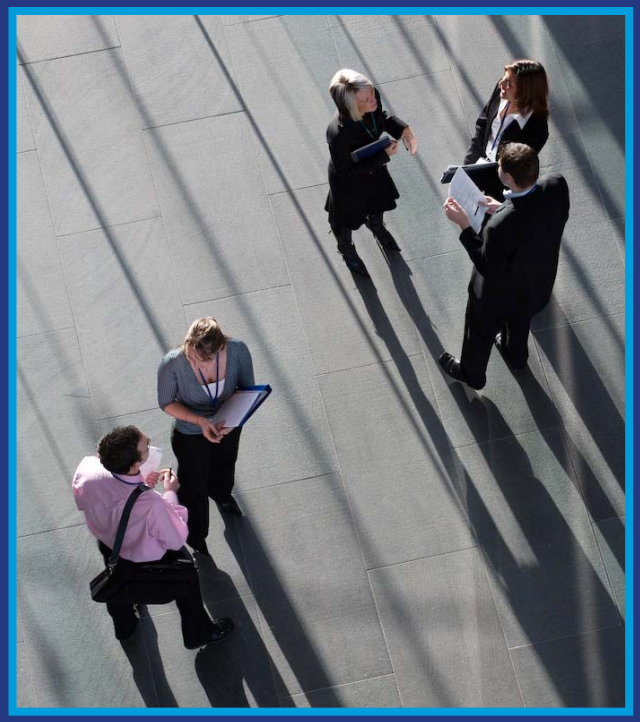
TROOPERS 08

get skilled, or get owned

The data went down the drain



Can something be learned from the Lichtenstein tax affair?

Presenter: Dror-John Roecher

My Personal Disclaimer

There are many rumors regarding what happened.

There are many unanswered questions regarding what happened.

For this talk we assume that what is publicly known is what acutally happened.

The ideas & opinions presented are my own and do not represent my employers‘ views or opinions.

Agenda

1. The Script
2. The InfoSec Incident
3. Risk Management view on the incident
4. Controls with regard to Data Leakage
5. Technical Data Loss / Data Leak Prevention
6. Could Lichtenstein have been prevented?
7. Lessons Learned

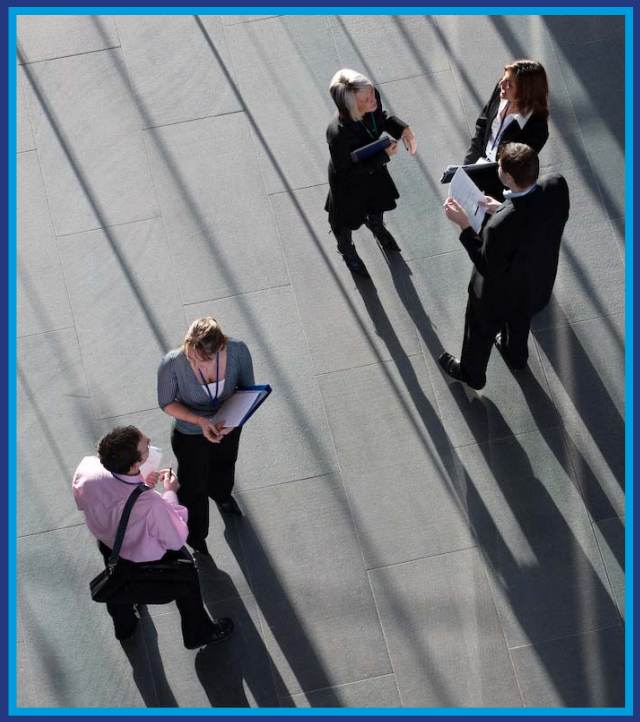
Agenda

1. The Script
2. The InfoSec Incident
3. Risk Management view on the incident
4. Controls with regard to Data Leakage
5. Technical Data Loss / Data Leak Prevention
6. Could Lichtenstein have been prevented?
7. Lessons Learned

TROOPERS 08

get skilled, or get owned

The script



What happened?

Who was involved?

