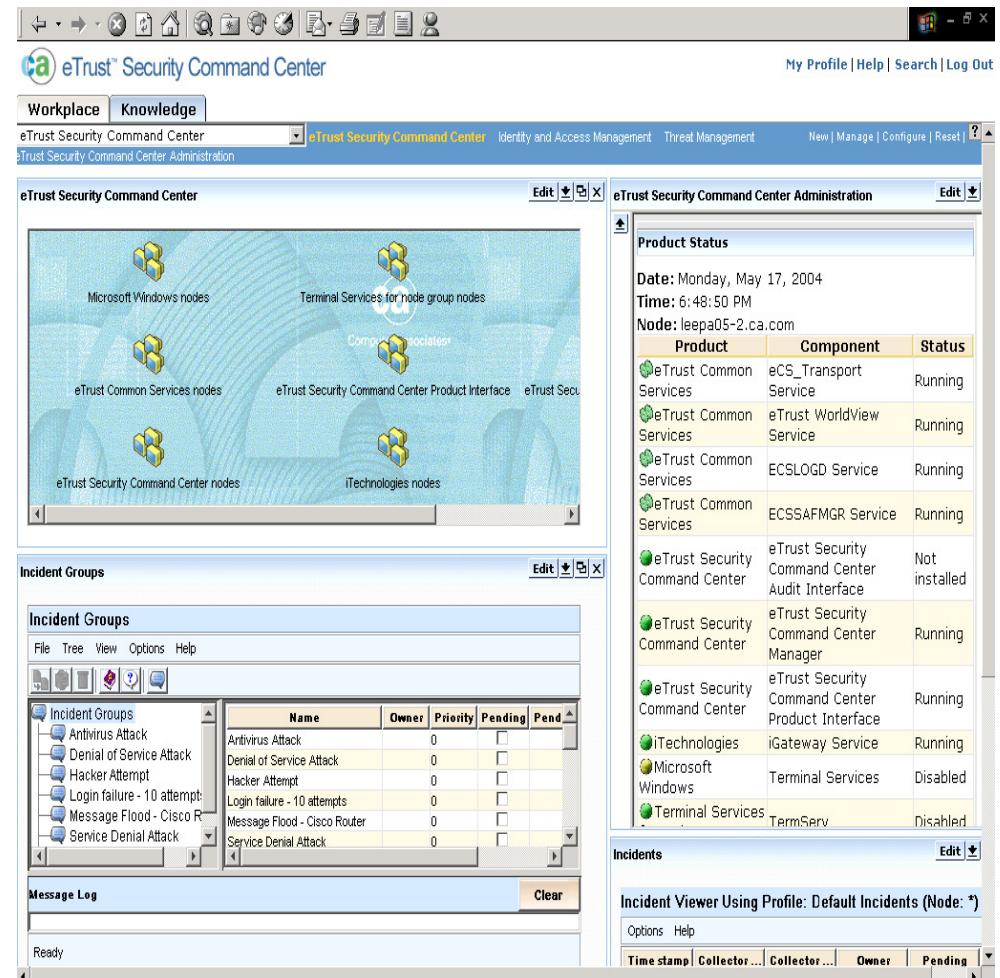
**Step 1: Local
Collection of Security Events (Millions)**



© Computer Associates

Collection of Relevant Data

- Collection of events, traps, reports, status messages from a large number of sources.
- Prioritisation.
- First assessment of system and application security and availability status, possibly selection and execution of immediate measures.



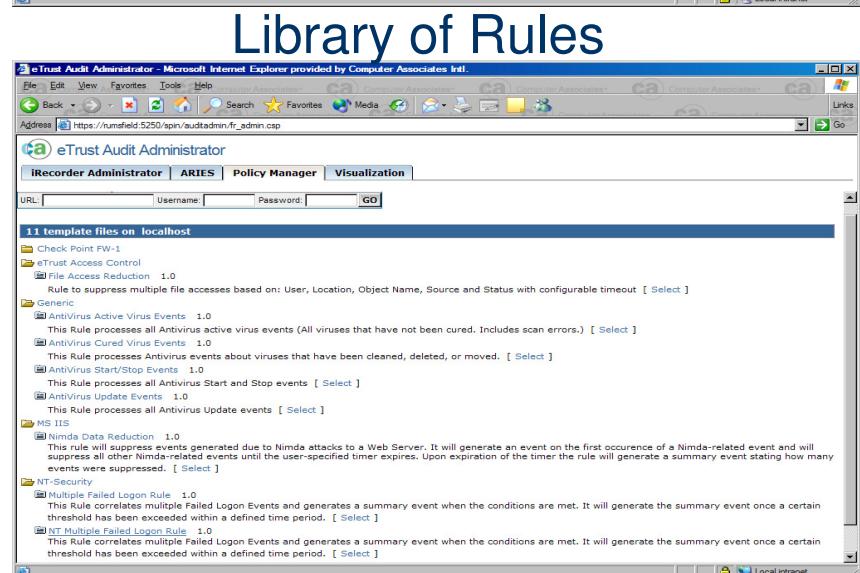
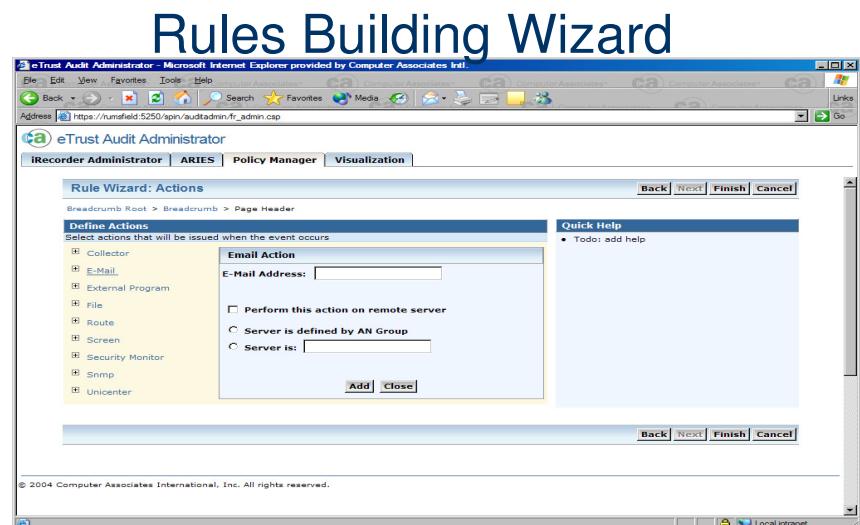
© Computer Associates

Normalisation and Plausibility Check

- Synchronised system clocks
- Normalisation of character sets, syntax etc.
- Detection and filtering of duplicates
- Filtering of “similar” messages
- Evaluate plausibility of events

Correlation and Assessment

- Library of pre-defined correlation rules.
- Templates and wizards for creating / modifying rules.
- Correlation across technologies and vendors.
- Asset-based correlation with known vulnerabilities.
- Prioritisation of security-relevant events based on pre-defined priority classes.



© Computer Associates

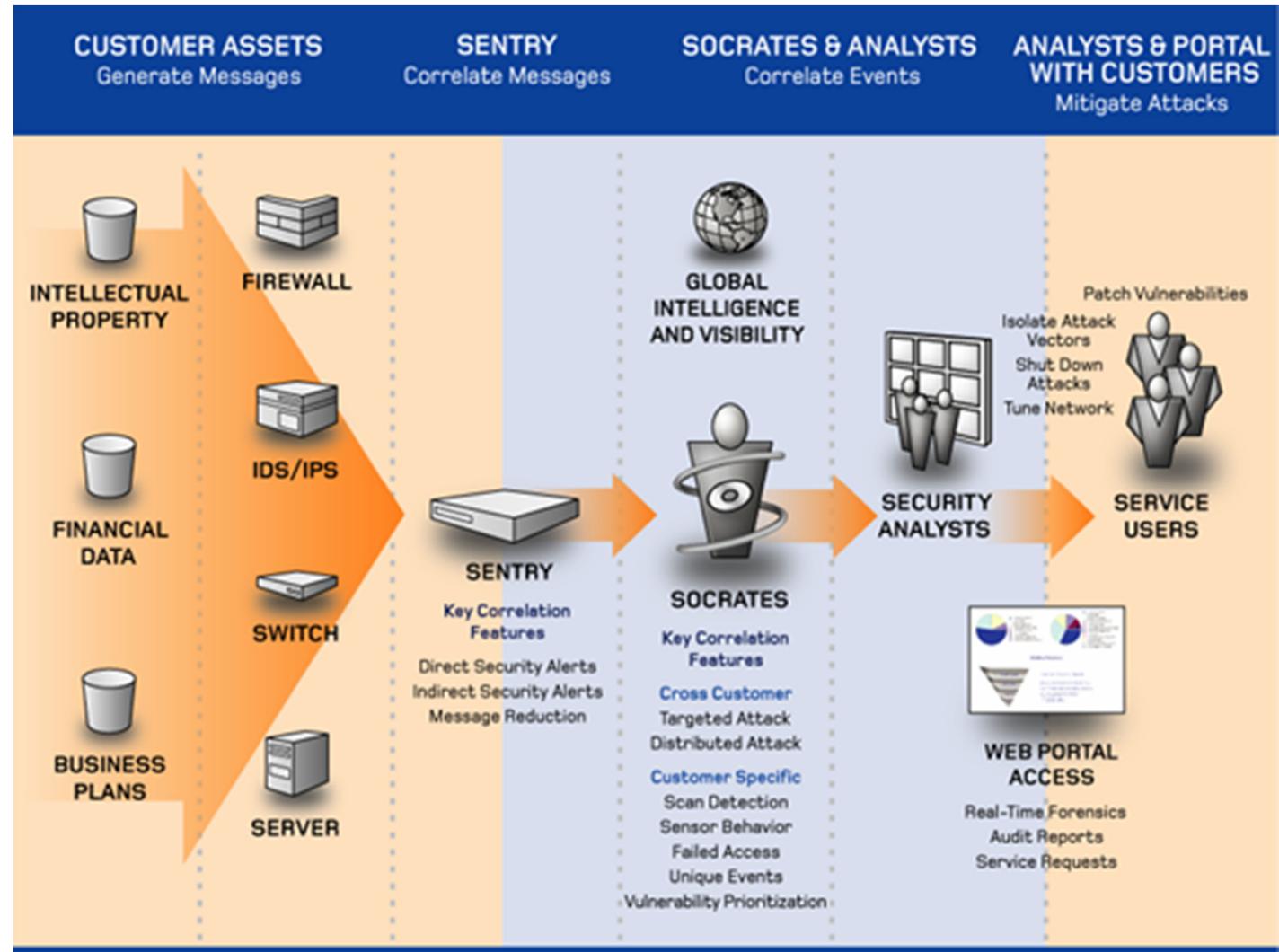
Monitoring, Reporting, Alarming, Escalation

- Pre-defined reports for different types of recipients.
- Real-time display and reporting of security and compliance status.
- Adaptable reports, based on role or function, but still connected to data.
- Incident management, based on workflows and best practices.
- Automatic or manual execution of countermeasures (via vulnerability management, patch- and configuration management, helpdesk, trouble ticketing etc).
- Linking of security activities with (ITIL) processes and workflows (change mgmt, release mgmt etc).



© Computer Associates

Security Event Monitoring as a Managed Service



Source: BT Counterpane

BT Customer Portal - Windows Internet Explorer

C:\Documents and Settings\{twj\Desktop\Downloads\portal\html\dashboard.html

Microsoft Outlook Web Access BT Customer Portal

Administration Dashboard Device Status Statistics & Reports Search Email Security Service Description - 10.31.2006 : Micro

Dashboard

Firewall Statistics

FW/Cluster Name: trii_chkcp_fw_ng

Last: 3 Hours Edit

	IP/Port	Quantity
Top Destination IP	205.115.3.2	6,000
Top Destination Port	80	5,000
Top Source IP	115.80.72.10	1,000
Top Source Port	80	500
Top Source-Destination IP pairs	25.15.3.0	10,000
Top Source-Destination Port pairs	192.168.1.24	5,577
Top Destination/IP Port	172.16.40.236	5,000
Top Source IP/Port	5.115.3.1/321	467
All Traffic	5.115.3.1	345

Ticket Statistics

Last: 3 Hours Edit

Tickets Awaiting Customer Acknowledgement: 15

FusionCharts Evaluation - An InfoSoft Global Creation
Tickets Generated in 3 Hours

Time	Critical	Suspicious	Relevant	Period Mean
Current	2	8	28	35
9AM	2	8	28	42
6AM	2	8	28	45
3AM	2	8	28	32
12AM	2	8	28	28
9PM	2	8	28	38
6PM	2	8	28	40
3PM	2	8	28	45
12PM	2	8	28	18

FusionCharts Evaluation - An InfoSoft Global Creation
Vulnerability Scan Results

Date	Critical	High	Medium	Low
02-16	2	8	12	24
02-15	2	8	12	16
02-08	2	8	12	24
02-07	2	8	12	28
02-06	2	8	12	28

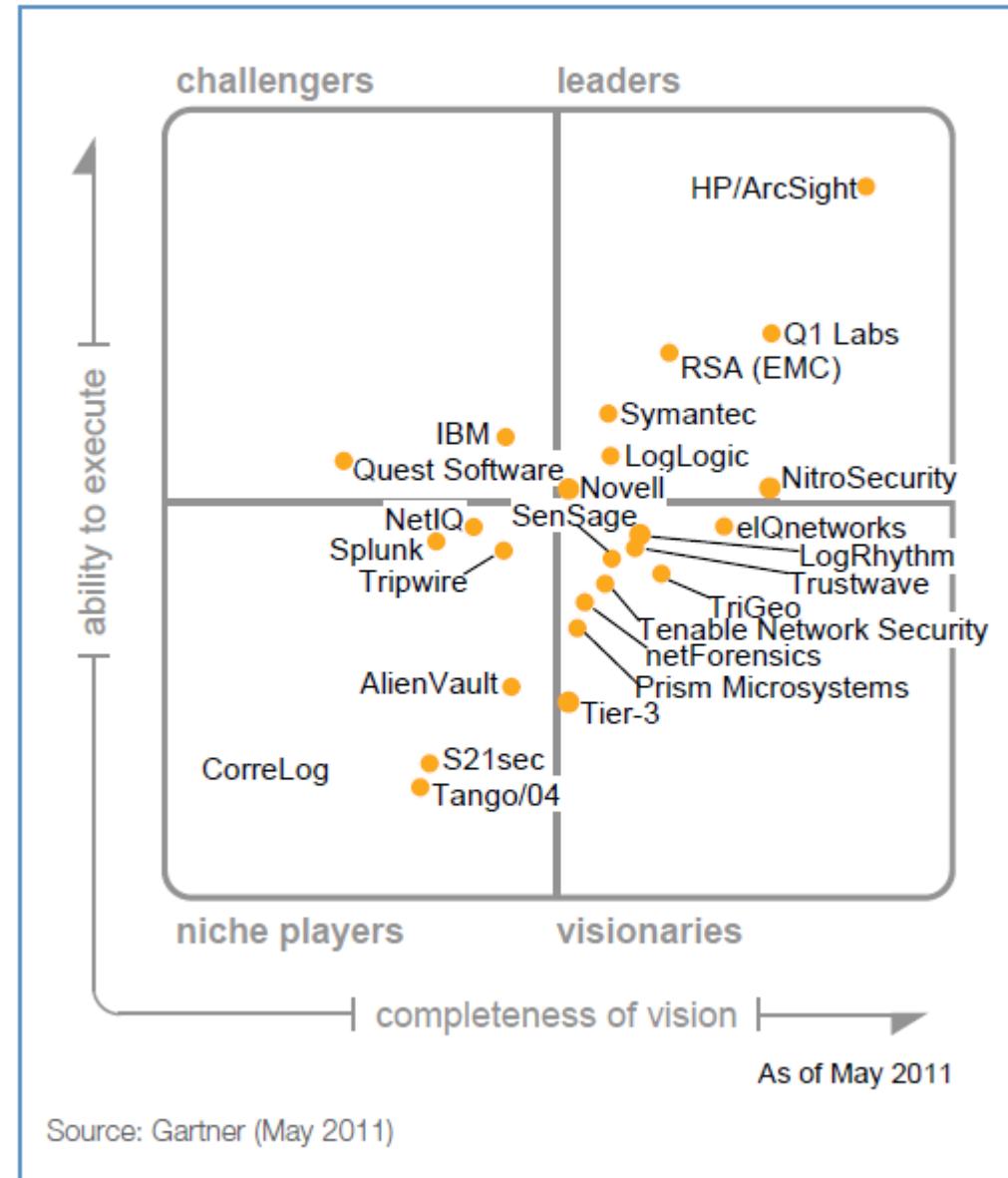
Top 10 Vulnerable Hosts

FusionCharts Evaluation - An InfoSoft Global Creation
Top 10 Most Vulnerable Hosts

Host	Critical	High	Medium	Low	Mean of last 10 scans
92.168.10.14	2	2	18	38	45
192.168.12.5	2	2	18	38	42
10.10.5.3	2	2	18	38	12
205.73.16.23	2	2	18	38	48
205.73.10.6	2	2	18	38	24
205.73.10.7	2	2	18	38	2
10.10.5.7	2	2	18	38	12
192.168.15.10	2	2	18	38	24
205.73.15.50	2	2	18	38	12
205.73.15.91	2	2	18	38	12

Market Overview (Gartner Quadrant)

Magic Quadrant for Security Information and Event Management



Pause

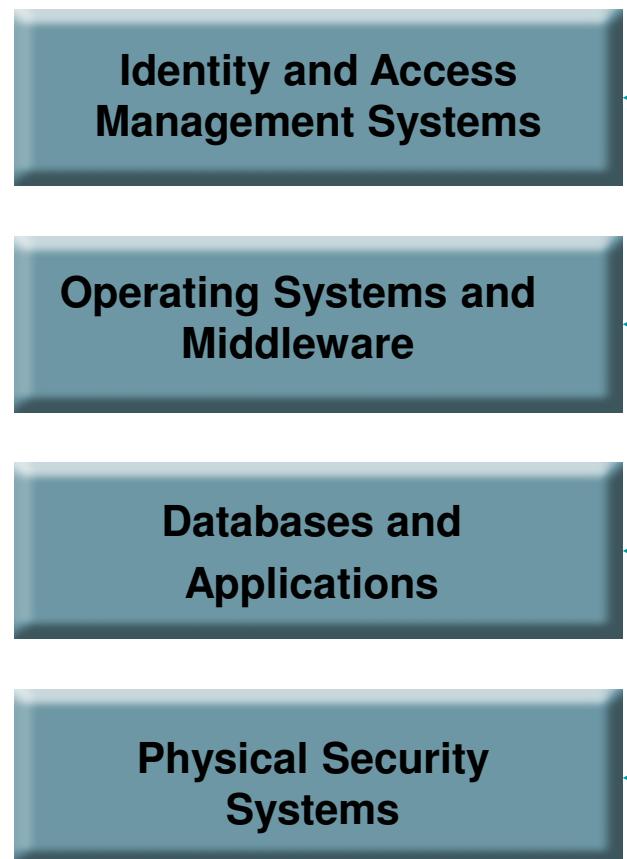


Interfaces with other IT Management Systems

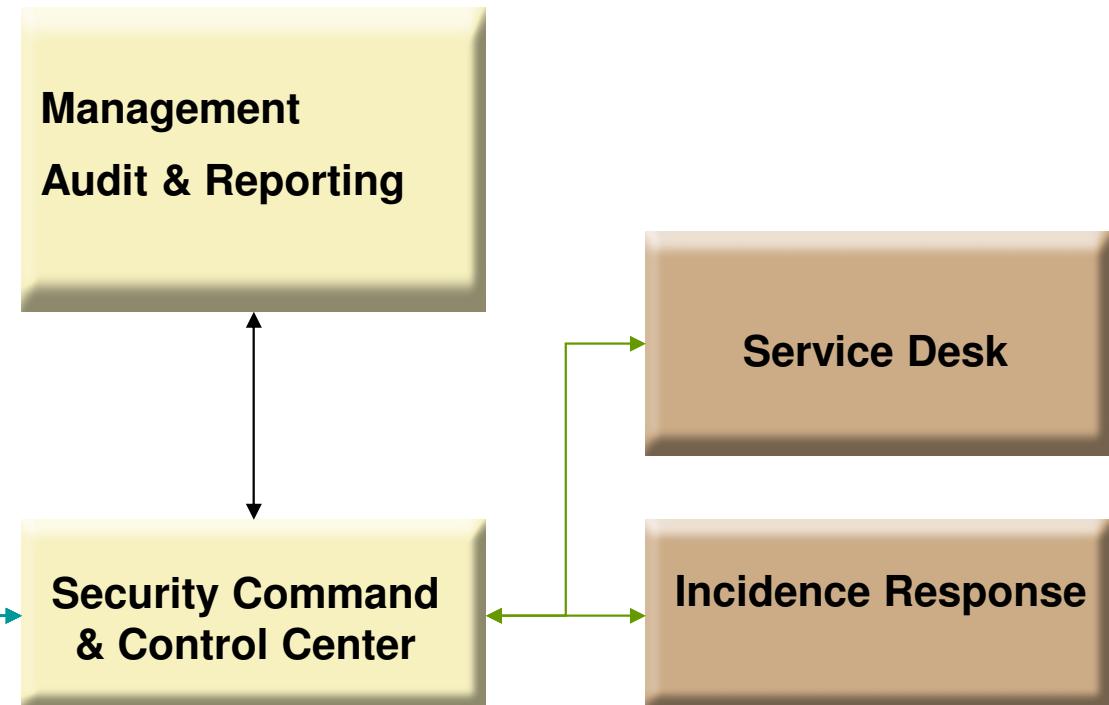


From Security Data to Information

Security Data



Security Information



Value of Mgmt Information Integration

- Quickly respond to security events
 - Network Operation Centers leverage network activity in addition to the real-time security event data to avert security incidents
 - Security Operation Centers similarly leverage network activity related to security events to further refine the identification of a specific security event
 - SOCs can expedite resolution of events through integration with the help desk systems
- Enables communication
 - Provides one central console for network and security situational awareness
 - Enables effective communication between network and security teams

Example Management Command Center

Management Command Center

Business Process Views

- WorldView
 - ENGMI02NET1
 - ENGMI02XP
 - FOXGR01-TECRA
 - Database
 - Ingres
 - MS SQL Server
 - 138.42.185.101
 - 138.42.185.111
 - 138.42.185.114
 - Oracle
 - 138.42.185.117
 - 138.42.185.118
 - Domain
 - Finance
 - 138.42.197.115
 - Ingres
 - MS SQL Server
 - Oracle
 - Payroll
 - 138.42.197.122
 - 138.42.197.125
 - Printers
 - Finance
 - 138.42.197.115
 - Payroll
 - 138.42.197.122
 - 138.42.197.125
 - Shop Floor
 - 138.42.197.119
 - Warehouse
 - 138.42.197.12
 - WBEM
 - Web Management

Unicenter - Network and Systems Management Alerts

Idle	Age	Origin	Text	Details
25	25	USSDTND	Agent Exception	Host:Windows2000_Server Windows2000_Server caIW2kOs Trap Agent:caIW2kOs:w2kNe
25	25	USSDTND	Agent Exception	Host:Windows2000_Server Windows2000_Server caIW2kOs Trap Agent:caIW2kOs:w2kNe
25	25	USSDTND	Agent Exception	Host:Windows2000_Server Windows2000_Server caIW2kOs Trap Agent:caIW2kOs:w2kNe
25	25	USSDTND	Agent Exception	Host:Windows2000_Server Windows2000_Server caIW2kOs Trap Agent:caIW2kOs:w2kNe
25	25	USSDTND	Agent Exception	Host:Windows2000_Server Windows2000_Server caIW2kOs Trap Agent:caIW2kOs:w2kNe
25	25	USSDTND	Agent Exception	Host:Windows2000_Server Windows2000_Server caIW2kOs Trap Agent:caIW2kOs:w2kNe

eTrust - Security Alerts

Idle	Age	Origin	Text	Details
8418	8418	WORKGROUP\USSDTND	eTrust Compromise	eSCCCompromise MyDoom detected on node maruv99
8418	8418	WORKGROUP\USSDTND	eTrust Exploit Detected	eSCCExploit Nimda worm detected on node harde01
8408	8408	WORKGROUP\USSDTND	eTrust Compromise	eSCCCompromise MyDoom detected on node maruv99
8408	8408	WORKGROUP\USSDTND	eTrust Policy Violation	eSCCPolicyViol AV Policy Violation on node ferti01. Version out of date. Notification sent via
8407	8407	WORKGROUP\USSDTND	eTrust Policy Violation	eSCCPolicyViol AV Policy Violation on node ferti01. Version out of date. Notification sent via

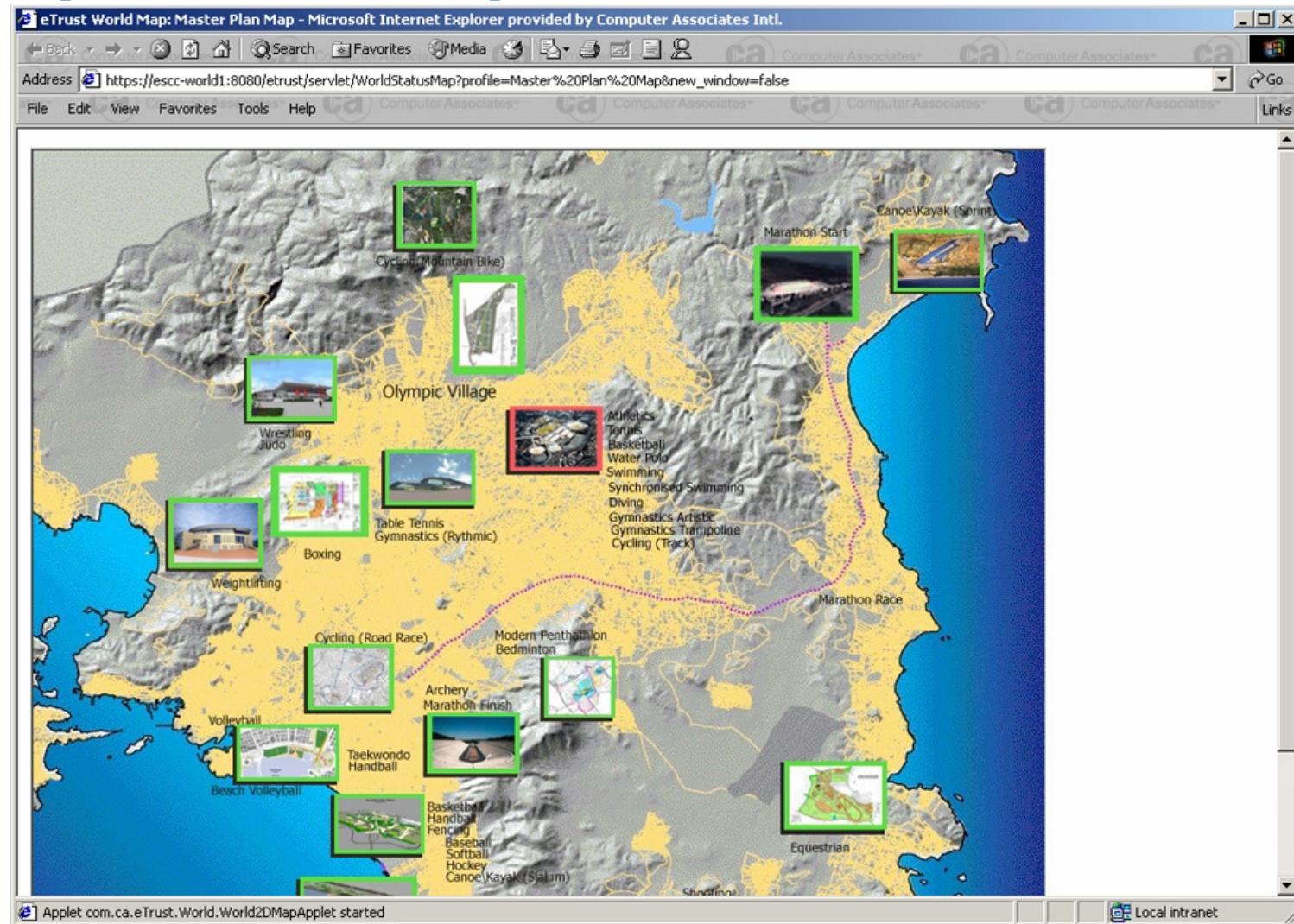
BrightStor - Storage Alerts

Idle	Age	Origin	Text	Details
52	52	WORKGROUP\USSDTND	ARCserve Exception	Backup ** Operation failed - Media Error. **
46	46	WORKGROUP\USSDTND	ARCserve Exception	Backup ** Failed to write to media. **
46	46	WORKGROUP\USSDTND	ARCserve Exception	Backup ** Operation cancelled by OPERATOR**
46	46	WORKGROUP\USSDTND	ARCserve Exception	Backup ** Operation incomplete.**
46	46	WORKGROUP\USSDTND	ARCserve Exception	Backup ** Operation failed - Media Error. **

Unicenter - Service Level Management Alerts

Idle	Age	Origin	Text	Details
51	51	WORKGROUP\USSDTND	Sevice Level Violation	SLA Violation (MS Exchange) - User felan01 has exceeded their mailbox quota on usilms21
45	45	WORKGROUP\USSDTND	Sevice Level Violation	SLA Warning (Netflow Traffic Monitor) - Marketing has exceeded 90 megabytes of HTTP traffic
45	45	WORKGROUP\USSDTND	Sevice Level Violation	SLA Violation (MS Exchange) - User felan01 has exceeded their mailbox quota on usilms21
45	45	WORKGROUP\USSDTND	Sevice Level Violation	SLA Violation (Operating System) - Host usihu28 availability is less than 99.5%
45	45	WORKGROUP\USSDTND	Sevice Level Violation	SLA Violation (Web Services) - The average GoogleSearch:doGoogleSearch response time

Graphical Example



© Computer Associates



Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Forensic Analysis



Definitions

- "*Computer forensics is the scientific examination and analysis of data held on, or retrieved from, computer storage media in such a way that the information can be used as evidence in a court of law.*" (DIBS USA Inc)
- Network forensics is the real-time and „post mortem“ examination and analysis of data transmitted via networks such that the data content or data flow patterns can be used either as evidence in a court of law, or as input for security / network management and operation.

Collecting Evidence

- ➲ Make Exact copies of all hard drives & disks using computer software
 - ⇒ Date and Time stamped on each file; used for timeline
- ➲ Protect the Computer system
 - ⇒ Avoid deletion, damage, viruses and corruption
- ➲ Discover files
 - ⇒ Normal Files
 - ⇒ Deleted Files
 - ⇒ Password Protected Files
 - ⇒ Hidden Files
 - ⇒ Encrypted Files
- ➲ Reveal all contents of hidden files used by application and operating system
- ➲ Access contents of password protected files if legally able to do so
- ➲ Analyze data
- ➲ Print out analysis
 - ⇒ Computer System
 - ⇒ All Files and data
 - ⇒ Overall opinion
- ➲ Provide expert consultation/testimony

How Evidence is Protected

A Computer Forensic Specialist promises to:

- Not delete, damage or alter any evidence
- Protect the computer and files against a virus
- Handle all evidence properly to prevent any future damage
- Keep a log of all work done and by whom
- Keep any Client-Attorney information that is gained confidential

Risks of Computer Forensics



- Digital evidence accepted into court
 - ⇒ must prove that there is no tampering
 - ⇒ all evidence must be fully accounted for
 - ⇒ computer forensic specialists must have complete knowledge of legal requirements, evidence handling and storage and documentation procedures

Risks of Computer Forensics



Costs

⇒ producing electronic records & preserving them is extremely costly



Presents the potential for exposing privileged documents



Legal practitioners must have extensive computer knowledge

How Computer Forensics is Used



Criminal Prosecutors

- ⇒ Child Pornography cases
 - Michael Jackson Case
- ⇒ Homicides
 - Scott Peterson Trial
- ⇒ Embezzlement
 - John Gotti, Bugsy Siegal
- ⇒ Financial Fraud
 - ENRON



Civil Litigations

- ⇒ Fraud
- ⇒ Divorce
- ⇒ Breach of Contract
- ⇒ Copy right



Insurance Companies

- ⇒ False Accident Reports
- ⇒ Workman's Compensation Cases



Large Corporations

- ⇒ Embezzlement
- ⇒ Insider Trading
 - Martha Stewart Case



Law Enforcement

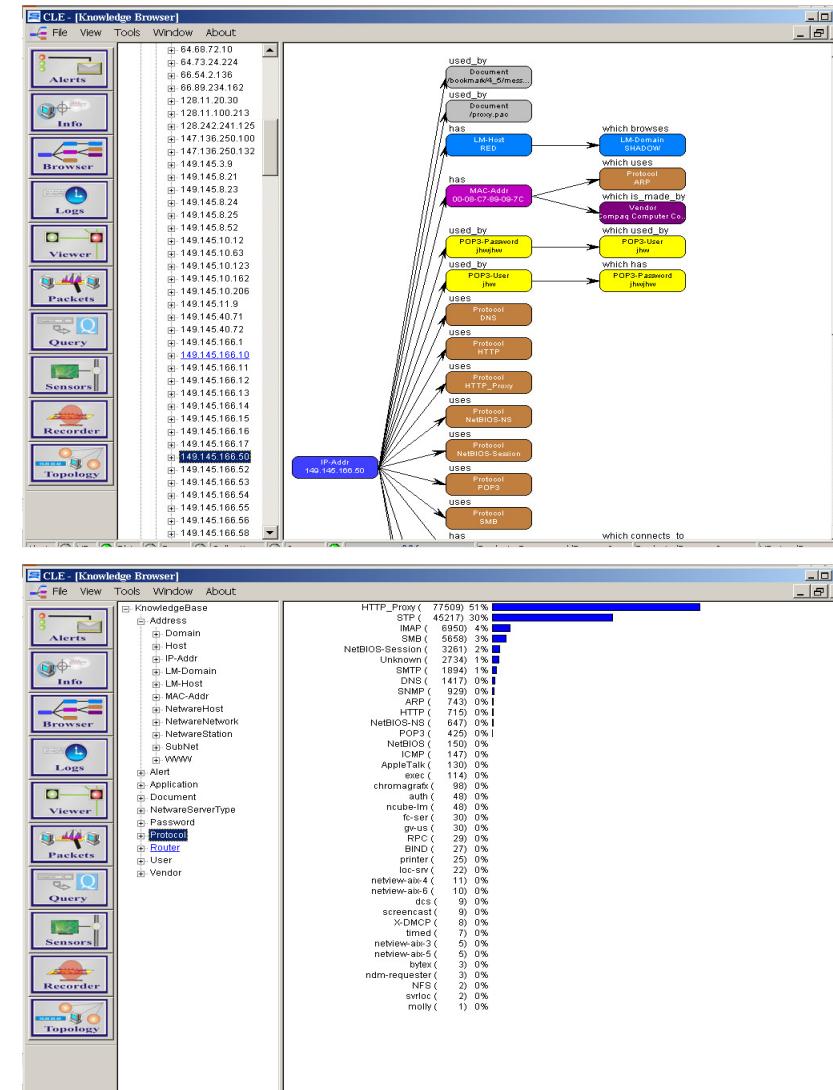


Any Individual

- ⇒ Claims
 - Sexual harassment
 - Age discrimination
 - Wrongful termination from job
 - Background checks

Example: CA Network Forensics Collector: Knowledge Base

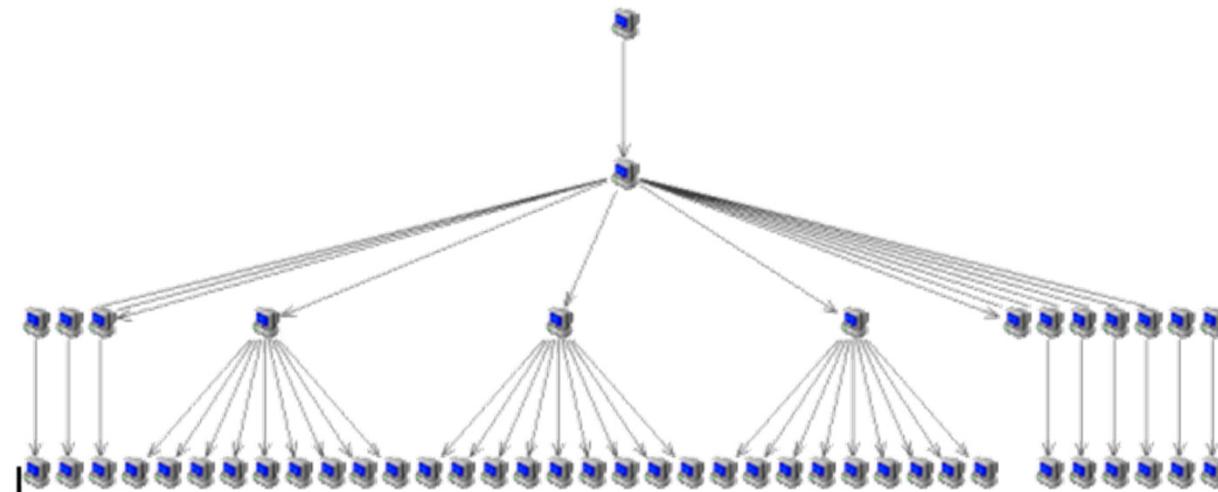
- Allows rapid identification of relationships between users, network resources, protocols etc.
- Allows pre-defined analysis of > 1500 protocols and services. Other protocols and services can be added on request.

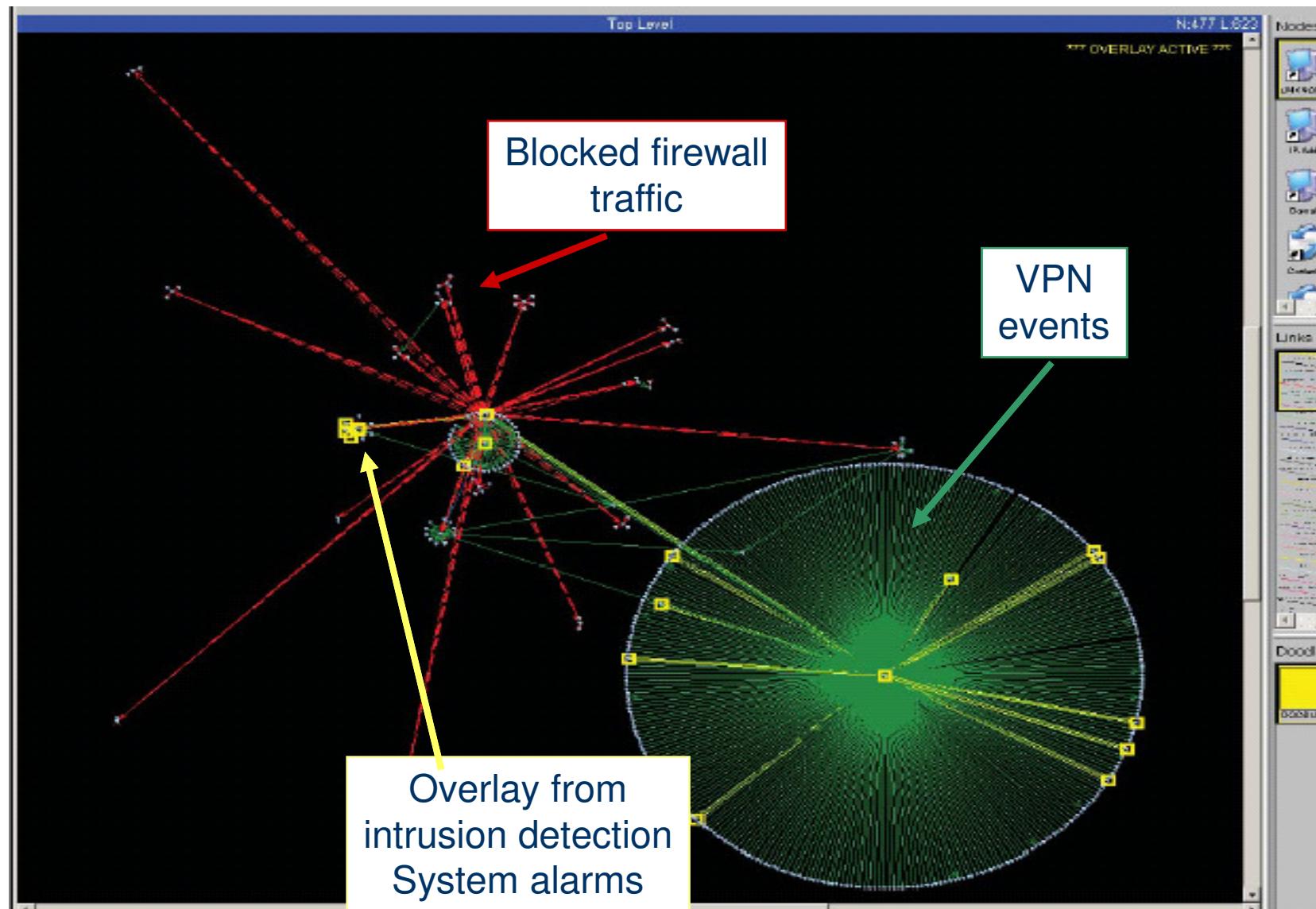


Example: CA Network Forensics

Analysis: Data Propagation

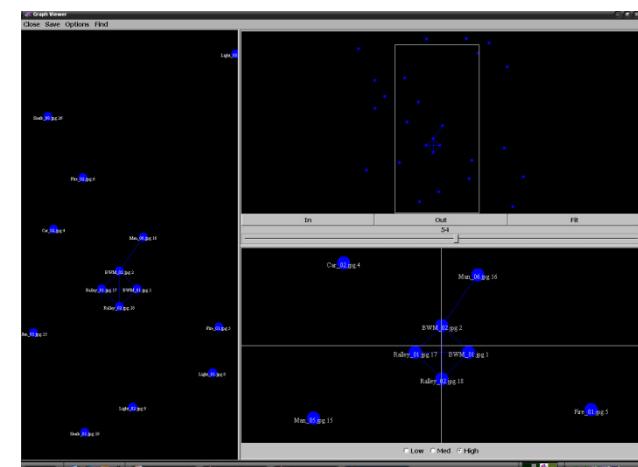
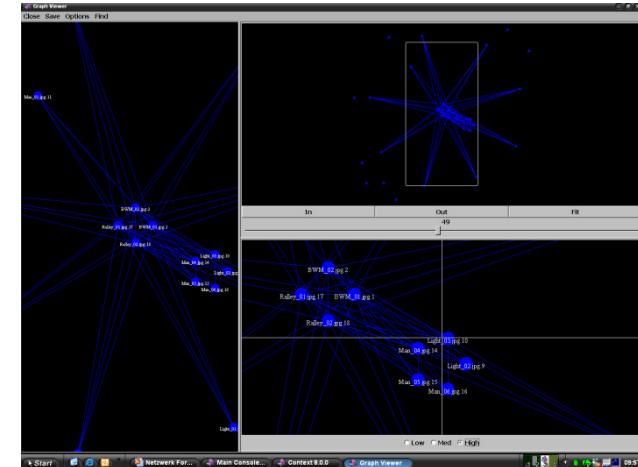
- Different dependency tree display algorithms and sorting keys, depending on preference of user (volume, flow direction, timing etc)





Example: CA Network Forensics: Context Management

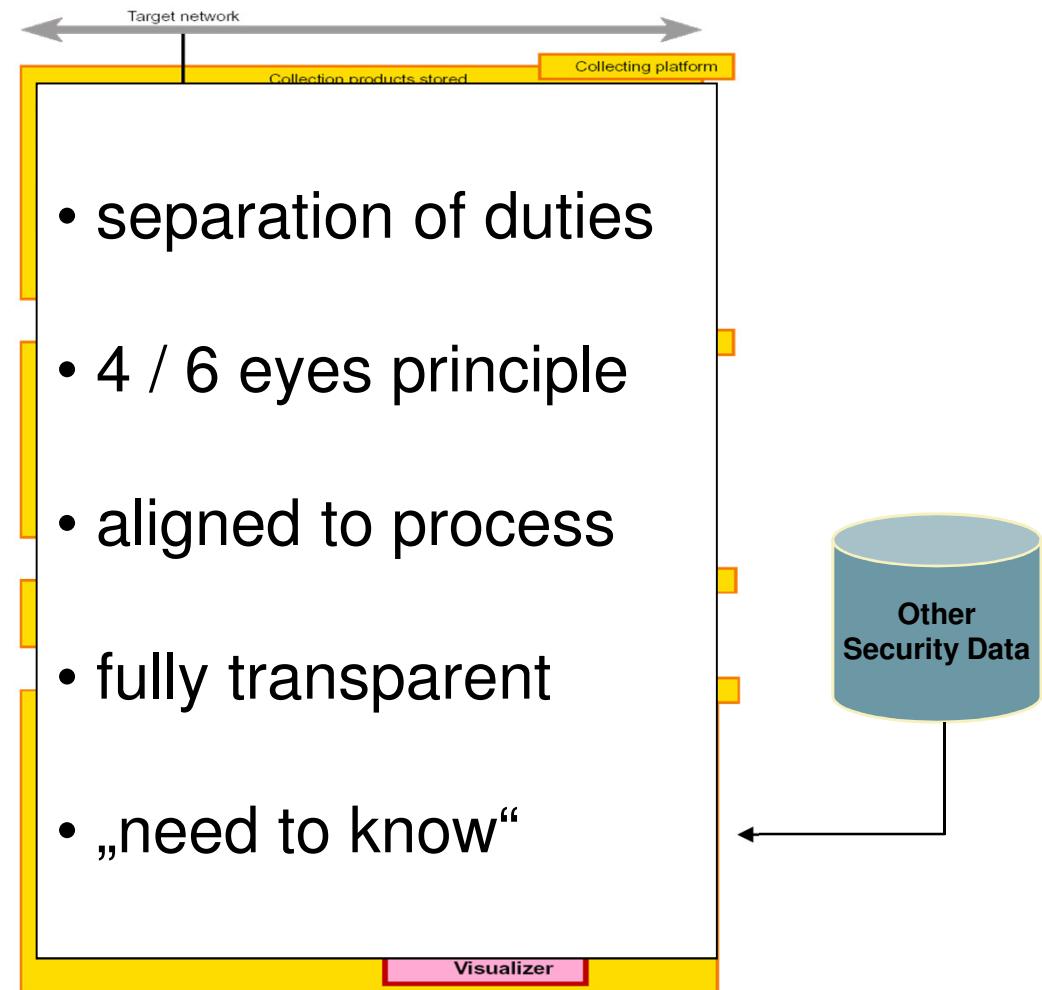
- Context management allows the graphical content analysis based on n-gram similarity.
- Data formats do not matter, thus data can be followed even if the format changes.
- Similar data is grouped into clusters.
- Similarity threshold levels can be modified interactively.
- Capability for keyword and proximity searches.