The Actors

Mule: Mr. Kieber

Intelligence: BND

Tax Crime Investigation

A Bank: LGT

Legal Prosecution

Wealthy Individuals

The Stage

Sells DVD

Passes DVD on as „administrative assistance“

Calls on legal prosecution

Starts tax evasion Investigation

Found trust with LGT to evade German taxes

Copies data regarding trusts/accounts on DVD

Common questions…

Did the BND break German or Lichtenstein law?

Did Mr. Kieber break Lichtenstein law?

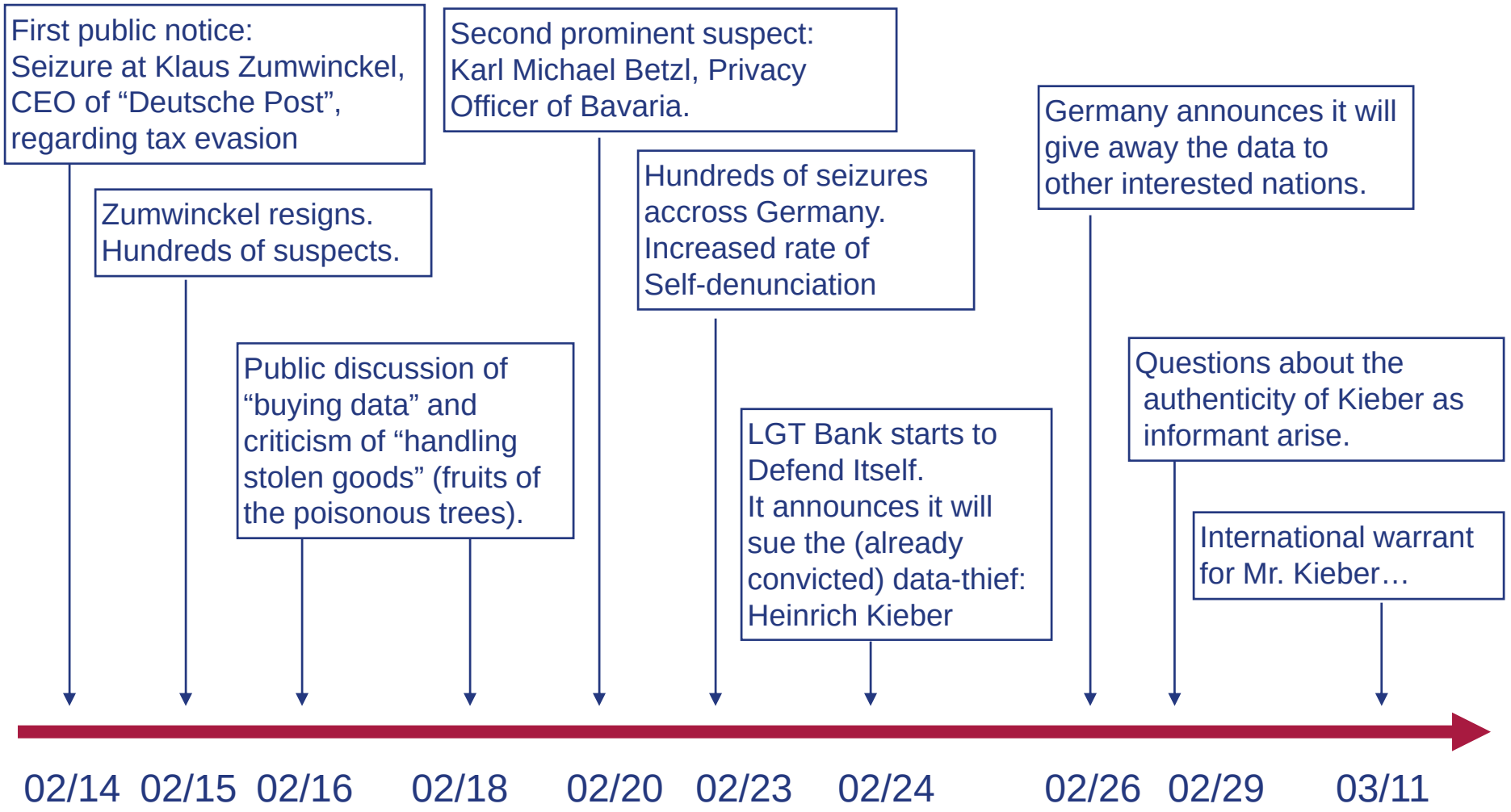
Was the action taken by the BND legitimate?