© Computer Associates

Example: CA Network Forensics: Operational Aspects

- Collector/Forwarder →
- Loader →
- Central Repository →
- Analysis Station →



© Computer Associates



Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

The Big Picture

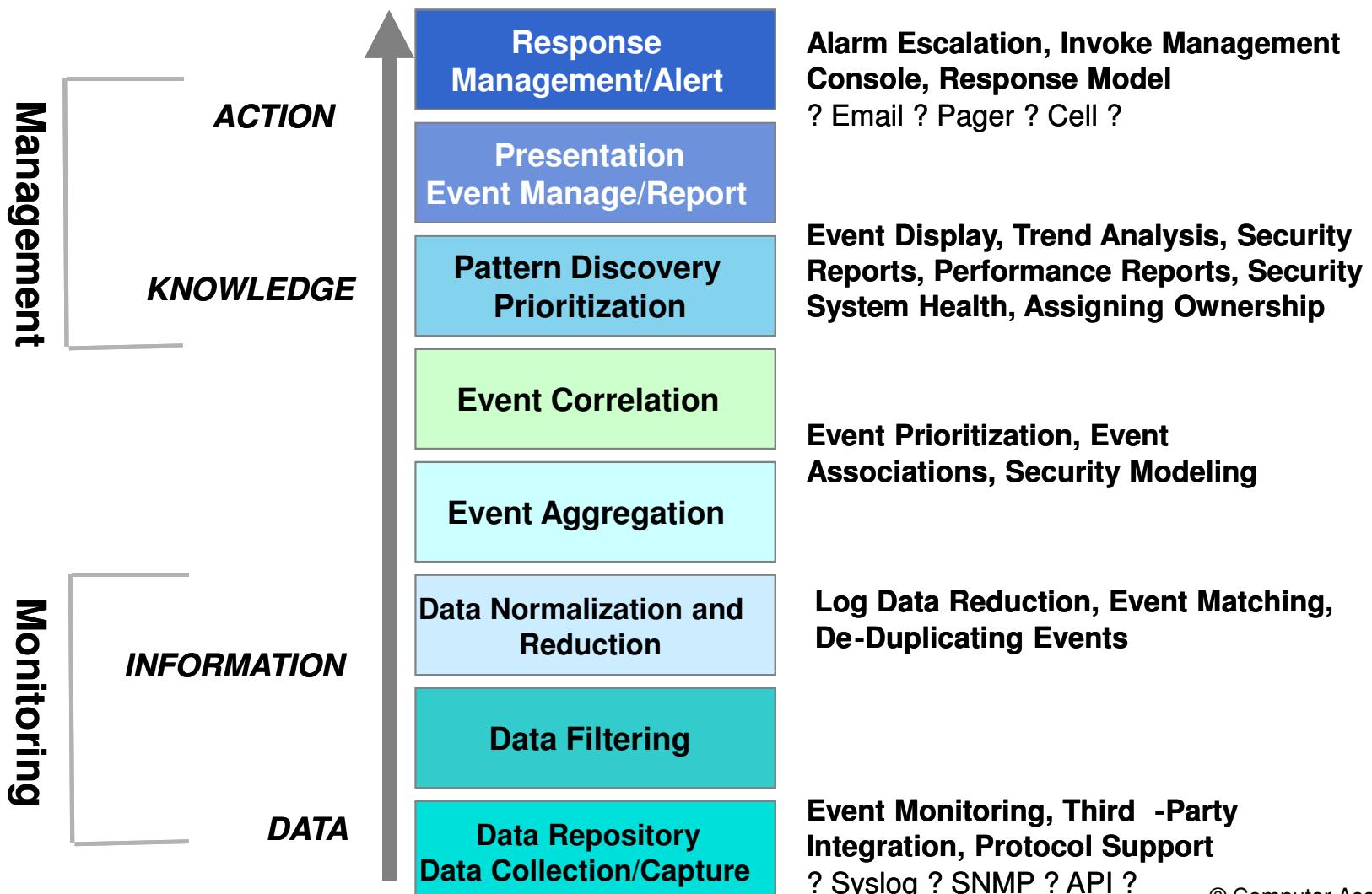




Unified System, Network and Security Monitoring

- Knowing what you have („real time“ IT asset inventory)
- Knowing what state all assets are in (release, patch level)
- Defining who is who (identity management) and who is allowed to do what (policy setting / role-based access)
- Knowing who does / has done what (access mgmt, logs)
- Knowing what is currently going on internally / externally (security information management, event correlation etc.)
- Being able to (re)-act (security/risk mgmt team, incident handling, damage containment, crisis management, emergency planning etc)
- Being able to identify / prove what has happened and why (forensics, reporting, auditing etc)

Security Information Mgmt Readiness



Summary – Take Home Message

- Security Information Management is a technical and procedural means to deal with security event data overflow.
- Security information management is only as good as the correlation rules and associated processes.
- Security information can be enhanced by other sources (e.g. forensic data or physical security).
- Correlated security information provides input for associated IT management systems (helpdesk, incident management, release planning etc).

Cost / Benefit Analysis of IT Security

Risk and Security Management – HS 2012

PD Dr. Hannes P. Lubich



Motivation

Stay in bed

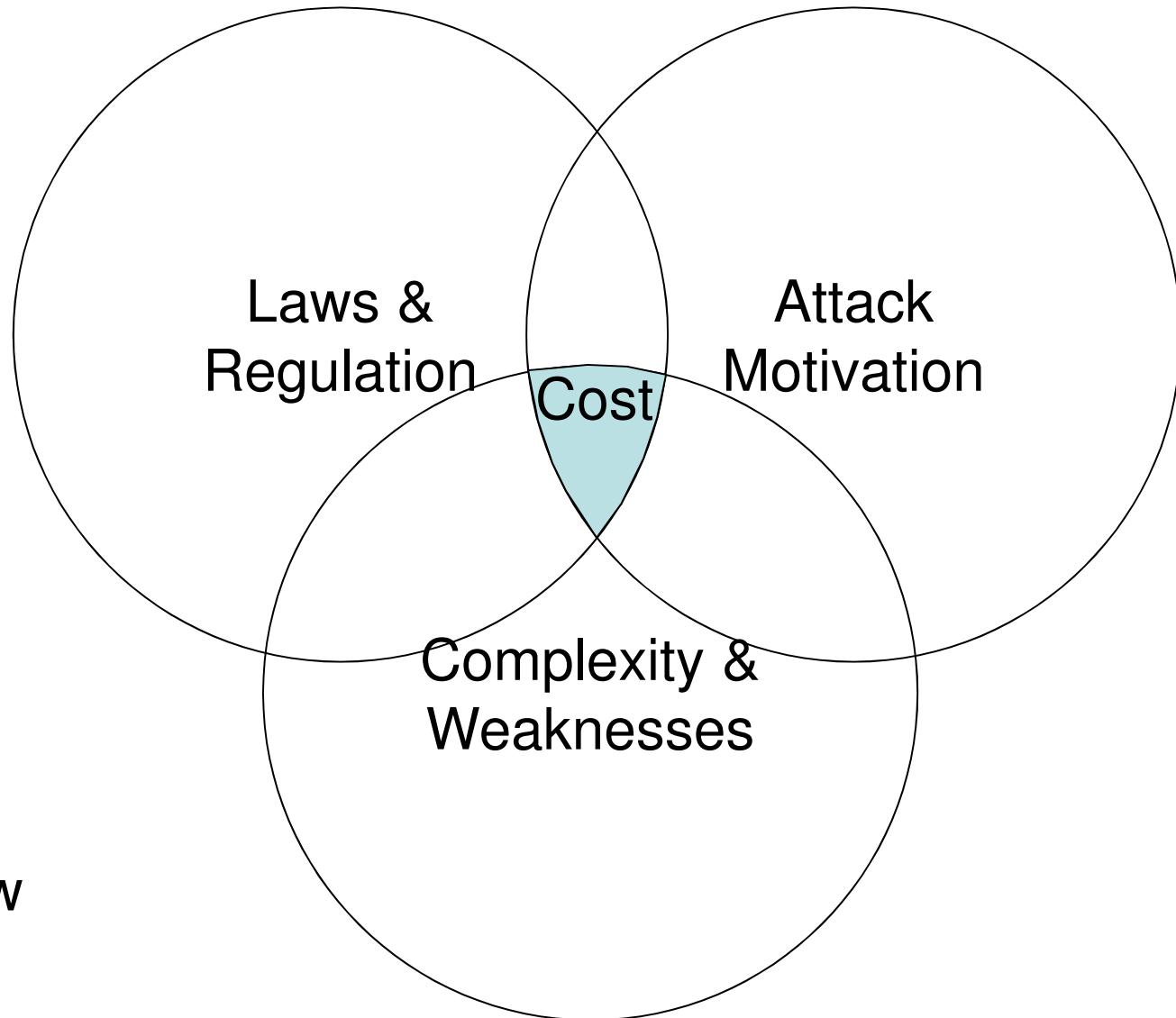
Buy insurance

Blame it on
someone else

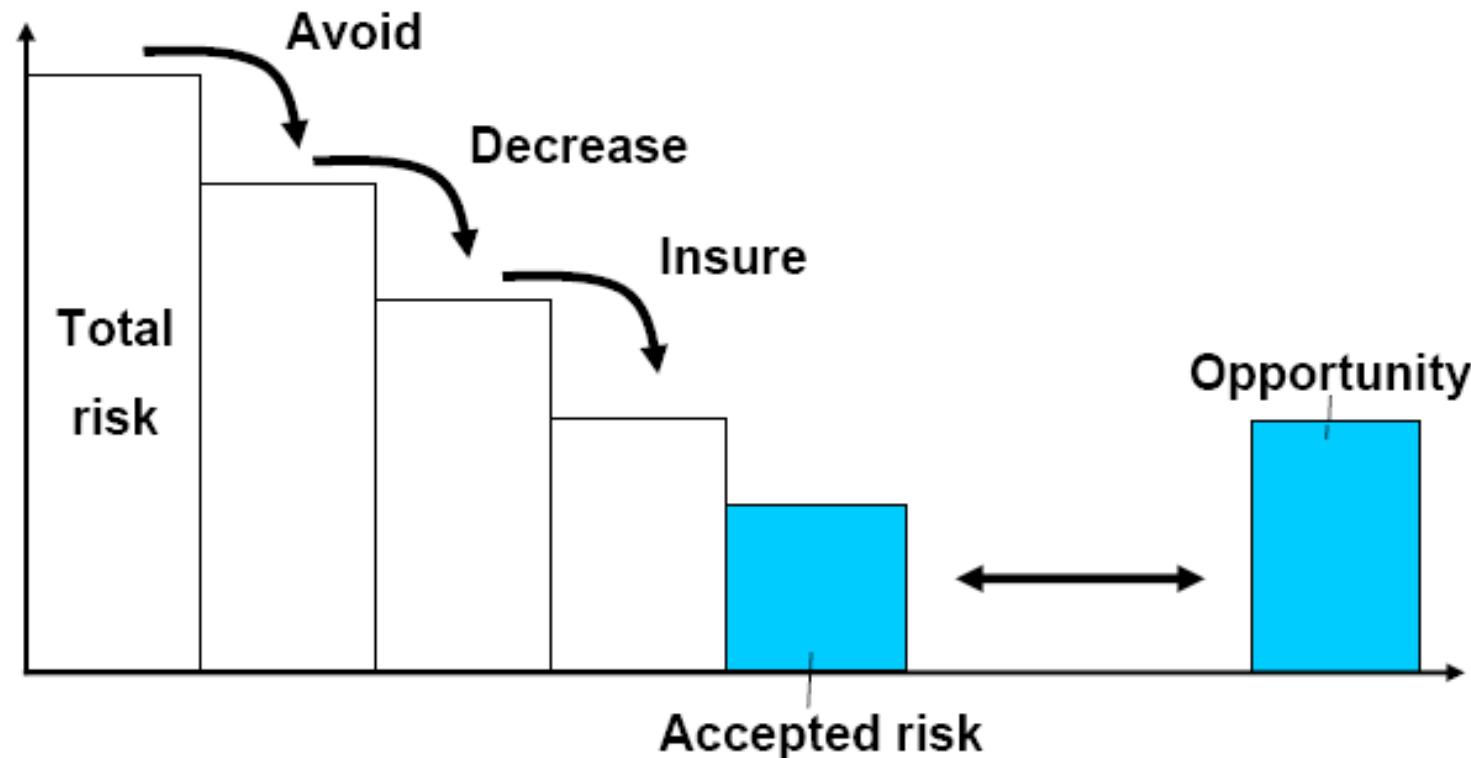
Face it

Ignore it

Reduce it (but how
much is enough?)

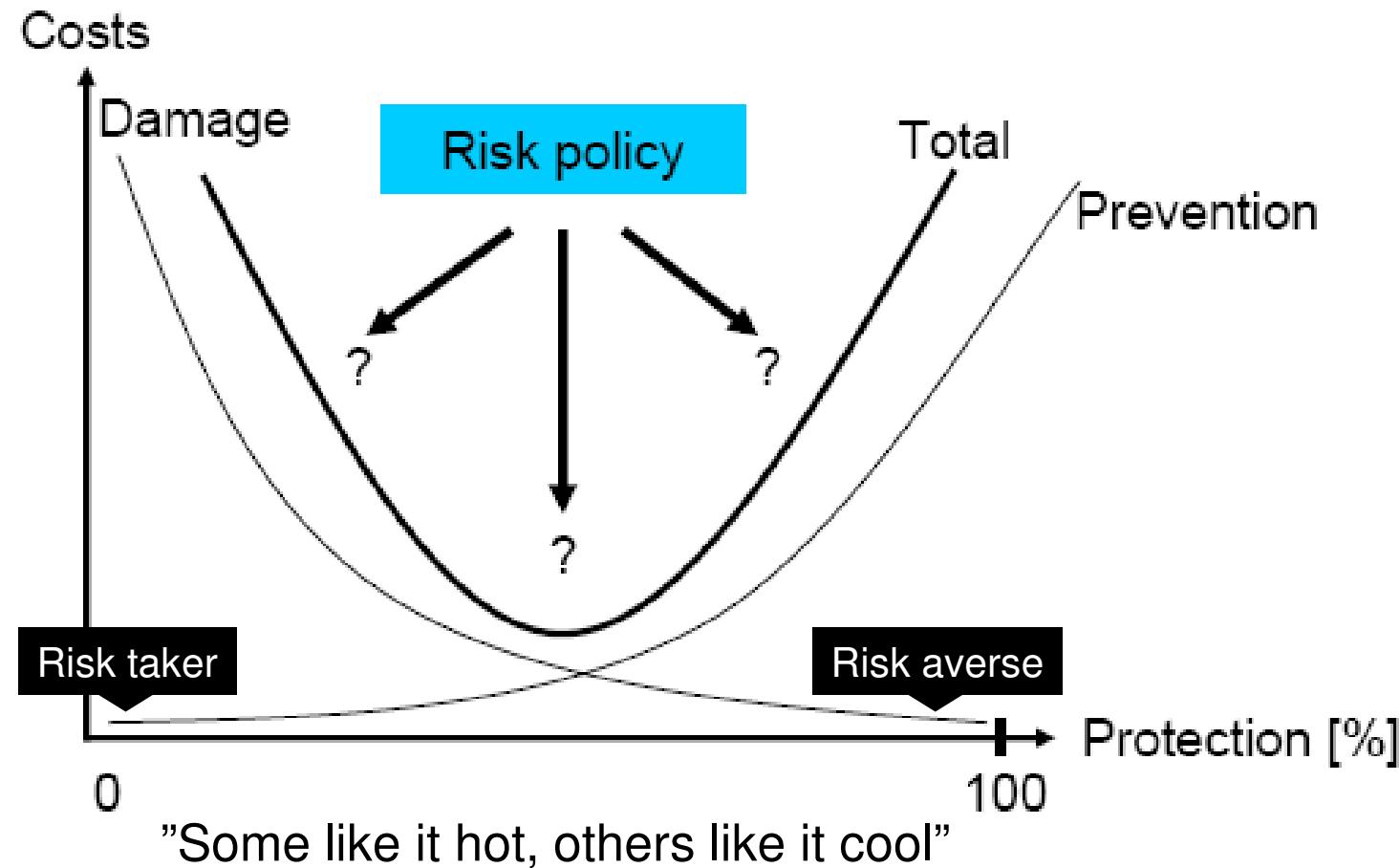


Cost / Benefit is NOT a Yes/No Decision



Source: ETH D-MTEC R. Boutelier

Cost Manifestations



Source: ETH D-MTEC R. Boutelier

Outline

- Cost Drivers of IT Security
- Benefits of IT Security
- Cost Estimations for IT Security
- Dealing with Cost
 - Cost reduction
 - Cost justification

Cost Drivers of IT Security





Information Security: Preventive Cost

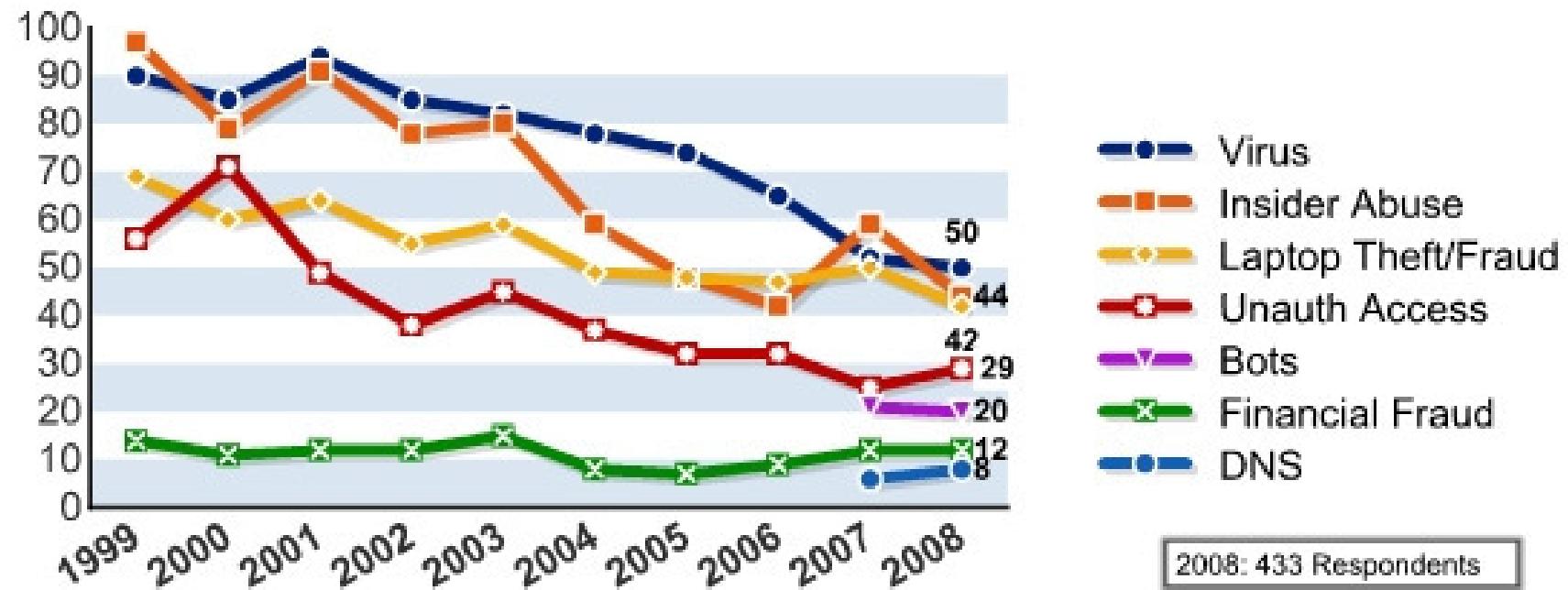
- Recruiting, operating and maintaining a standing security organisation
- IT Governance: creating, maintaining and publishing security guiding principles, best practices, checklists etc.
- Supervising and consulting all projects, procurements, locations etc w.r.t. IT Security, and resulting technical, operational and organisational efforts
- Awareness: education of new hires, periodical refresher courses, distribution of corresponding awareness materials
- Insurance against damages through attacks on IT systems, data feeds etc, potentially including indirect damages (claims by customers, loss of business opportunities etc)