The answer to all these questions is: **I don’t care.**
Whether or not the players acted within legal boundaries or not is not relevant:

Incidents don’t care about “legality”

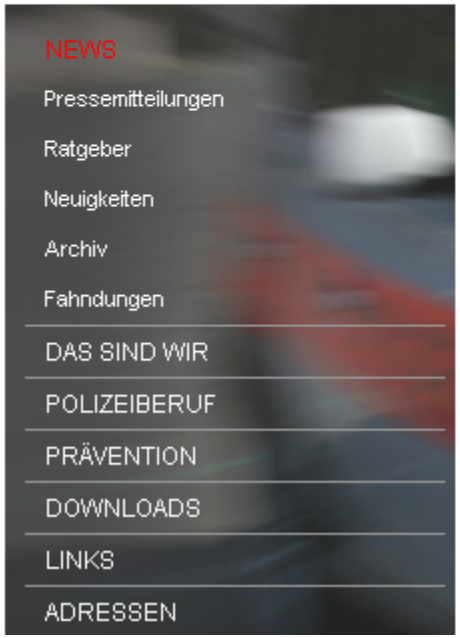
Incidents don’t care about “legitimacy”

Chronology ([1], [2], [4], [5])



Looks like a really „bad guy“ [5]

Sicher. Ihre Landespolizei



News > Pressemitteilungen

Pressemitteilungen

Öffentliche Fahndung nach Heinrich KIEBER

11.03.2008 -

KIEBER wird dringend verdächtigt, zum Nachteil einer Liechtensteiner Treuhandfirma Kundendaten ausgekundschaftet, sich verschafft und ausländischen Behörden preisgegeben zu ha KIEBER soll gemäss Medienberichten vom Deutschen Bu nac st (BND) er neuen Identität und neuen Rei ku estatte sein.

Es wi t, E nis halt KIE ER der Landes des ten dienststelle zu melden. n KIEBER besteht ein i er hl, wesh festzunehmen ist. Die liechtensteinischen Strafverfo behörde unverzüglich die Auslieferung von KIEBER begehren.

WANTED

STECKBRIEF

Personendaten

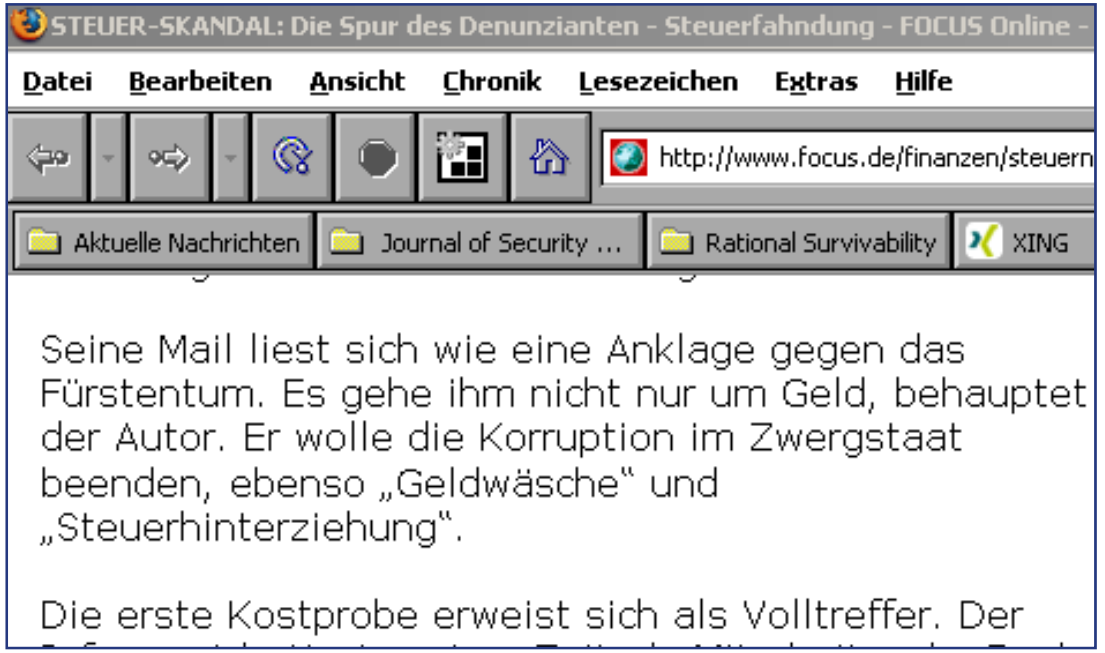
Name: Heinrich KIEBER
Geschlecht: männlich
Geburtsdatum: 30.03.1965
Staatsangehörigkeit: Liechtenstein