Information Security: Retrospective Cost I

- Annual *FBI and Computer Security Institute Survey* (> 500 US companies). 2/3 of all companies queried report security incidents with direct financial damage of several hundred mio USD.
- Main security problems:
 - viruses
 - Unauthorised access to information by insiders
 - Data theft (i.e. criminal activities)

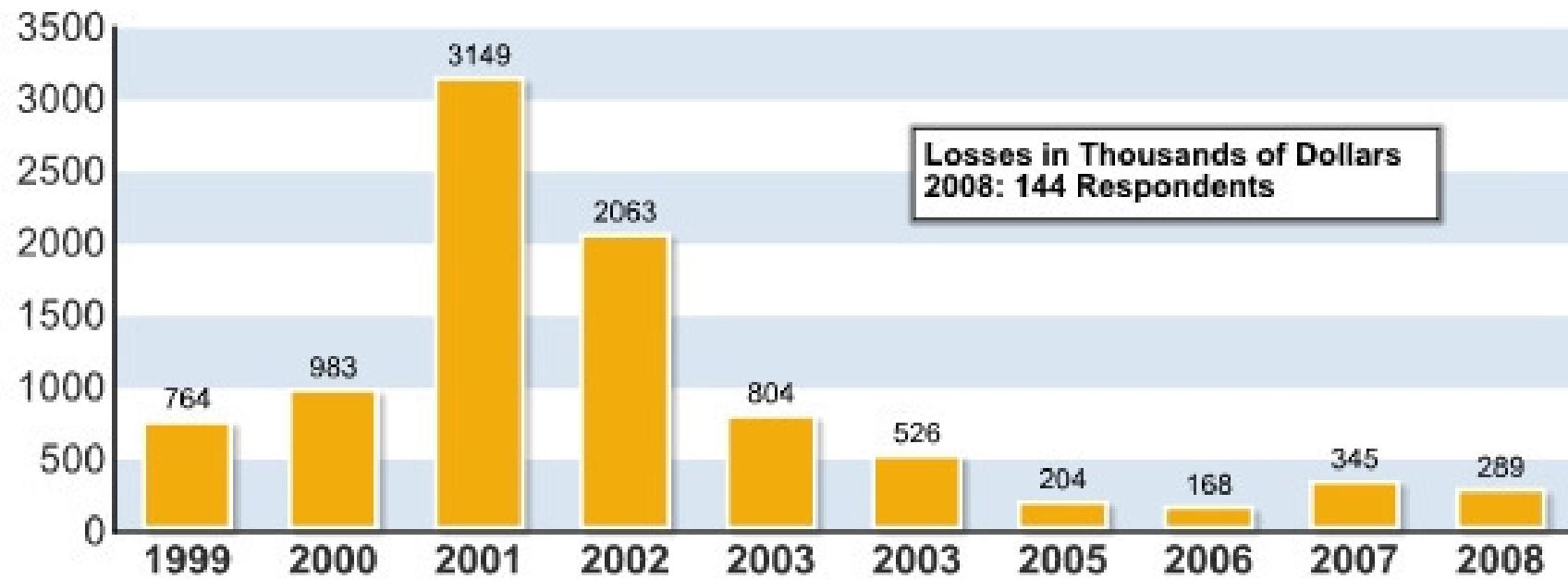
CSI / FBI Survey 2008 (latest free issue)

Figure 13: Percentages of Key Types of Incident



CSI / FBI Survey 2008 (latest free issue)

Figure 14: Average Losses Per Respondent



Information Security: Retrospective Cost II

- June 2002 study of the *British Department of Trade and Industry and PriceWaterhouseCoopers*: average damage through IT Security incidents throughout the British industry in 2001 was ca. 30'000 £, ca. 4 % of all cases reported damages over 500'000 £. In small companies, 32 % of all security violations are internal, in medium and large companies, internal causes amount for less than 50 % of all known cases.
- Large uncertainty w.r.t. numbers, due to problem ignorance or attempts to cover up errors.

Do we Know the Cost?

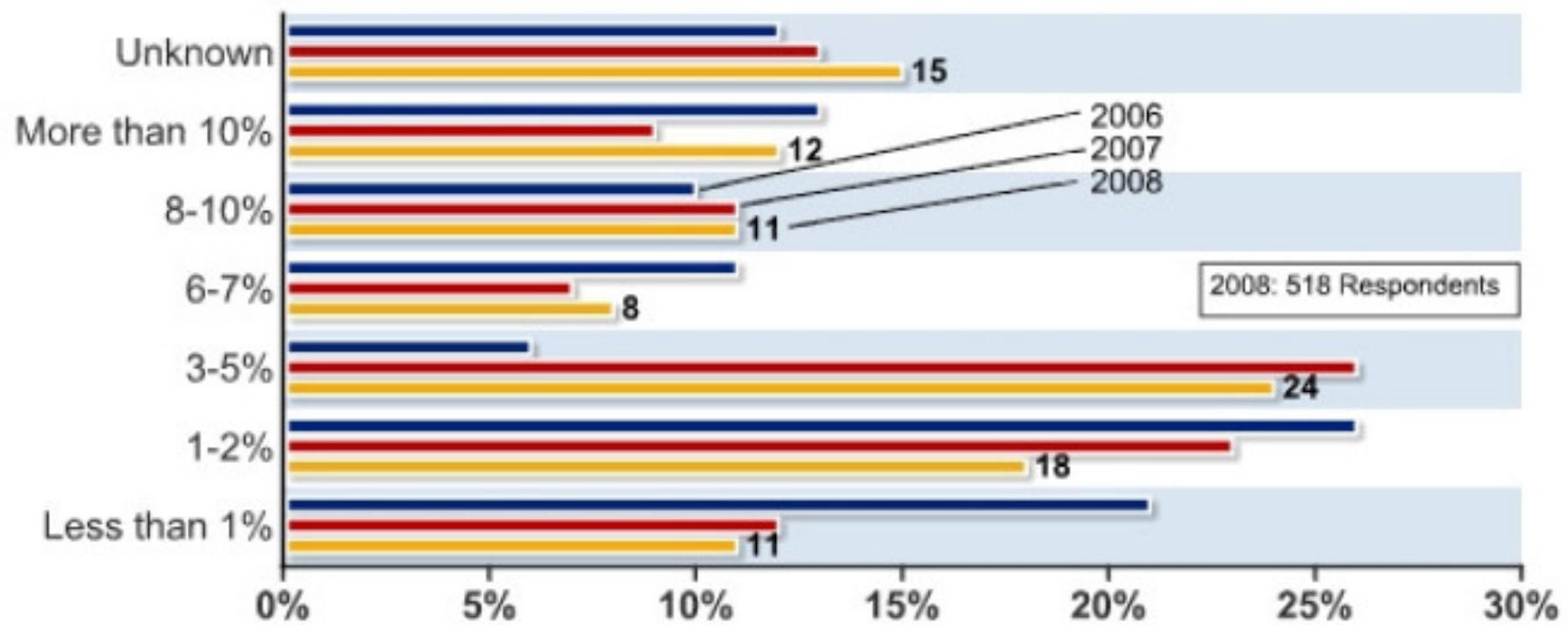
Incident Category	< \$100'000 in %	\$100'000 - \$250'000 in %	\$250'000 - \$1M in %	> \$1M in %	Amount Un-known in %
Malicious Acts / internal	25	3	5	2	65
Malicious Acts / external	26	2	4	3	65
Loss of availability (non-natural disasters)	25	7	4	4	60
Macro Viruses	28	5	3	1	63
Other Viruses	34	4	3	1	58
Industrial Espionage	12	-	-	-	88
Unknown Source	14	-	-	-	86

PhD Thesis N. Thodén, University of St. Gallen, 1999:

„Managing the Vulnerability of Banks to Information Technology Related Criminal Type Risks“

Do we Know the Cost?

Figure 5: Percentage of IT Budget for Security



Source: 2008 CSI/FBI Survey

Pause



Benefits of IT Security



Staying Out of Jail

- Corporate officers are forced to be able to prove that they have obeyed all applicable laws.
- This responsibility cannot be delegated in most jurisdictions.
- Law enforcement usually has no sense of humour (neither do shareholders).
- Out of court settlements are more difficult when the case is built on criminal offences.

Staying in Business

- Shareholders, customers, partners, employees etc. will desert companies with a bad security record / reputation.
- Non-adherence to sector- or national regulations may result in license being revoked / suspended.
- Having to provide additional budgets for dealing with security issues will influence your balance sheet and financial reporting, which in turn influences your credit ratings etc.

Beating the Competition

- Profiting from a competitor's bad reputation
- Providing value-add security services for clients
- Protecting company assets against espionage
- Attracting / retaining the best employees
- Spending less on “fixing problems” or re-gaining market acceptance / market share.

Cost Estimations for IT Security



Cost: Insurance Model

Cost: RoSI

- Return on Security Investment (University of Idaho)
- Recovery cost – cost reduction + investment = Annual Loss Expectancy (ALE)
- Recovery cost - ALE = RoSI
- Example: 40'000\$ investment in IT Security, which results in 85% security, carries a risk of 100'000\$, but reduces cost by 45'000\$.
$$(100'000 - 85'000 + 40'000 = 55'000;$$
$$100'000 - 55'000 = 45'000)$$
- But: empirical data is often not sufficient / precise.
- http://www.infosecwriters.com/text_resources/pdf/ROSI-Practical_Model.pdf

Other Measurement Approaches

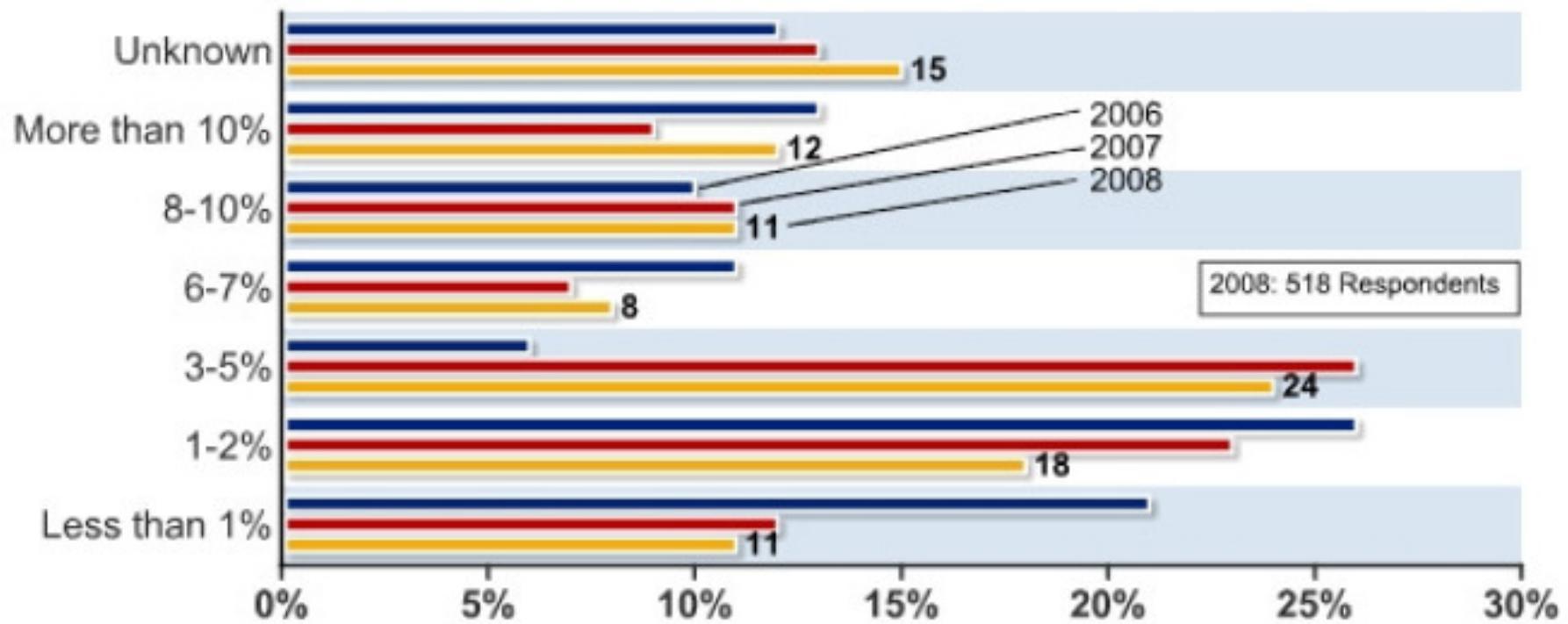
- Net Present Value (NPV)
 - Standard method for the financial appraisal of long-term projects
 - Each cash inflow/outflow is discounted back to its present value, then they are summed up.
- Internal Rate of Return (IRR)
 - The annualised effective compounded return rate which can be earned on the invested capital
 - A project is a good investment proposition if its IRR is greater than the rate of interest that could be earned by alternative investments (investing in other projects, buying bonds, even putting the money in a bank account). The IRR should include an appropriate risk premium.
- Maximum Possible Loss (MPL)
 - The maximum amount of (direct / indirect) money lost on an incurred risk.
- Value at Risk
 - A measure of how the market value of an asset or of a portfolio of assets is likely to decrease over a certain time period under usual conditions or – in this context – under a risk scenario.

Empirical Cost Estimation

- “cross industry” estimate by Gartner Group as of June 2002: expenditure for IT Security averages 3-5% of IT budgets, with significant variations for some industries (e.g. financial, military) and without calculating cost for recovery from incidents.
- Paradox: IT Security expenditures grow reverse-proportionally to cost reductions in projects and procurements.
- But: vague cost allocation for IT Security (e.g. cost for user administration, regulatory requirements etc.)

CSI / FBI Survey 2008 Estimate

Figure 5: Percentage of IT Budget for Security



Judging Cost by Experience

■ Expenditures

- ca. 5 – 10 % of IT project costs (including “high risk” projects)
- ca. 15 % of IT infrastructure costs (network, servers, etc)
- ca. 10 % of IT operating costs (firewall, encryption, antivirus, ...)
- ca. 3 – 5 % of IT personnel

■ Mapping to Activities

Property	Typical Activity	Expenditure
Protect from outside	Firewall design, antivirus	10 %
Protect from inside	Reviews, analysis, IDS	20 %
Projects / Engineering	Consulting, project sign-off	40 %
Locations / Partners	Reviews, recommendations	10 %
Awareness	Education, awareness	15 %
Governance	Guidelines, procedures	05 %

Dealing with Cost



Cost-Reducing Measures I

- Central coordination of all security efforts, but distributed realisation throughout the organisation.
- Use of a „baseline security“ model, that defines the minimum protection standard, and helps to avoid a large number of individual evaluations.
- Integration of IT Security into the quality and process model, as well as into the operational risk management, in order to utilise conceptual and operational synergies, and to allow re-use of methodologies.

Cost-Reducing Measures II

- Use of synergies with related activities, such as audit, compliance, legal services, physical security, risk office (e.g. through joint reviews, checklists etc)

- Integration of IT Security into the IT Governance (IT Strategy, Architecture, controlling etc), as well as into the project and procurement process as early as possible.

Cost-Justifying Measures

- Proof of prevented damages
- Proof towards regulators concerning the ability to protect and sustain regular operations
- Proof of IT Security capabilities towards business partners (due diligence) as part of an agreement / contract
- Better service towards customers (e.g. through an extension of the security perimeter)
- Competitive advantage

Benchmarking – the “Internet Storm Center”

Firefox Reports | SANS Internet Storm Center; Coo... + sans.edu https://isc.sans.edu/reports.html Google

Threat Level: GREEN YELLOW ORANGE RED

Storm Center Tools Data/Reports My ISC Contact Handler on Duty: Russ McRee Contact Us

Reports

Data Collection | Top 10 Ports | World Map | Top 10 Source IPs | Additional Reports

Data Collection

- ISC/DSHield API
- HTTP Headers
- 404Project
- Report Fake Tech Support Calls

Top 10 Ports

by Reports		by Targets		by Sources	
Port	Reports	Port	Targets	Port	Sources
3389	136321	5900	62090	445	19500
445	132101	22	56989	26863	14057
23	100844	23	53419	23	11795
22	89380	1433	52248	3389	9933
1433	81473	3389	45974	5559	2707
5900	68839	8080	43227	39455	2088
8080	55413	445	29295	210	2085
80	52554	80	20716	5644	1958
139	34042	27977	11283	25	1347
26863	26533	21	10888	80	1334

[View Port Report Page](#)

Worldmap

The colored circles in the world map correlate to a color key of port numbers in the lower left corner. This is the break down of the top ports being reported in to the ISC from sensors around the world.

Top of page ↑

site/port/ip search: GO

Get ISC Swag!!

Advertisement

SANS London 2012
Europe's biggest and most important training event

Big Ben and the Palace of Westminster at night.

Top of page ↑

<https://isc.sans.edu/>

Summary – Take Home Message

- Security (or lack of security) results in up-front as well as in retrospective cost.
- The true costs for security are hard to calculate, the cost / benefit ratio is even harder to assess.
- The costs for security can be reduced and/or justified.
- Theoretical cost calculation models are available, but do not satisfy all requirements

Sourcing of Security Services

Risk and Security Management – HS 2012

PD Dr. Hannes P. Lubich



Motivation

GRAND AVENUE

BY STEVE BREEN



© UFS, Inc.

Outline

- Outsourcing, Outtasking, Offshoring, ...
- Benefits and Risks of Outsourcing
- Security Sourcing Models and Offerings
- Sourcing Process and Steps
- Governance Retention and Service Levels

Outsourcing, Outtasking, Offshoring, ...



Terminology

- **Outsourcing**
 - The delegation of non-core operations from internal production to an external entity specialising in that operation.
- **Outtasking**
 - The delegation of individual work packages and tasks.
- **Near-Shoring / Offshoring**
 - The relocation of an organizational function to a foreign country, but not necessarily a transformation of internal organisational control or task execution.
- **Insourcing**
 - The opposite of outsourcing, often applied (quietly) after an unsuccessful outsourcing strategy.
- **Rightsourcing**
 - More flexible approach to outsource, based on business dynamics
- **Co-Sourcing**
 - Services are performed jointly, the scope of work may focus on one or more individual aspects of the sourced activity.

Based on: www.wikipedia.org

Benefits and Risks of Outsourcing





Benefits

- Lower cost of production (personnel, capital, operational expenses, ...)
- More flexible cost structure (fixed → variable)
- Better quality of service (less production errors, better execution, higher productivity, ...)
- Better time to market (faster turnover from design to implementation, ...)
- Better access to resources (skills, ...)
- Focus on core competencies
- Transfer of innovation risk

Risks

- Loss of know-how / jobs in the local economy
- Dependencies on semi-independent entities
- „Culture gap“ (esp. for off-shoring)
- Intellectual property dispersion / theft
- Exploitation of developing countries' resources
- Hidden cost / singular effect on overall budget

BIS/BIZ Outsourcing Risk Landscape

- Strategic Risk
- Reputational Risk
- Compliance Risk
- Operational Risk
- Exit Strategy Risk
- Counterparty Risk

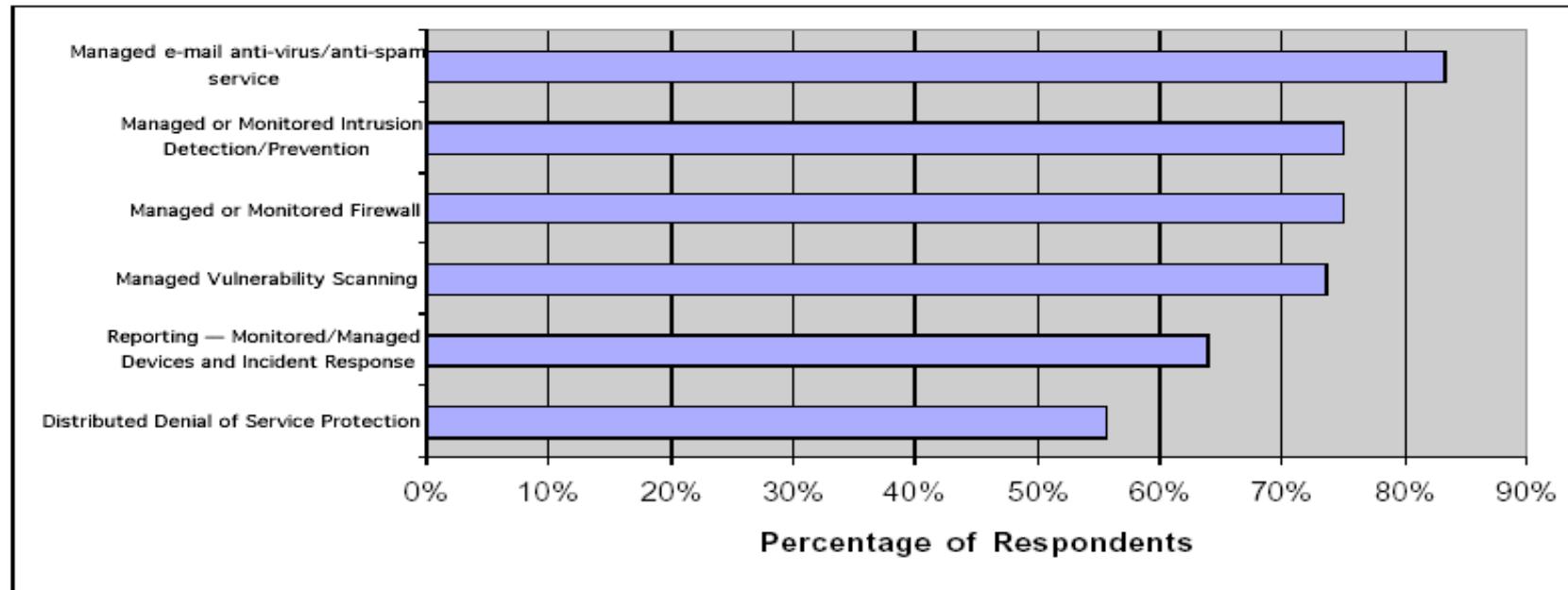
Security Sourcing Models and Offerings



General IT / Operations Sourcing Examples

- Helpdesk / 1st level support sourcing
 - Privacy/data protection, password reset, ...
- Network (data, voice, video) operations sourcing
 - Data protection, intrusion, trans-border routing, ...
- System provisioning and operations sourcing
 - Provider selection criteria, baselines & controls, data protection, integration with corporate security, ...
- Data processing (HR, financial, back-office, transaction processing, ...) sourcing
 - Privacy / information / intellectual property protection, ...
- Software development / engineering / 2nd level support sourcing
 - Design criteria and controls, integration, test data, ...
- Business process sourcing
 - Loss of competitive advantage, leaks, espionage, ...

What Security Services are Outsourced?



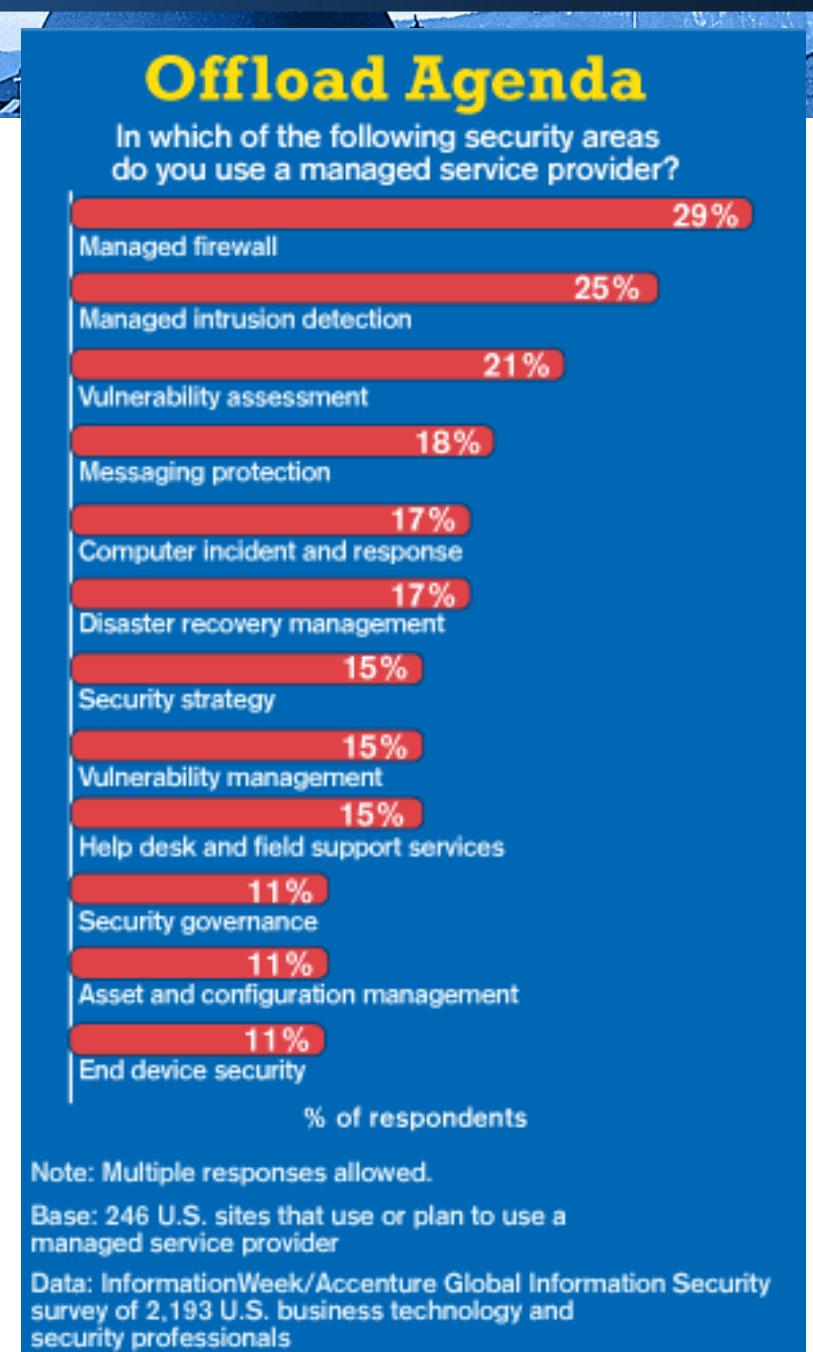
N=72

Source: Gartner, November 2005

Respondents in France, Germany, Spain, Portugal and the U.K.

Gartner

What Security Services are Outsourced?



Source: <http://www.informationweek.com/news/196604332>, 2006

Security-specific Sourcing

- Security Assessment & Awareness
 - e.g. external security reviews, peer-comparison, education, ...
- Security Design & Architecture
 - e.g. architecture consulting, vendor selection, best practice dev, ...
- Security Development & Engineering
 - e.g.: devices & solutions, integration, testing, 2nd level support, ...
- Security Control & Monitoring
 - e.g. monitoring, incident response, 1st level support, forensics, ...
- Managed Security Service Provision (MSSP)
 - e.g. full-service secure hosting/housing of IT infrastructure & operations, e.g. for SME's, or dedicated security service provision, e.g. certification/PKI, secure network provision, ...

Externalising Equipment and/or People?

	Internal Equipment	External Equipment
Internal Personnel	Internal operation or „body leasing“	Seldom used, e.g. in pure housing / hosting scenarios
External Personnel (Remote Access)	Firewalls/IDS monitoring or management	Firewalls at the provider sites, security scans or other services

Pause



Sourcing Process and Steps



Internal Preparation

- What is the goal of the sourcing efforts (immediate cost cuts, re-sizing of company, planned expansion, ...)?
- Are the internal IT processes, IT architecture and infrastructure ready for full/partial sourcing?
- Will the sourcing efforts effect the workforce, and if yes, how (i.e. are people part of the sourcing deal, or will the internal resources be re-used)?
- What are the KPI's for IT and IT security?

Provider Selection

- Longevity / experience / track record of operation
- Real-time analysis and response capability
- State-of-the-art facilities and know-how
- Global/appropriate intelligence and coverage
- Annual revenues / financial stability
- Management / operational experience in relevant sectors
- Breadth of services
- Security management processes
- Vendor neutrality
- Auditing
- Reporting
- Contract / service level / due diligence
- Reputation in the market / with peers

Adapted from: Key Considerations for Outsourcing Security
by Brian Dunphy - Director of Global Analysis Operations
for Symantec Managed Security Services - 25 May 2004

Sourced Security Operation

- Internal security
- 7 x 24 monitoring of provided service elements
- Threat management
- Incident response
- Availability management
- Business continuity & crisis management
- Change and configuration management
- Regular reporting
- Alarming / escalation
- Staffing / know-how retention
- Handover point to customer processes

Governance Retention and Service Levels



Governance Responsibility

- Whatever you are outsourcing – the overall responsibility stays:
 - “Nicht auslagerbar sind die Oberleitung, Aufsicht und Kontrolle durch den Verwaltungsrat sowie zentrale Führungsaufgaben der Geschäftsführung.”
(EBK-RS 99/2 Outsourcing, basierend auf dem OR,
<http://www.ebk.admin.ch/d/publik/mitteil/1999/m14-99-2.pdf>)
- **Governance** (in business) is the action of developing and managing consistent, cohesive policies, processes and decision rights for a given area of responsibility. For example, managing at a corporate level: privacy, internal investment, the use of data, etc.



Service Level Agreements

- A SLA is a formal negotiated agreement between two parties. It is a contract that exists between customers and their service provider, or between service providers. It transcripts the common understanding about services, priorities, responsibilities, guarantee, etc. with the main purpose to agree on the level of service. For example, it may specify the levels of availability, serviceability, performance, operation or other attributes of the service like billing and even penalties in the case of violation of the SLA.
- Typical (general) SLA elements:
 - **ABA** (Abandon Rate): **Percentage** of waiting issues abandoned
 - **ASA** (Average Speed to Answer): Average **time** to answer to an issue
 - **TSF** (Time Service Factor): **Percentage** of issues settled within a definite timeframe, e.g. 80% in 1 day.
 - **FCR** (First Call Resolution): **Percentage** of incoming issues that can be resolved without a callback or reminder
 - **Uptime Agreements** (various measurements, objectives etc)
- See also <http://www.sla-zone.co.uk/>

Source: www.wikipedia.org

Security-Specific SLA Elements

- Handling of infrastructural / technical issues, e.g.:
 - Virus/worm/spyware outbreaks
 - Unauthorized access
 - Theft of proprietary Information
 - Denial of service attacks and subsequent service loss / degradation
 - Insider network abuse
 - Documented cases of financial fraud
 - Application misuse
 - System breaches
 - Network misuse
 - Sabotage
- Governance / management services, e.g.:
 - Provision of reports, escalations etc. in defined time
 - Response to security incidents etc. in defined time

Results of a Gartner Group Study on Assessing Outsourcing and Third-Party Security Risks



Key Findings

- Each unexamined player increases risk ambiguity exponentially.
- Although a contract may contain penalty clauses, they are risk transfer mechanisms that are tantamount to insurance. The signing of a contract provides no evidence that required risk controls are in place and functioning. Without some form of periodic assessment or auditing, there can be no assurance that contractual security requirements are being met.
- Extending physical and personnel security requirements to contractors, partners and travelling employees remains a key element in safeguarding critical information.
- Technical solutions for remote access security are increasingly effective and affordable, but they cannot totally compensate for weaknesses in physical and staff security.

Gartner Group: Assessing Outsourcing and Third-Party Security Risks, J. Heiser, 22 June 2006, ID Number: G00140128

Predictions

- During 2006 to 2007, several organizations will suffer from negative public relations (PR) when they are forced to notify customers an authorities that privacy data was lost because family members or friends accessed the home terminal of an off-site call centre worker.
- Hype about the purported short-term cost savings will prevent the formal assessment and acceptance of third-party and outsourcing risk from being widely considered as a best practice before 2008.

Gartner Group: Assessing Outsourcing and Third-Party Security Risks, J. Heiser, 22 June 2006, ID Number: G00140128



Recommendations

- Ensure that corporate security and compliance policies apply to all uses of corporate information assets, including outsourcing projects.
- Demand risk transparency from service providers and other third parties that access sensitive data.
- Use a mix of technical, procedural and contractual compensating controls.

Gartner Group: Assessing Outsourcing and Third-Party Security Risks, J. Heiser, 22 June 2006, ID Number: G00140128

MSSP on the Gartner Hype Cycle

Figure 1. Hype Cycle for Information Security, 2006



Summary – Take Home Message

- All IT sourcing activities have an impact on IT security.
- Even IT security service elements can be sourced, if planning, implementation and supervision are done correctly.
- Whatever you source, the governance responsibility remains with you (no delegation).
- Sourcing provision is a growing market.

Organisation of IT Security

Risk and Security Management – HS 2012

PD Dr. Hannes P. Lubich



Motivation



Outline

- Security Job Profiles and Skills
 - Security Organisation
 - Related Organisational Functions
 - Security Continued Education
- Disclaimer: all information presented in this lecture may differ substantially between contexts



Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Security Job Profiles and Skills





Job Descriptions

- Chief Information Security Officer (CISO)
- Information Security Officer
- Security Architect
- Security Engineer
- Security Administrator

Chief Information Security Officer (CISO)

- IT security professional (minimum 5-7 years experience in complex IT environments, minimum 3 years as security officer or security architect)
- Up-to-date IT Security and risk management know-how
- Extensive program / project management skills
- Negotiation and communication skills on the CxO level
- Ability to work in virtual teams and under constant pressure
- Business-specific expertise and skill recognition
- People management (**direct reports and “dotted lines”**)

Information Security Officer

- IT professional (minimum 3 years experience in complex IT environments)
- Up-to-date IT Security know-how (possibly also certification)
- Specific technology or project management skills
- Negotiation, communication and conflict resolution skills
- Ability to work in virtual teams and under constant pressure
- Willingness to conduct security-relevant operational tasks

Security Architect

- IT professional (minimum 5 years experience in complex IT environments)
- Up-to-date IT Security know-how and certification
- Specific technology, vendor/market and project management skills
- Negotiation and communication skills
- Ability to work in virtual teams and under constant pressure

Security Engineer

- Similar to security architect, but potentially limited to specific technologies (e.g. Unix, Microsoft) or security topics (e.g. IAM, Threat Mgmt)
- Good „entry level“ position for security architect or security officer position
- Main task is to build / engineer / evaluate specific security solutions within the boundaries of a given security concept and architecture
- Can be part of project / engineering IT unit, or part of the security organisational unit

Security Administrator

- IT operations person with full operational responsibility for security-relevant infrastructure, such as:
 - User, role, access rights mgmt, incl. PKI, directory services, token mgmt etc.
 - Security infrastructure elements, e.g. firewalls, intrusion detection and prevention systems, DMZ's
- Part-time IT operations person with non-exclusive operational responsibility for security-relevant functions, e.g.:
 - IT platforms (Server, Clients, Notebooks, etc with local security elements, such as security patches, anti-virus, anti-spyware
 - Helpdesk / 1st level support tasks, such as password reset, anti-virus counter-measures etc.
- Security entry level position for IT support staff with “training on the job” possibility
- Willingness to carry out operational tasks, possibly in shifts or “on call” availability



Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Security Organisation



Security Functional Units / Topics

- Security Governance
- Security Operations
- Security Engineering

Security Governance – Organisation

- Corporate Function
 - Central point of governance and control
 - Can be rather detached from “IT realities”
- Line Management Function
 - Close to events, people, and incidents
 - Too distributed, not enough coordination / synergies
- Hybrid Solution
 - Central governance, methodology, reporting etc.
 - Local execution and responsibility

Security Governance – Mandate

- Single point of contact for all IT security questions and issues
- Issuer of relevant security policy, concept, architecture, guidelines, checklists etc.
- Provider of security awareness measures and materials
- Review of IT operations concerning IT security
- Security reporting & escalation

Security Governance – List of Duties

- Actual and documented standards, methodology, technologies and best practices
- Security concept actively promoted on all levels of the organisation
- Conceptual security consulting for all relevant projects, procurements, modifications and extensions of the IT environment
- Identification / escalation of relevant risks and agreed countermeasures
- Risk and activity reporting (incurred losses, “near misses” etc) in “near time”
- Coordination with all relevant organisational units and decision bodies within and outside IT
- Reviews of IT security status, and summary reporting



Security Governance – Core Processes

- Security governance and IT risk management
- Security awareness
- Consulting for IT projects, procurements and operational changes / extensions
- Aid the engineering or operation of highly security-relevant IT infrastructures
- Security reviews and audits of IT operation
- Escalations

Security Governance – Interfaces

- IT Strategy & Architecture
- Project Management
- Procurement
- IT Asset Lifecycle Management
- (Change & Configuration Management)
- (Incident & Problem Management)

Security Governance – Key Performance Indicators

- Number of security incidents detected / handled
- Project consulting efforts versus overall number of IT projects
- Number / coverage of security reviews
- Supervision and reporting efforts (reviews, security monitoring etc)
- Pro-active efforts (standards, architecture, concepts, awareness etc)
- Security engineering and security operations efforts
- Security innovation (strategies, technologies, products, tools etc)
- Continued security education efforts

Pause



Security Operations – Organisation

- Usually embedded into regular IT operations units, including operational SLAs, on call duty ...
- Can be dedicated sub-units (e.g. access rights management) or part-time (e.g. helpdesk staff handling virus incidents or password reset)
- Line management within IT operations, but dotted line from / to Security Governance



Security Operations – Mandate

- Operation and support of all security-relevant IT infrastructures (security, performance, reliability).
- Operation of security-relevant IT infrastructure (firewalls, IDS/IPS, DMZ, anti-virus, anti-spyware, SSO-, directory- and PKI infrastructures, administration and provisioning of users, roles and access rights, testing and roll-out of security-relevant patches / changes / updates, security logging, monitoring and correlation of events etc)
- Potentially distributed across several organisational units (server, desktop, networks, applications, 1st / 2nd level support etc), based on conceptual considerations or because of necessity for separation of duties.

Security Operations – List of Duties

- Precise and near-time documentation and supervision of security-relevant IT infrastructures, systems, applications
- Administration and supervision of all user roles, access rights, configurations etc.
- Continuous actualisation of all IT components concerning security-critical patches, updates, configuration changes
- Coordination of all planned and actual activities with regular IT operations (maintenance windows etc)
- Near-time reaction to operational IT security incidents, problems etc.
- Continuous reporting of key performance indicators to IT operations and Security Governance

Security Operations – Core Processes

- Documentation / supervision of security elements
- Identity and access rights management, provisioning, configuration etc.
- Modification of operated security elements (patches, updates etc)
- Incident handling, reacting to security issues etc
- Reporting

Security Operations – Interfaces

- Security Governance
- IT Operation
- First Level Support
- Change & Configuration Management
- Incident & Problem Management

Security Operations – Key Performance Indicators

- Number of systems / components operated (plus growth rate)
- Number of attack attempts on operated systems (successful, not successful)
- Number / severity of unplanned service interruptions / degradations because of security incidents or implementation of countermeasures
- Root cause analysis for security incidents and correlation with internal / external processes and sources



Security Engineering – Organisation

- Usually embedded into either IT or business-side project development or engineering units
- Can be dedicated sub-units (e.g. IT security engineering) or part-time (e.g. “security-aware” project managers or project specialists/developers)
- Line management within IT or business line(s), but dotted line from / to Security Governance

Security Engineering – Mandate

- Most IT projects, procurements, replacements etc. require complex security elements, which must be identified, assessed, engineered, configured, tested and integrated with respect to methodology, provider/vendor, technology etc. Security Engineering is responsible for providing these services.
- The primary mandate of Security Engineering is the evaluation, engineering and integration of IT security solutions in close cooperation with the project/task management, the business side, as well as Security Governance and Security Operations.
- Depending on defined service level agreements, Security Engineering may also provide 2nd level support for security solutions being operated by IT.

Security Engineering – List of Duties

- Build and retain sufficient know-how concerning security methodology, solutions, technologies, vendors
- Active participation in projects, procurements, changes, integration efforts etc. concerning security solutions or components
- Design and evaluation of corresponding concepts, calls for information / proposal, tests, pilots, trials etc.
- Design, implementation, documentation and integration of “ready-to-operate” security solutions or components
- 2nd level support for security solutions, based on SLA's

Security Engineering – Core Processes

- Know-how acquisition, retention and transfer
- Project / procurement management and participation
- Evaluation of security solutions
- Design and engineering of security solutions
- 2nd level operations support, where required

Security Engineering – Interfaces

- Security Governance
- Project Management
- Software / Solution Development
- Procurement
- IT Asset Lifecycle Management
- Change & Configuration Management
- Incident & Problem Management (2nd level)

Security Engineering – Key Performance Indicators

- Number of projects / procurements covered versus total number of projects / procurement activities
- Time spent in projects / procurements (utilisation and growth rate)
- Time spent on 2nd level support
- Proper identification of security problem root causes
- Proactive time (market / vendor overview, test lab, education etc)

Related Organisational Functions



Watch for Allies and/or Issues with ...

- Audit
- Legal Services
- Compliance
- Business Continuity / Disaster Recovery and Crisis Management
- Quality Management
- Service & Process Management



Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Security Continued Education



Different Continued Education Methods

- University Level
 - General security, e.g. <http://www.infsec.ethz.ch/>, ZISC etc.
 - Specific courses/research, e.g. <http://www.csg.ethz.ch/research>
- Post-Graduate Courses
 - Master of Advances Studies on Information Security (HSW Luzern)
- Organisations
 - CSO Online (<http://www.csoonline.com/>)
 - ISACA (audit-related organisation, courses/certificates, e.g. CISA, CISM)
 - Information Security Society Switzerland (<http://www.isss.ch/>)
 -
- Courses / Exams (see e.g. <http://www.mit-solutions.com/main.php?show=news.de>)
 - CISSP (must be renewed periodically)
 - BSI (BS7799 or ISO2700x Auditor / Lead Auditor)
 -
- Vendors
 - Microsoft (various certifications)
 - Sun/Oracle (Sun Certified Security Administrator (SCSECA))
 -

Summary – Take Home Message

- Security offers a variety of jobs and profiles.
- The security organisation is usually more than one dedicated organisational unit.
- Security must be well-organised with respect to mandate, list of duties, core processes, interfaces and key performance indicators.
- Security people need to have access to broad continuous education and training.