Personenbeschreibung

Mr. Kieber's Motivation?

According to [3]:

- Money
- Help stopping
  - Tax evasion
  - Corruption
  - Money laundering



Mr. Kieber's history… [6], [7], [8]

1997 International warrant against Mr. Kieber for a CHF 600.000 check-fraud in Spain.

04/2001 – 01/2003 LGT employee: tasked with the digitalization of paper-based account data.

2003 attempted extortion against Lichtenstein (tried to get 2 fake passports in order to escape the international warrant).

2003: Turned himself in to Lichtenstein criminal prosecution.

Mr. Kieber's history… [6], [7], [8]

2004: Pleaded guilty at trial, promised to return all stolen (LGT) data, was sentenced to 1 year prison (3 years according to some sources).

10/2004: Spanish International warrant canceled.

11/2005: Procedures in Spain discontinued.

01/2006: First Email to BND offering data…

More questions…

If Mr. Kieber worked at LGT from 2001-2003, how come the BND claims to have data up to 2005?

Was/is there an other informant?

Who leaked Mr. Kieber's name and why?

The answer to all these questions is: I don't care – for the scope of this talk, these questions are not relevant: **The data was disclosed, regardless of personal history / political motives.**

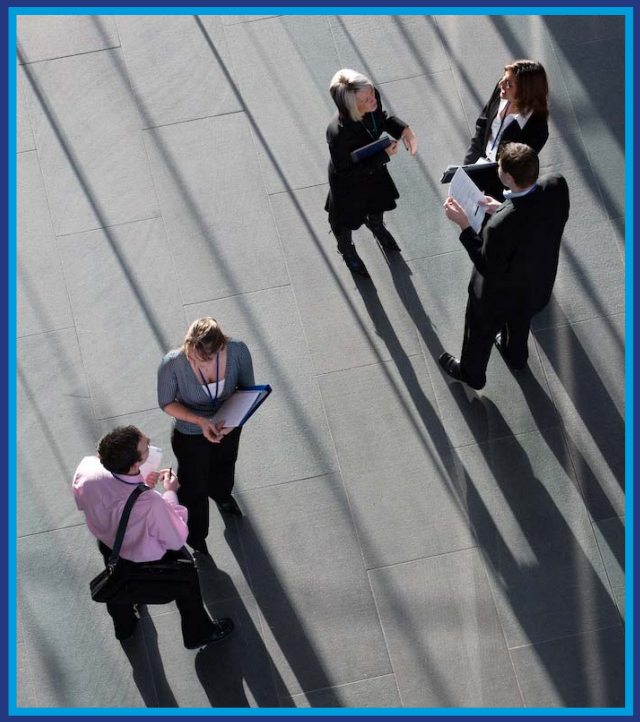
Agenda

1. The Script
2. The InfoSec Incident
3. Risk Management view on the incident
4. Controls with regard to Data Leakage
5. Technical Data Loss / Data Leak Prevention
6. Could Lichtenstein have been prevented?
7. Lessons Learned