Risk Management, Relations with IT Security, Governance and Compliance

Risk and Security Management – HS 2012

PD Dr. Hannes P. Lubich



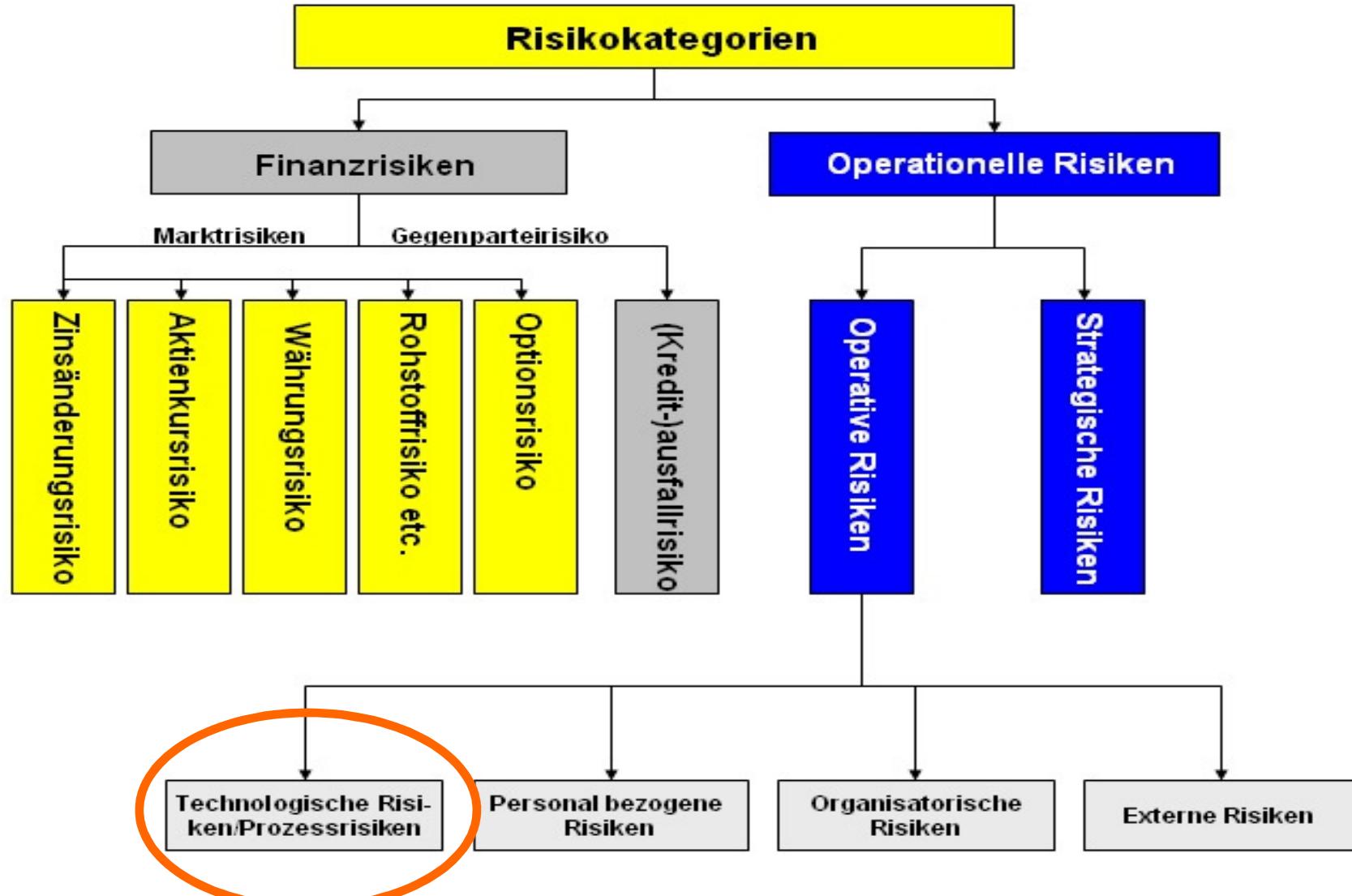
Motivation



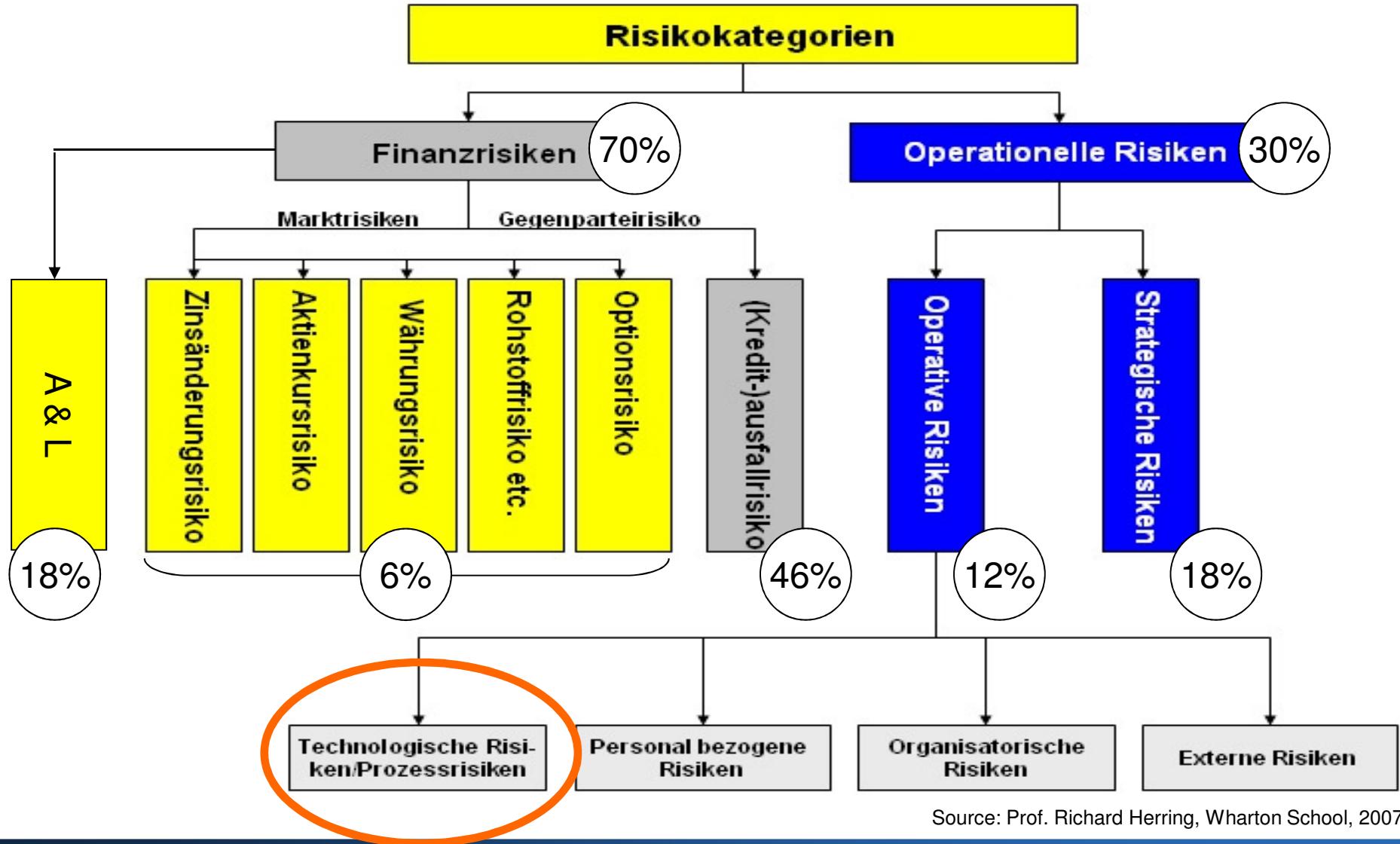
Outline

- Risk Management
- IT Security within Risk Management
- Governance & Compliance

Risk Categories



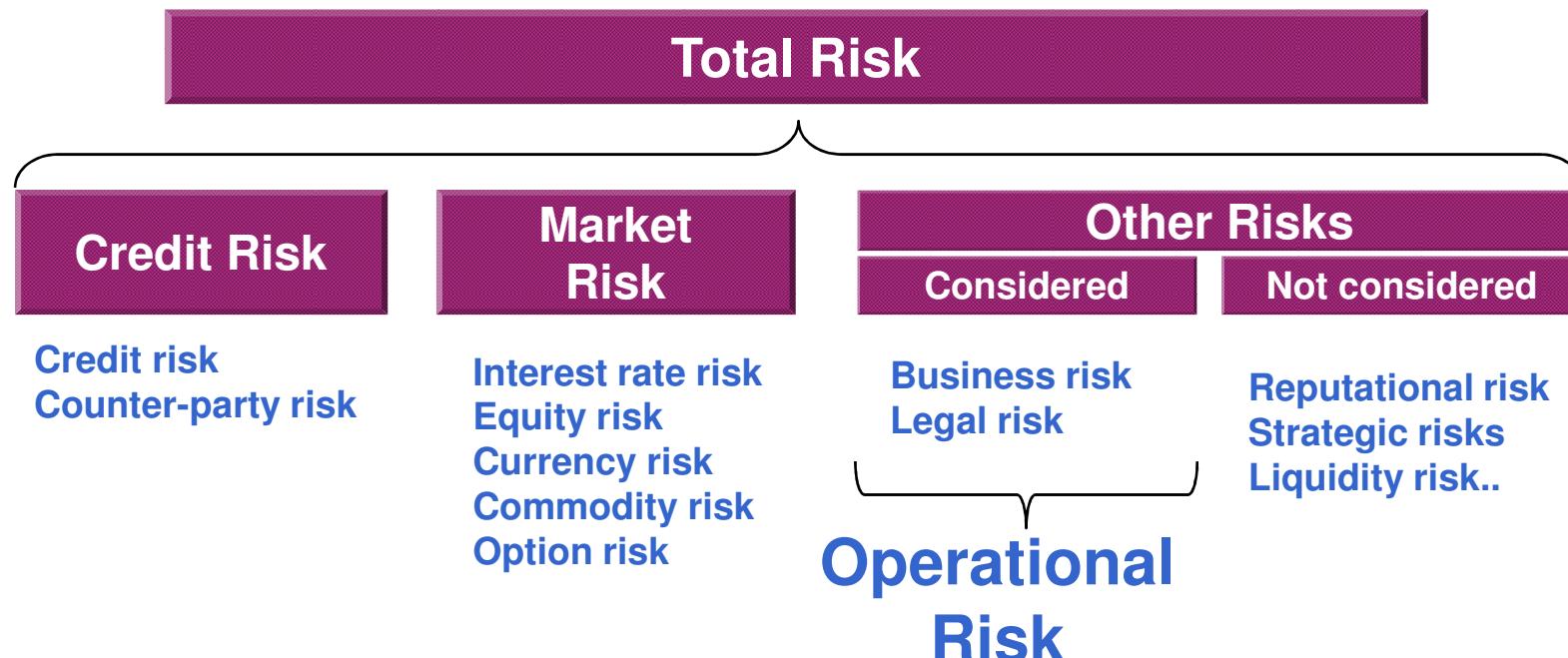
Risk Categories (Banking)



Source: Prof. Richard Herring, Wharton School, 2007

Basel II: Risk Classification

Basel II links *operational risk* to the capital requirements for financial services institutions. The lower the risk, the lower the capital requirements.



*The risk of loss resulting from inadequate or failed internal processes,
people, systems or from external events*

What is an Operational IT Risk?



Risk only



IT Risks:
- Abstract!
- No reward!



Concrete

Abstract



Risk & Reward

Risks in Electronic Environments

- Speed of introduction and complexity of IT environments result in an increase of (additive) weaknesses, that cannot be detected in due time.
- Networking and time/location independency of access allows better coverage of attacks, and the possibility to search for specific weaknesses.
- Better connectivity / tools benefit the attack side - e.g. through virus construction kits or use of foreign systems as platforms for an attacks (mostly denial of service).
- Origin and motivation of attackers varies substantially – so does the method of attack, and the resources used.
- Growing number of legal and compliance requirements, with personal liability to company officers.



Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Risk Management



Content

- The Internal Control System
- Risk Assessment and Management
- Enterprise Risk Standards: COSO

The Internal Control System

- Required by all relevant risk management frameworks (Basel II, COSO) as well as the Sarbanes-Oxley Act (SOX) Section 404: “Management Assessment of Internal Controls”
- Problems to be addressed (based on BIZ requirements):
 - Lack of adequate management oversight and accountability, and failure to develop a strong control culture
 - Inadequate recognition and assessment of the risk of activities.
 - The absence or failure of key control structures and activities, such as segregation of duties, approvals, verifications, reconciliations, and reviews of operating performance.
 - Inadequate communication of information between levels of management, especially in the upward communication of problems.
 - Inadequate or ineffective audit programs and monitoring activities.

The Internal Control System (BIZ)

Management oversight and the control culture

Principle 1:

The board of directors should have responsibility for approving and periodically reviewing the overall business strategies and significant policies of the bank; understanding the major risks run by the bank, setting acceptable levels for these risks and ensuring that senior management takes the steps necessary to identify, measure, monitor and control these risks; approving the organisational structure; and ensuring that senior management is monitoring the effectiveness of the internal control system. The board of directors is ultimately responsible for ensuring that an adequate and effective system of internal controls is established and maintained.

Principle 2:

Senior management should have responsibility for implementing strategies and policies approved by the board; developing processes that identify, measure, monitor and control risks incurred by the bank; maintaining an organisational structure that clearly assigns responsibility, authority and reporting relationships; ensuring that delegated responsibilities are effectively carried out; setting appropriate internal control policies; and monitoring the adequacy and effectiveness of the internal control system.

Principle 3:

The board of directors and senior management are responsible for promoting high ethical and integrity standards, and for establishing a culture within the organisation that emphasises and demonstrates to all levels of personnel the importance of internal controls. All personnel at a banking organisation need to understand their role in the internal controls process and be fully engaged in the process.



The Internal Control System (BIZ)

Risk Recognition and Assessment

Principle 4:

An effective internal control system requires that the material risks that could adversely affect the achievement of the bank's goals are being recognised and continually assessed. This assessment should cover all risks facing the bank and the consolidated banking organisation (that is, credit risk, country and transfer risk, market risk, interest rate risk, liquidity risk, operational risk, legal risk and reputational risk). Internal controls may need to be revised to appropriately address any new or previously uncontrolled risks.

Control Activities and Segregation of Duties

Principle 5:

Control activities should be an integral part of the daily activities of a bank. An effective internal control system requires that an appropriate control structure is set up, with control activities defined at every business level. These should include: top level reviews; appropriate activity controls for different departments or divisions; physical controls; checking for compliance with exposure limits and follow-up on non-compliance; a system of approvals and authorisations; and, a system of verification and reconciliation.

Principle 6:

An effective internal control system requires that there is appropriate segregation of duties and that personnel are not assigned conflicting responsibilities. Areas of potential conflicts of interest should be identified, minimised, and subject to careful, independent monitoring.



The Internal Control System (BIZ)

Information and communication

Principle 7:

An effective internal control system requires that there are adequate and comprehensive internal financial, operational and compliance data, as well as external market information about events and conditions that are relevant to decision making. Information should be reliable, timely, accessible, and provided in a consistent format.

Principle 8:

An effective internal control system requires that there are reliable information systems in place that cover all significant activities of the bank. These systems, including those that hold and use data in an electronic form, must be secure, monitored independently and supported by adequate contingency arrangements.

Principle 9:

An effective internal control system requires effective channels of communication to ensure that all staff fully understand and adhere to policies and procedures affecting their duties and responsibilities and that other relevant information is reaching the appropriate personnel.

The Internal Control System (BIZ)

Monitoring Activities and Correcting Deficiencies

Principle 10:

The overall effectiveness of the bank's internal controls should be monitored on an ongoing basis. Monitoring of key risks should be part of the daily activities of the bank as well as periodic evaluations by the business lines and internal audit

Principle 11:

There should be an effective and comprehensive internal audit of the internal control system carried out by operationally independent, appropriately trained and competent staff. The internal audit function, as part of the monitoring of the system of internal controls, should report directly to the board of directors or its audit committee, and to senior management.

Principle 12:

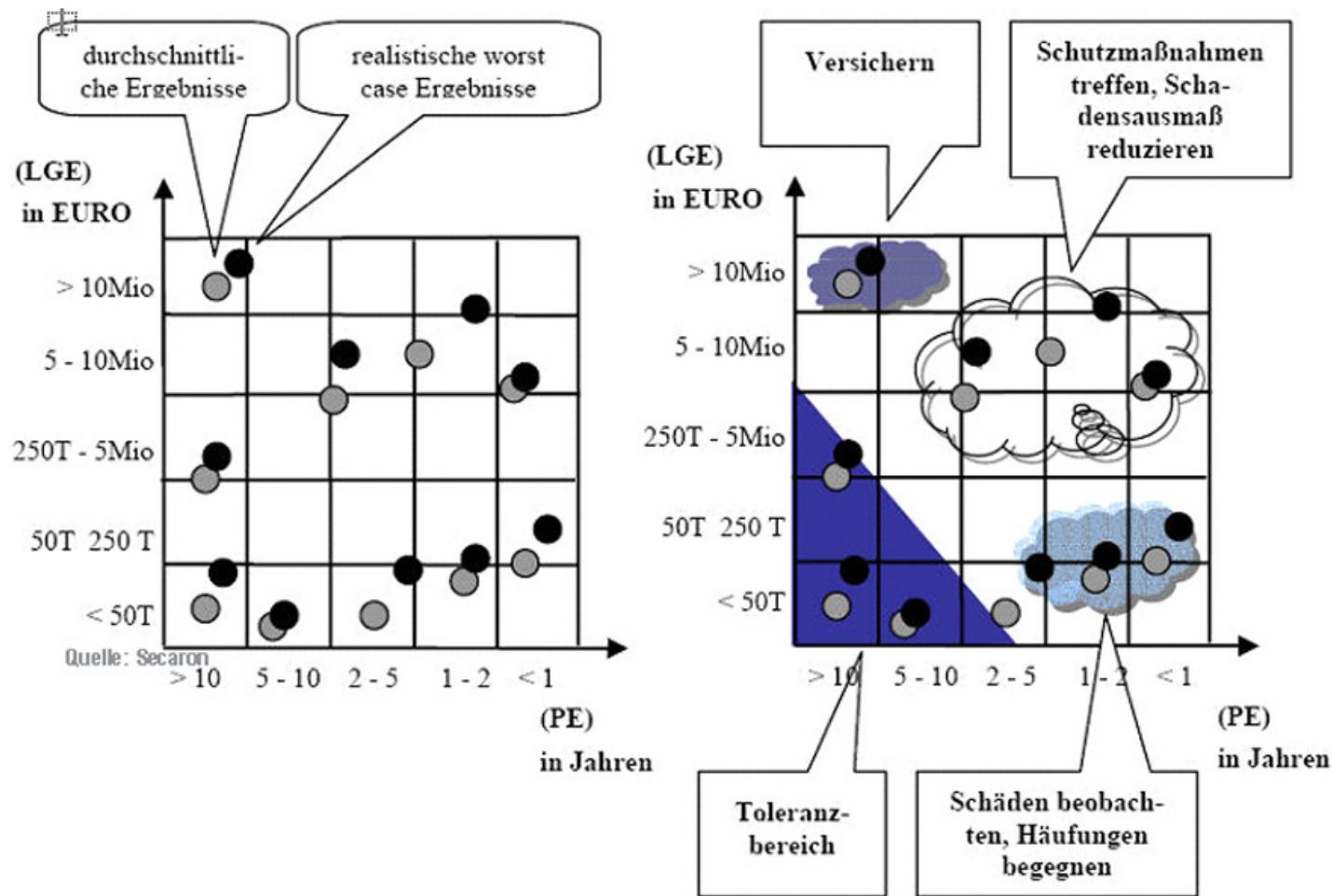
Internal control deficiencies, whether identified by business line, internal audit, or other control personnel, should be reported in a timely manner to the appropriate management level and addressed promptly. Material internal control deficiencies should be reported to senior management and the board of directors.