TROOPERS 08

get skilled, or get owned

The InfoSec Incident



Data Leakage / Data Loss

What happened in Lichtenstein is a case of

Data Leakage / Data Loss

This can happen (and it does) in many different ways:

- Accidentally
  - Loss of data medium (USB-stick, etc.)
  - Unintended disclosure (via email, mail to wrong recipient, etc)
  - …
- Deliberately
  - “Business breaks security” approach
  - Thief / Hacker steals data / laptop / USB-stick
  - Insider steals data / laptop / USB-stick / printer-output
  - Dumpster diving
  - …

Data Loss / Data Leakage can be a worst case scenario (think stolen identities, credit cards, r&d data …)

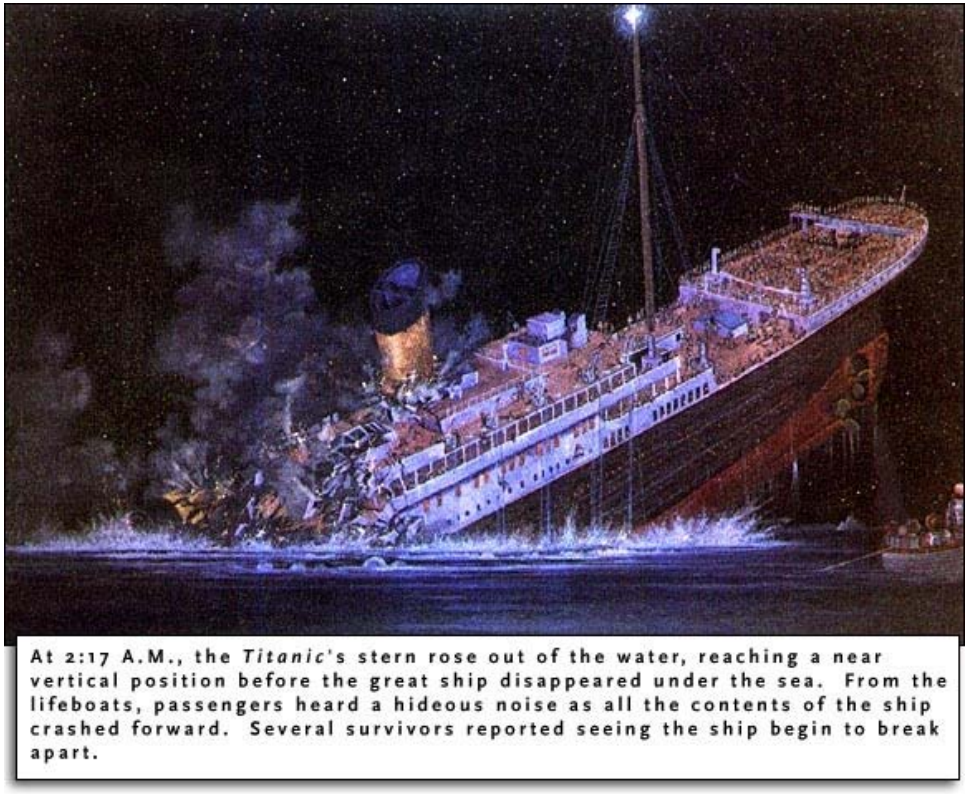
An incident usually happens…

A worst-case incident usually happens, when…

Risk is not properly controlled

AND

A couple of minor defects coincide



“Minor” defects w/ respect to Lichtenstein

HR of LGT failed to check or failed to be alarmed by Kiebers’ background, even tough he was hired to digitalize sensitive data.

“System” to digitalize data did not prevent copying of data (whereas system pertains the whole setup, including organizational controls, physical security, monitoring, etc.).

At the 2004 trial, LGT failed to assure the complete return of all data (how that could have been accomplished – I don’t know).