Evaluation of Internal Control Systems by Supervisory Authorities

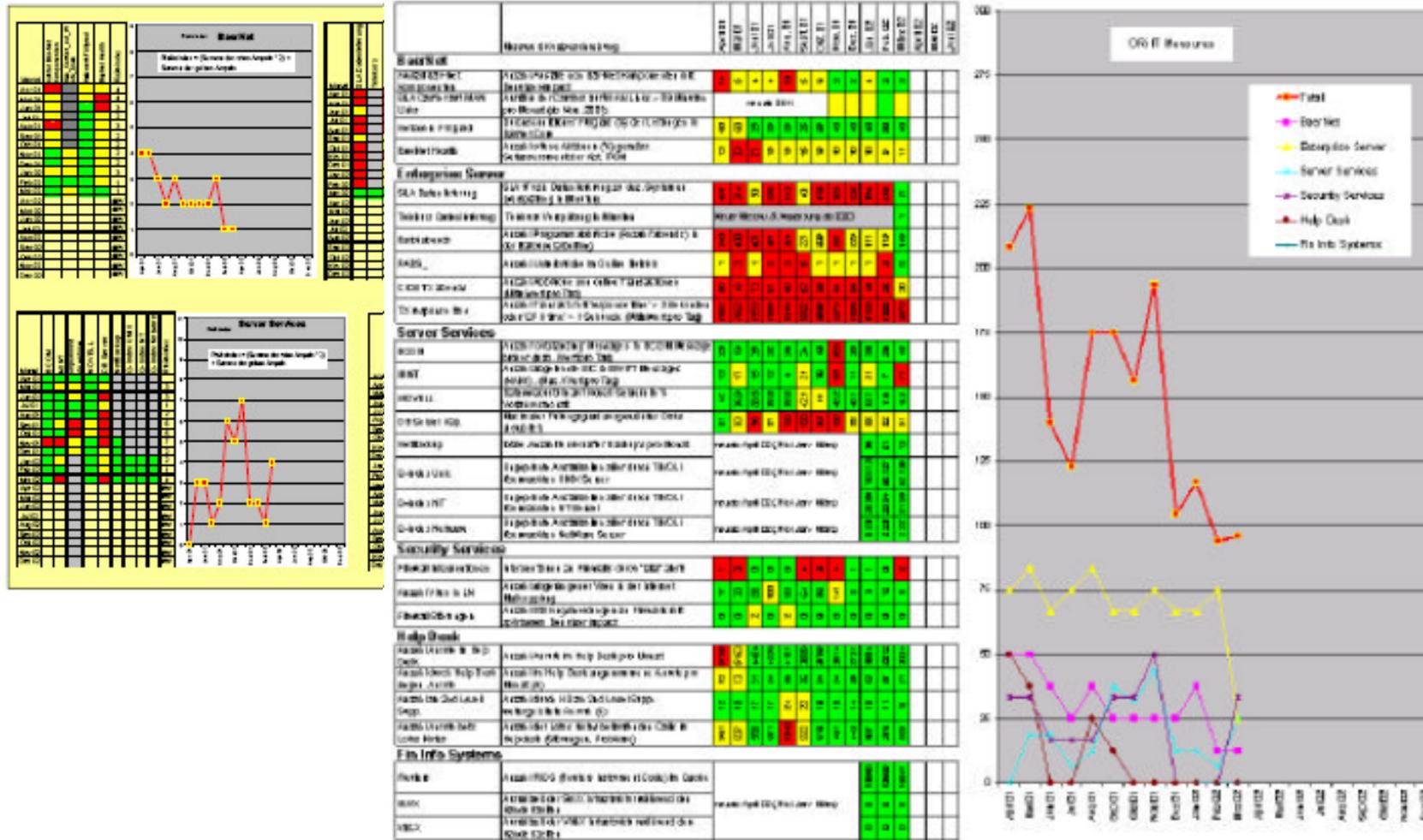
Principle 13:

Supervisors should require that all banks, regardless of size, have an effective system of internal controls that is consistent

Risk Assessment and Management



Example: Risk KPI's and Monitoring



Source: Julius Bär

Pause



COSO ERM Overview

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a voluntary private-sector organization, established in the United States, dedicated to providing guidance to executive management and governance entities on critical aspects of organizational governance, business ethics, internal control, enterprise risk management, fraud, and financial reporting. COSO has established a common internal control model against which companies and organizations may assess their control systems. (Wikipedia)

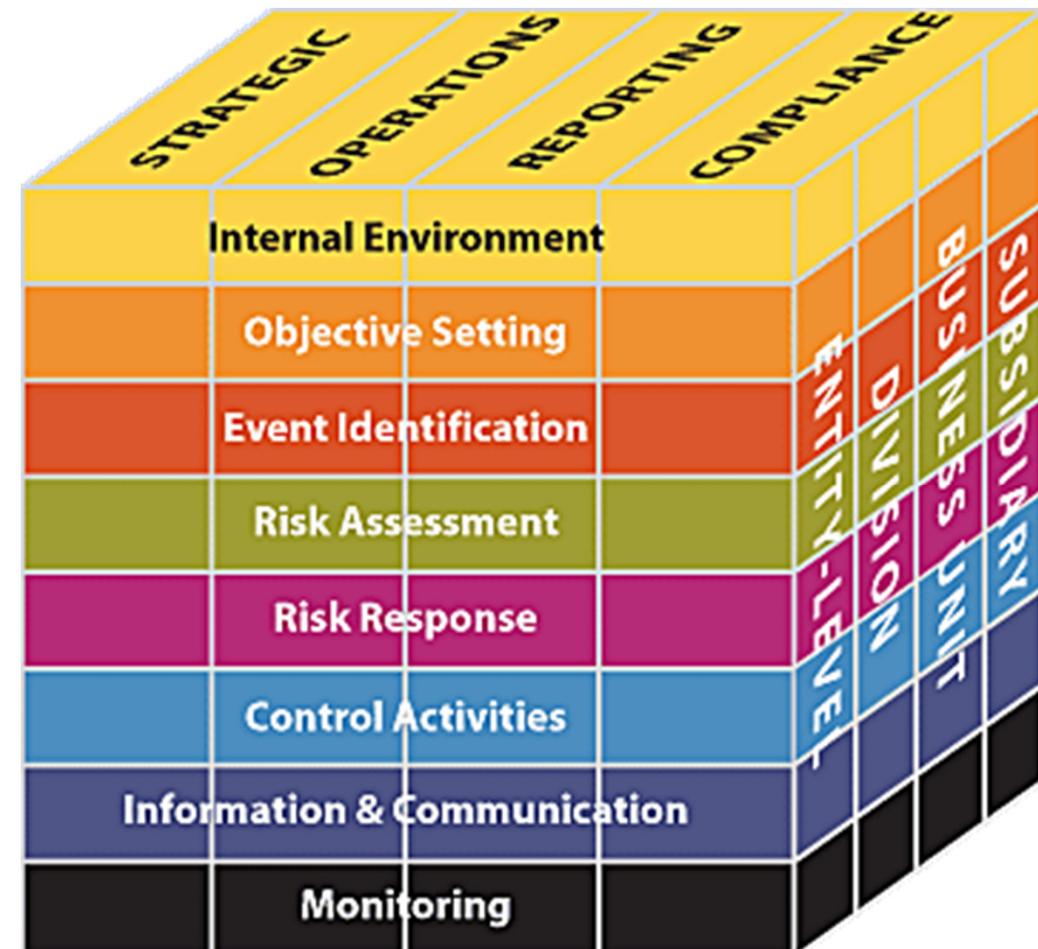
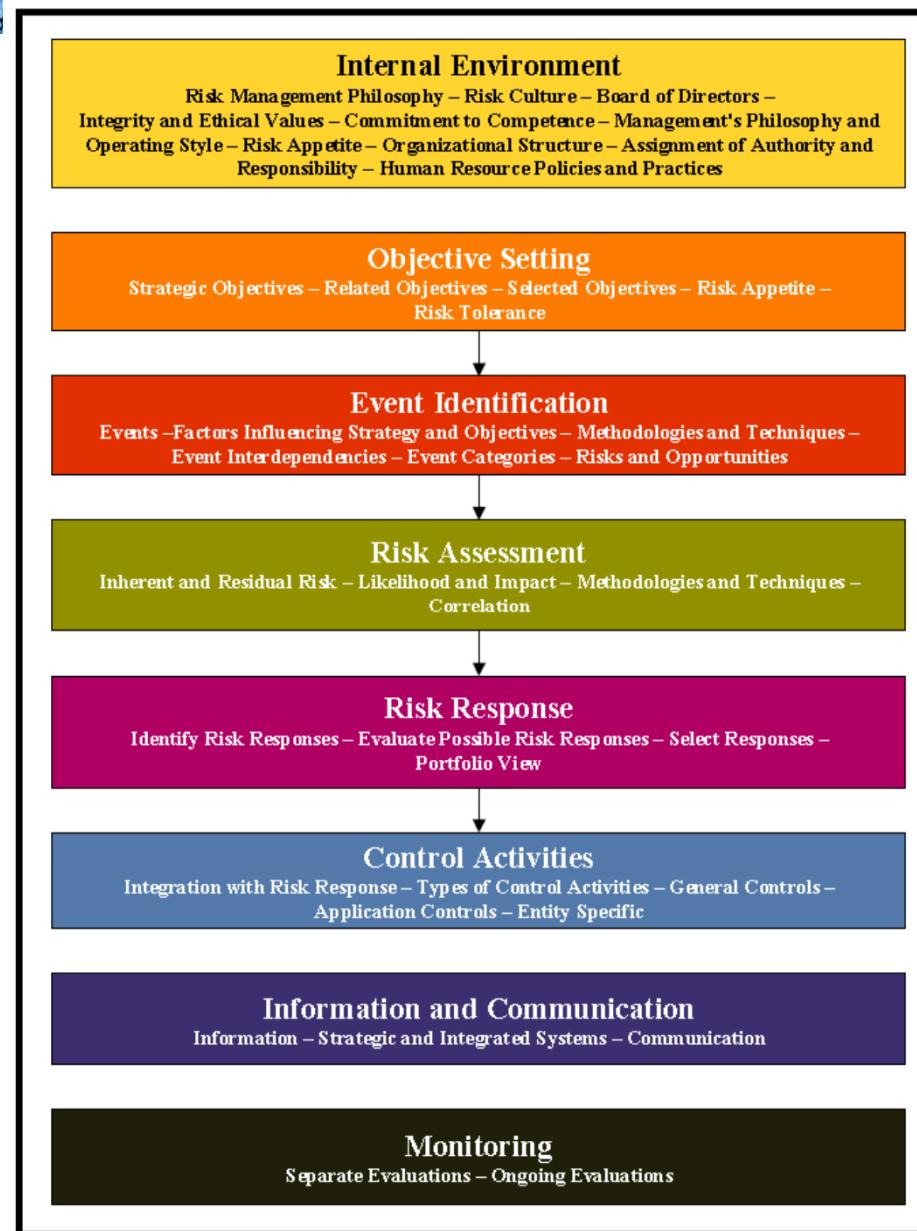


Exhibit 2

The COSO Layered Model



IT Security within Risk Management





Components of Security Management

Identity Management – the creation and management of all user identities, profiles, and entitlements.

Provisioning -- the allocation and de-allocation of corporate resources (typically, digital resources) to each identity.

Access Management – the creation and enforcement of policies that determine which users can access which resources, and the conditions under which access will be allowed.

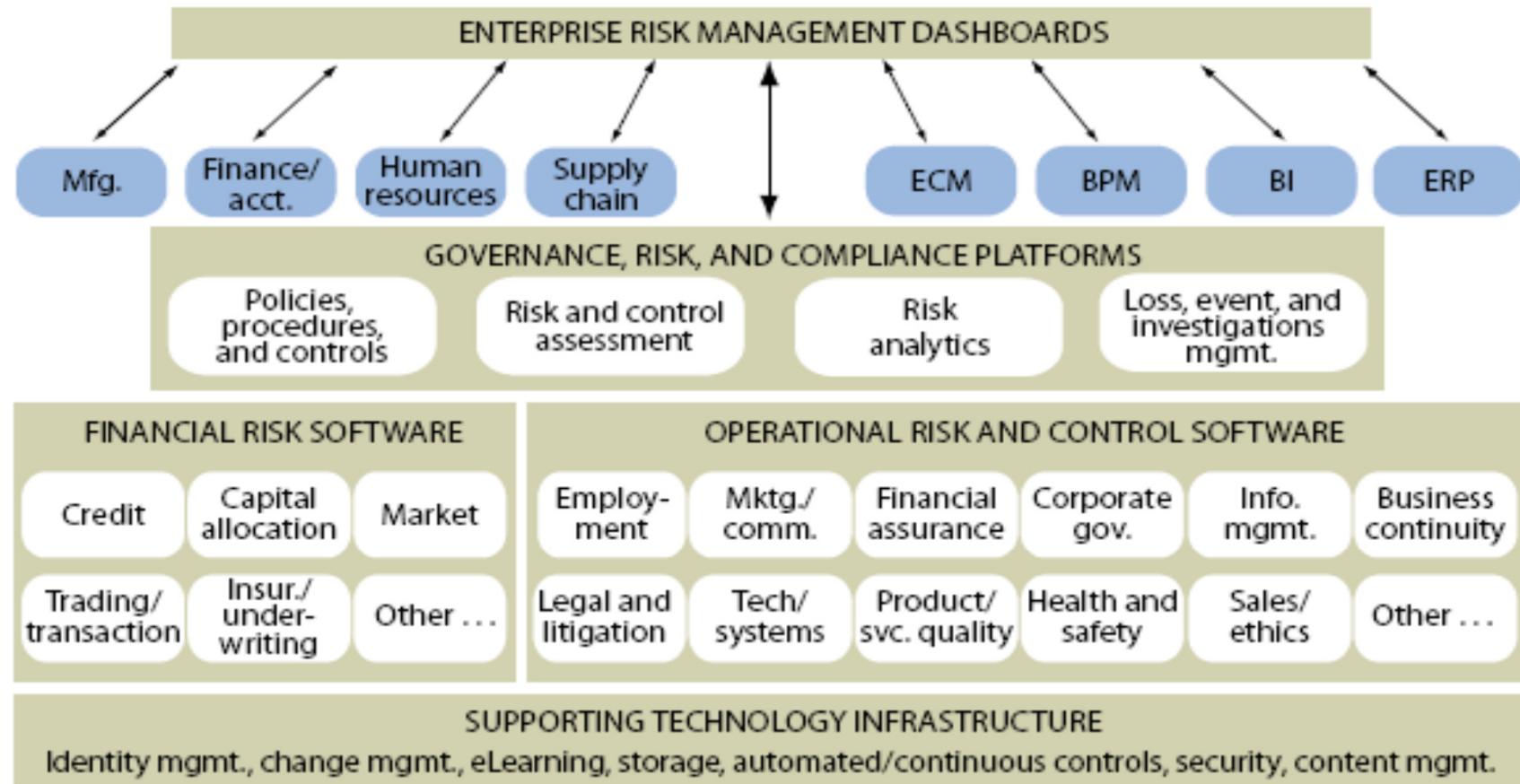
Threat Management – the identification and remediation of security threats (e.g. viruses, spam, spyware) and their respective causes (missing patches, security updates, configuration changes etc).

Monitoring/Auditing – Comprehensive auditing, logging, event correlation, and visualization tools to help monitor the security environment, and to respond to important security events.

Based on CA material

Integration of IT Security into Risk Mgmt

Figure 1 The Risk And Compliance Market Landscape



Source: Forrester Research, Inc.

Governance and Compliance





What is (IT) Governance?

\Gov"ern*ance\, n. [F. gouvernance.] Exercise of authority; control; Government; arrangement. --Chaucer. --J. H. Newman *Webster's Dictionary*

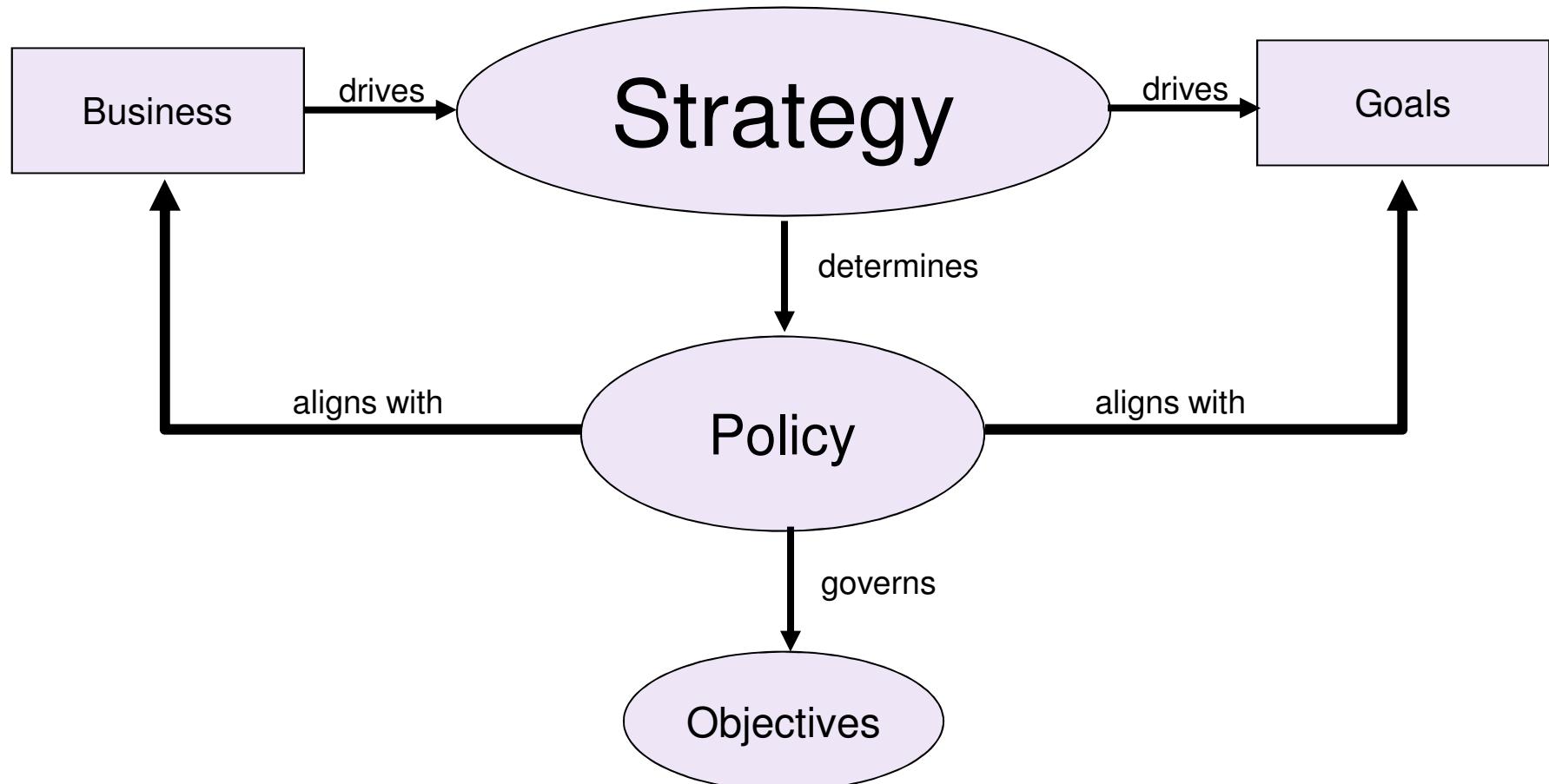
The assignment of decision rights and the accountability framework to encourage desirable behavior in the use of IT. Peter Weill MIT 2001

“... It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives. IT governance is the responsibility of the board of directors and executive management.” *IT Governance Institute, 2002*

Key Areas of IT Governance

- Operations management
 - Running your systems effectively
- Data management
 - Ensuring you keep the right data
 - Ensuring you can use the data that you've kept
- Process management
 - Ensuring that your processes have governance built in through all phases of technology adoption and use
- Asset management
 - Ensuring you pay for the things that you use
 - but not the things that you don't
- Security
 - Managing corporate IT so that it is “secure enough”

Key IT Governance Elements



The 3 Most Common IT Strategy Mistakes

- Mixing aspiration, strategy, and policy
 - Our strategy is Oracle..
- Completely forgetting about the business
 - Every IT strategy statement has to map directly onto the business strategy
 - It's amazing how few actually do..
- Mistaking “technologies” for “solutions”
 - “Web Services” is a classic example

The “Acid Test”

- **Simplification**
 - No new technology should make the environment more complex - without having a **COMPELLING** case
- **Standardisation**
 - Standardisation supports simplification, flexibility and cost, but may need up-front investments
- **Flexibility**
 - You have to be ready and able to understand and support business change
- **Cost**
 - Cost is bad, but must be transparent

IT Governance Assessment - *Test yourself*

IT governance effectiveness indicators	Disagree strongly Score: 0	Disagree somewhat Score: 1	Agree somewhat Score: 2	Agree strongly Score: 3
We have strongly differentiated business strategies				
We have clear business objectives for evaluating every type of IT investment				
Executives are engaged in IT governance and can describe these arrangements				
Our IT governance is stable, with few major changes year to year				
We use well-defined, formal IT exception processes				
We use multiple formal communication methods to engage business leaders				

Total



< 7 no effective IT Governance

7-9 Low-level IT Governance

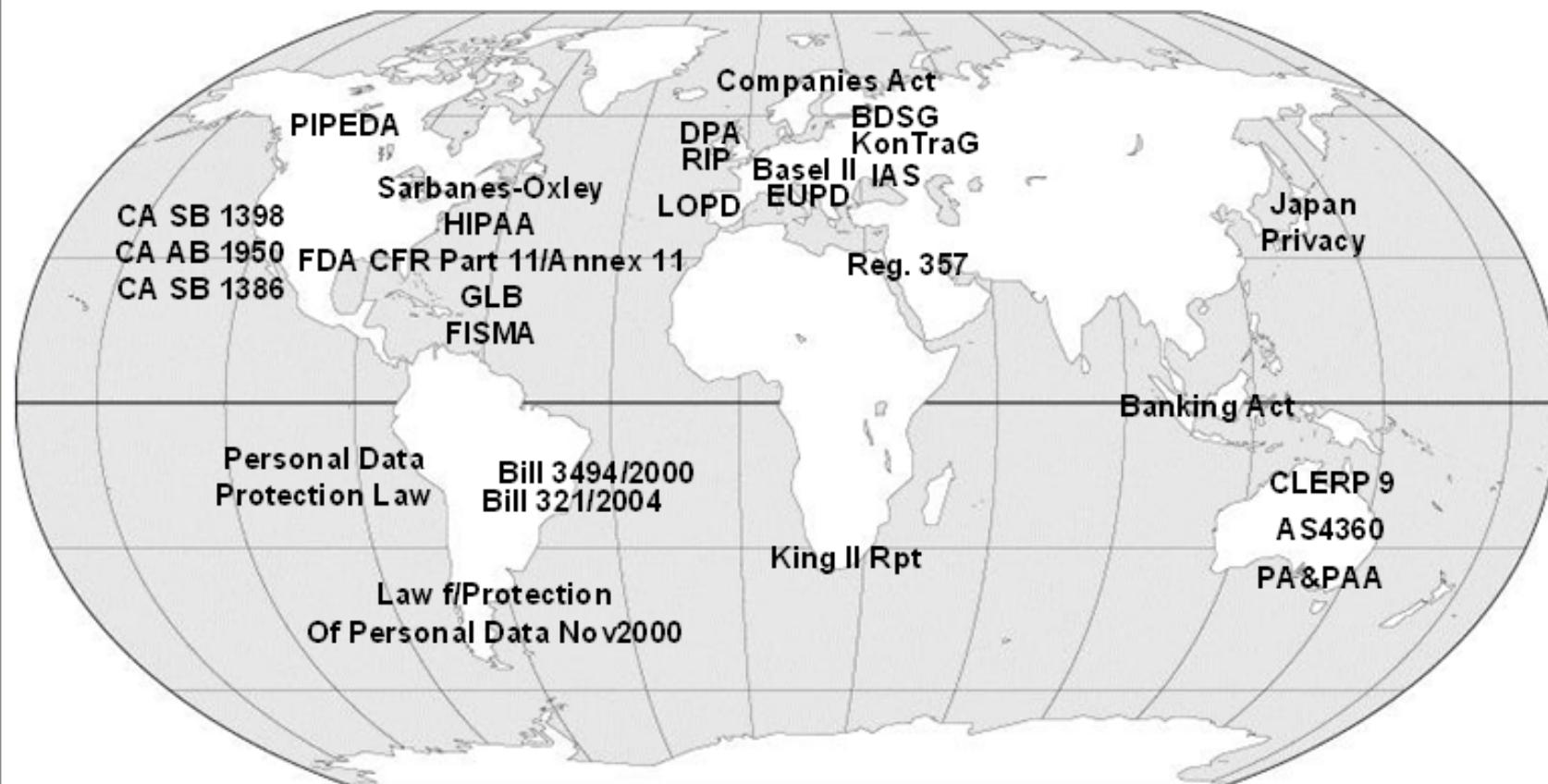
10-13 Maturing IT Governance

> 13 Top performer

Source: P. Weill MIT + GG

Other Laws and Regulations

Regulations/Compliance



Regulation: The Sarbanes-Oxley Act

SOX: An Act to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes.