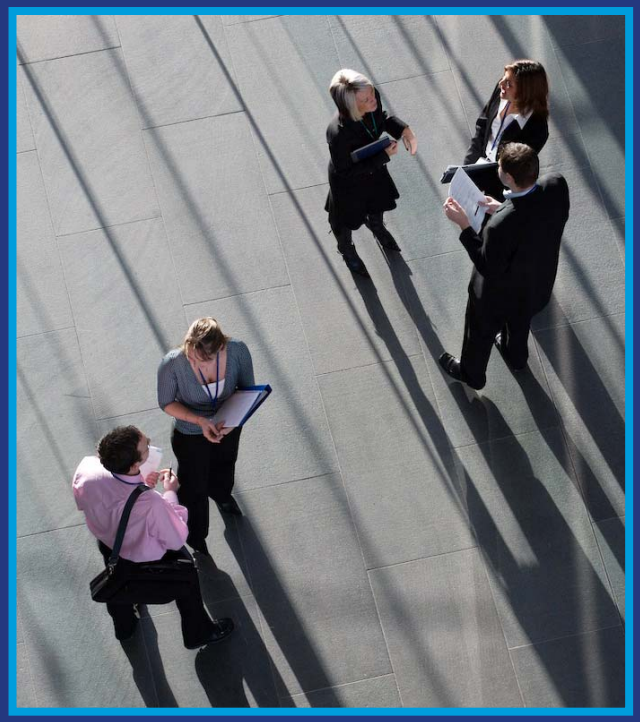
Agenda

1. The Script
2. The InfoSec Incident
3. Risk Management view on the incident
4. Controls with regard to Data Leakage
5. Technical Data Loss / Data Leak Prevention
6. Could Lichtenstein have been prevented?
7. Lessons Learned

TROOPERS 08

get skilled, or get owned

CISOs' / Risk Managers' Approach to the Lichtenstein Affair



Definitions: Threat, Risk & Vulnerabilities

Threats: Possible events with a negative impact. (E.g. “sensitive data is disclosed”).

Vulnerabilities: Circumstances which abet the “happening” of incidents. (E.g. “no classification of data present” – therefore no guideline for “what is classified?”)

Risk is always the risk associated with a threat and which is mitigated by controls.

Calculated risk and pyhsical control

- Threat: Trap is triggered, Impact: Death
- Vulnerability: Mouse is susceptible to cheese
- Mitigating Control: Helmet (physical control, reducing impact to headache)
- Risk: Probability x Impact (see next slide)

Simple Risk Formula

Risk(Threat) = Probability * Impact

How do controls come into place? Controls act either on the probability or on the impact…

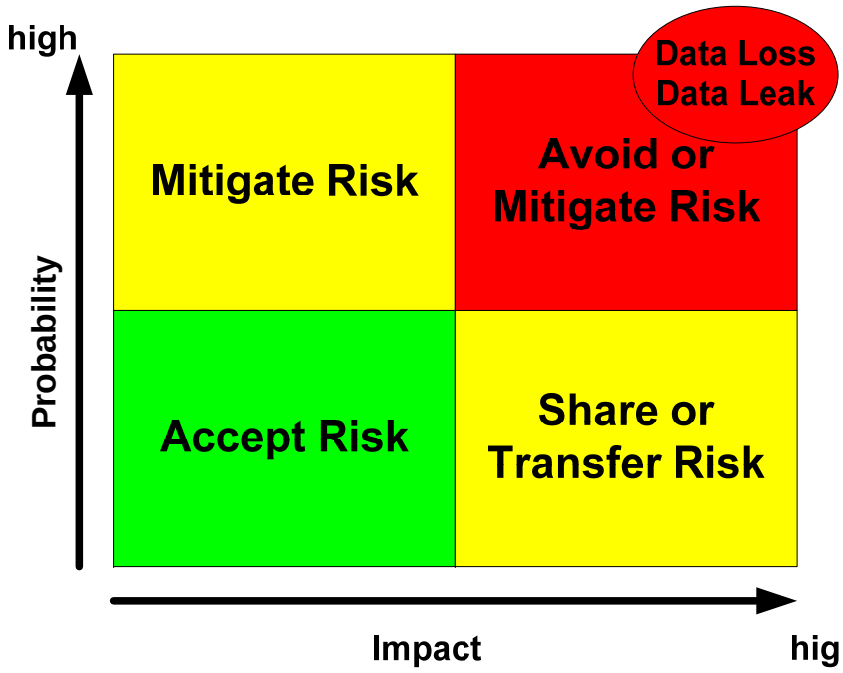
$$\mathbf{Risk = (P - Controls_P) * (I - Controls_I)}$$