SEC. 404. MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS.

(a) RULES REQUIRED.—The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall—

(1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and

(2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

(b) INTERNAL CONTROL EVALUATION AND REPORTING.—With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.



Summary – Take Home Message

- Risk management touches technology, processes, organisation, and management.
- The most important element of risk management is risk culture and risk awareness of people involved.
- Several standards and best practices for proper risk management exist, but they are subject to interpretation for every application context.
- IT security is an important source for risk mgmt.
- IT Security & IT Risk are embedded in overarching Governance and Compliance frameworks and standards.

Presentation /Defense of Lecture Project

Risk and Security Management – HS 2012

Detecon Consulting



Risk Culture, Security Awareness, Lecture Project Results, and Exam Preparation / Q & A

Risk and Security Management – HS 2012

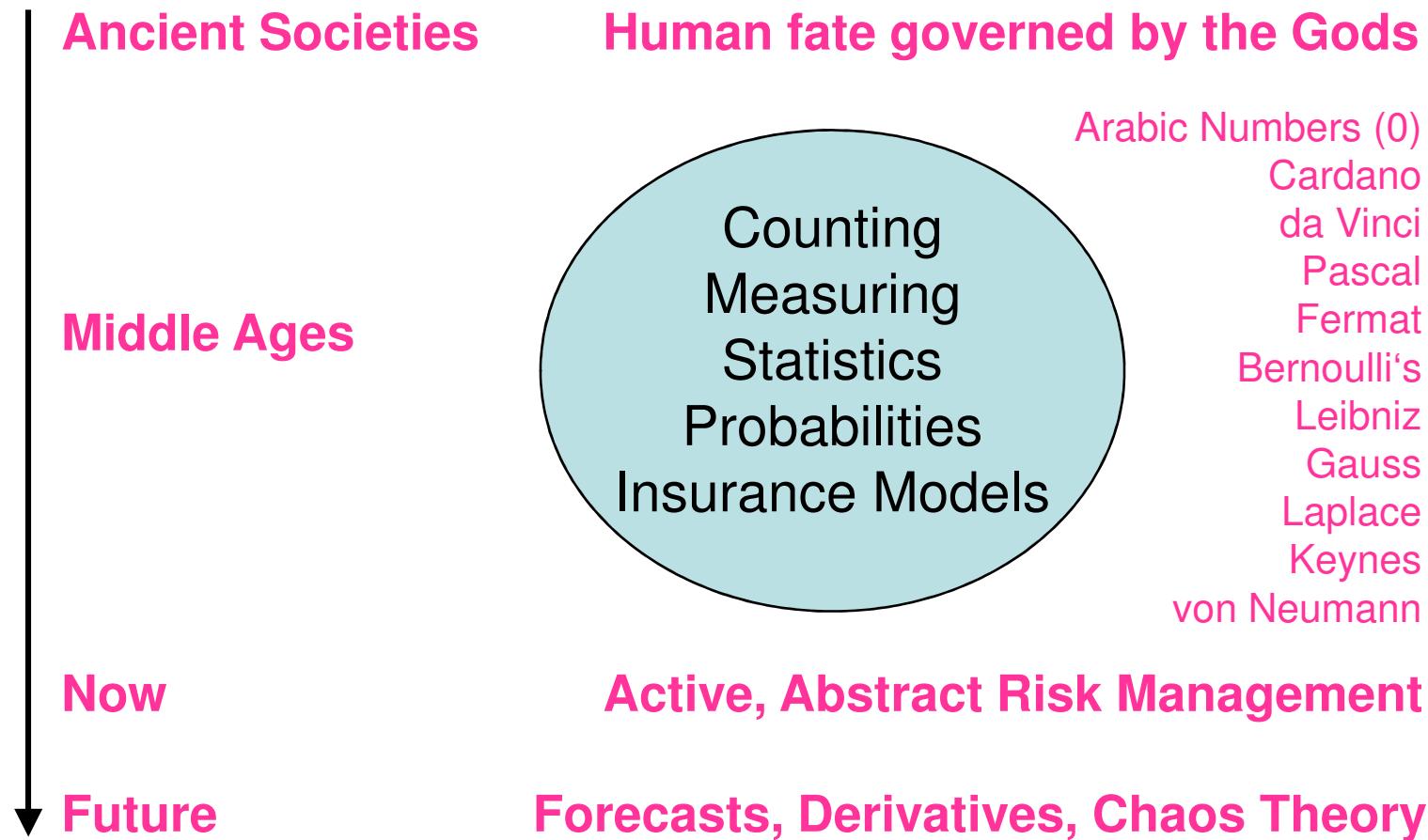
PD Dr. Hannes P. Lubich



Security and Risk Culture / Awareness



Our History of Risk Taking



What is a “Risk”?

- The conscious or unconscious acceptance of a loss within defined bounds in relation to a probability of the loss occurrence.
- Potential Risk Management by:
 - Avoiding (stay in bed, don't drive, ...)
 - Transferring (Insurance, body guard, ...)
 - Limitation (take preventive measures, ...)
 - Acceptance (formal, documented act)
 - Ignorance (look to the other side, ...)

depending on the type of risk and the accepted risk culture.

Risk Types



Abstract versus Concrete Risks



Abstract versus Concrete Risks



„Hidden“ Risks



Determining our Risk Culture

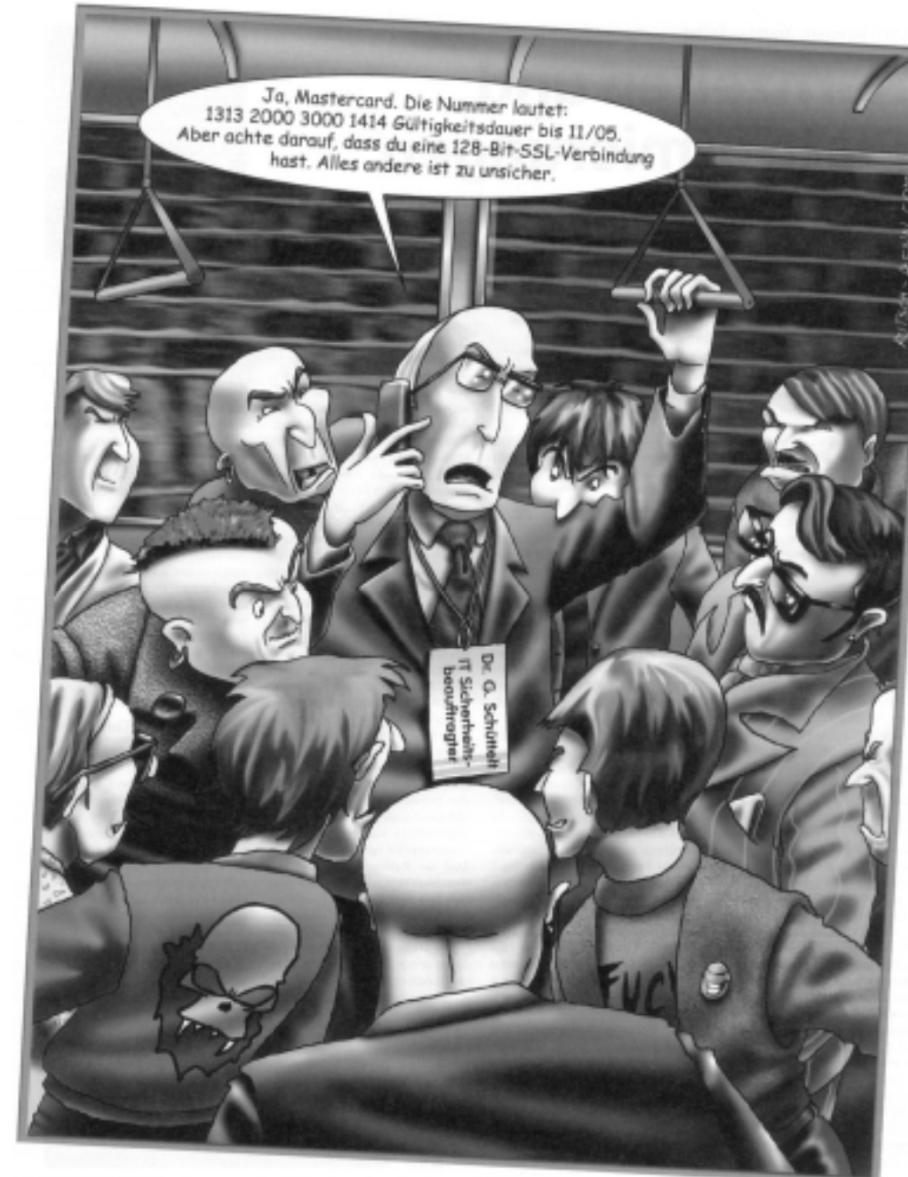
- Strategies to handle concrete risks (driving too fast, walking on ice) stem from our own social background, while strategies to handle abstract risks (IT, stock brokering) as well as group risks require detailed analysis.
- Our personal, business, legal and societal risk management is based on learning from incidents.
- We tend to ignore risks for which we do not have a solution.
- The faster we invent new technologies, the bigger the gap becomes between risk potential and risk management.



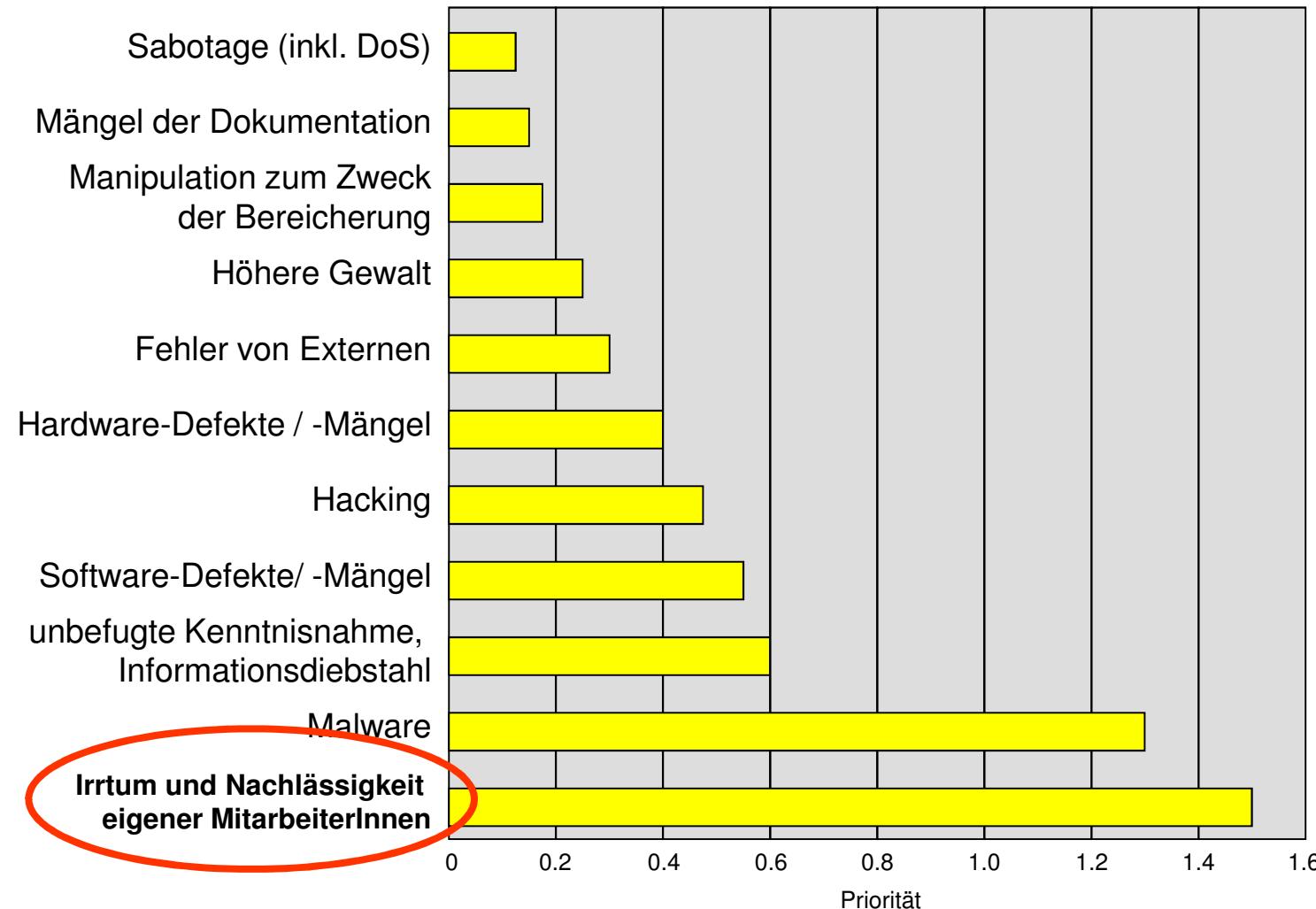
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Risk Awareness

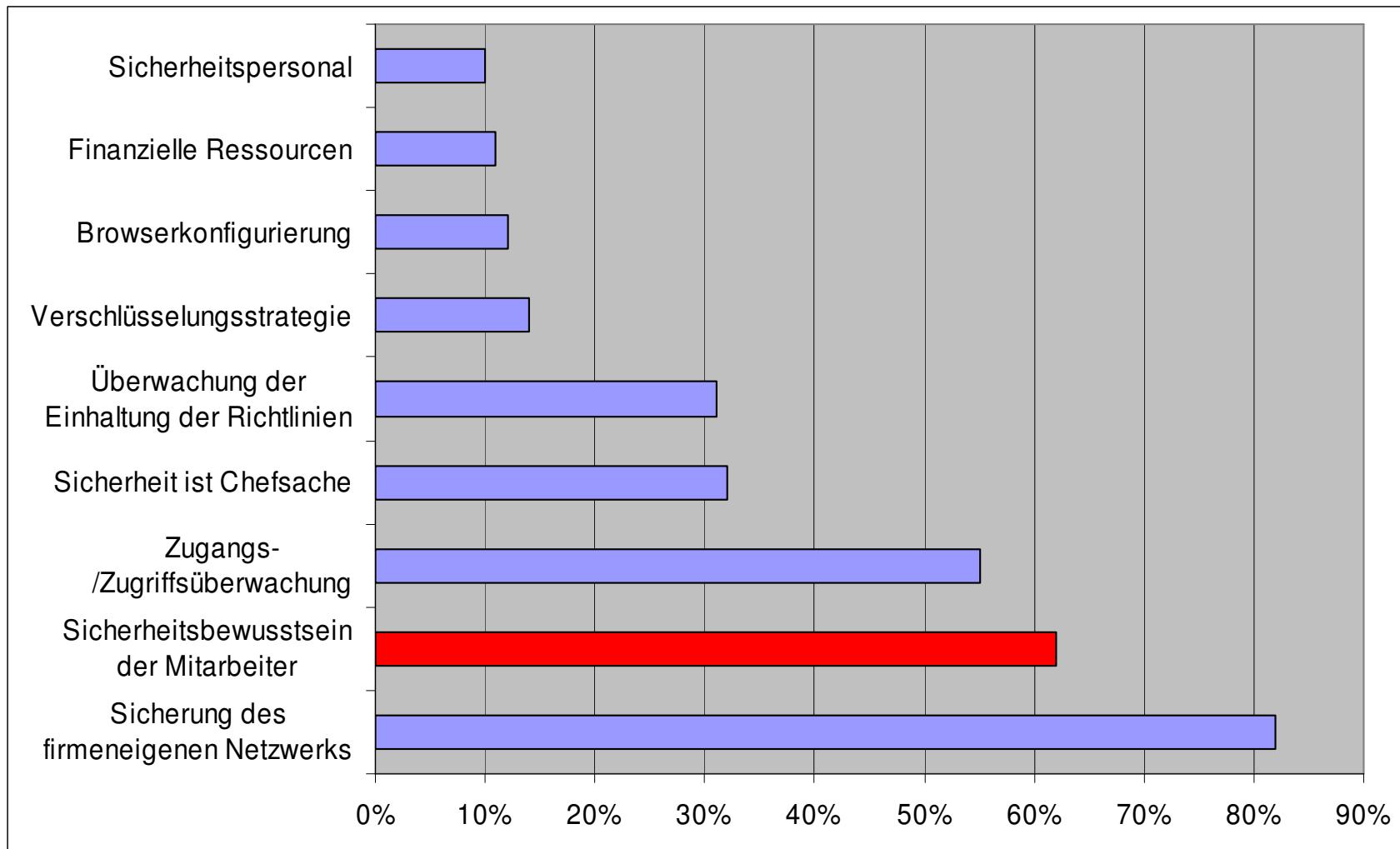




Why is Awareness Important?



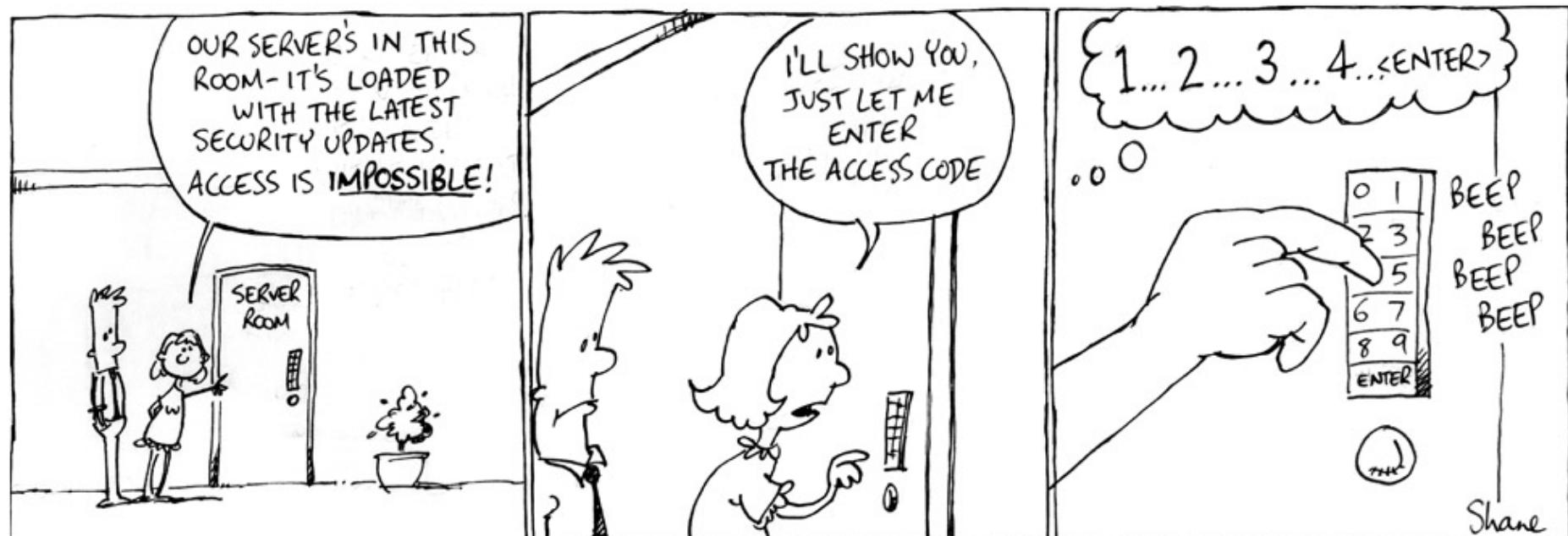
Why is Awareness Important?



How to Increase Security Awareness?

- Sustainable campaigns (by recipient group), e.g.:
 - Social engineering
 - Malware: viruses, trojans, worms, spyware, phishing, ...
 - Wireless networks (WLAN, Bluetooth, ...)
 - Secure Internet use (e-mail, e-banking, etc.)
 - Secure device handling (PC, notebook, smart phone, PDA, ...)
 - Dealing with confidential data (creation, transfer, use, disposal)
 - Personal discipline: clear desk policy, passwords, screensavers etc.
- Reviews, audits, computer-based trainings and tests
- Integration into performance appraisal, remuneration, etc

Remember: It Could Also Happen to You!



Copyright 2005

www.ShaneCollinge.com

Pause



Lecture Project Results



Exam Preparation: Hints, Q & A



Famous Last Words

- This lecture has covered a lot of material – each of which would warrant a separate lecture → “read on”.
- There are few “back & white” decisions, IT security means dealing with ambiguity → “don’t despair”.
- IT security is a growth area with interesting career paths (with business know-how and experience) → “just do it”.