Mitigating Controls

Controls can be grouped into:

- Managerial Controls
- Operational Controls
- Technical Controls

Risk Control Strategy



Managerial Controls

Address the design and implementation of the security planning process and security management

Management controls also address:

- Risk management
- Security control reviews

Operational Controls

Operational controls are those for operations and activities in such a way that they are conducted under specified conditions.

Operational controls may be documented through the use of work instructions, operational procedures or manuals.

Operational Controls

They include:

- Documentation
- Configuration and change management
- Incident response planning
- Disaster recovery planning
- Software development and test environment
- Outsourced facilities
- Personnel security
- Physical security

Technical Controls

Address technical issues related to designing and implementing security in the organization

Technologies necessary to protect assets are examined and selected

They include

- Identification and authentication
- Access control
- Audit and accountability
- …

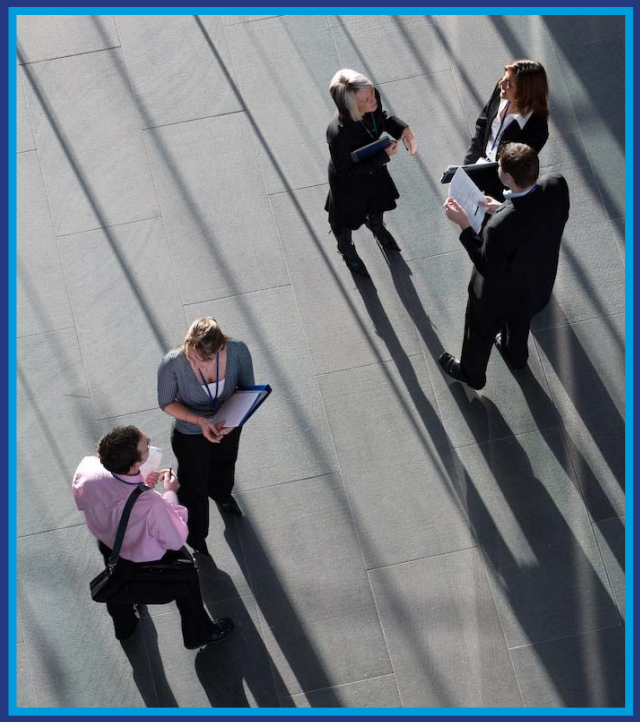
Agenda

1. The Script
2. The InfoSec Incident
3. Risk Management view on the incident
4. Controls with regard to Data Leakage
5. Technical Data Loss / Data Leak Prevention
6. Could Lichtenstein have been prevented?
7. Lessons Learned

TROOPERS 08

get skilled, or get owned

Controls with regard to Data Leakage



Threat: Deliberate Data Leakage

- Least Feasible
  - Memorizing data: writing it down at home
  - Manual notes: taken home/emailed home
- Somewhat Feasible
  - Paper copied: taken home - then digitized
  - Photographs: taken home on DigiCam
  - Screenshots: printed & taken home/emailed home
- Most Feasible
  - Data attached to Email: then mailed home
  - Data copied: to USB/CD/DVD, taken home

Most work

Least likely

Least work

Most likely

Managerial Controls

Perform Risk Analysis to identify and mitigate the risks. Forms the basis of all other controls.

Impact rating * Probability rating = Risk Level			
Impact Rating Ranges		*	**Probability Ranges**
High	10 -- 7		10 -- 7
Medium	6 -- 4		6 -- 3
Low	3 -- 0		3 -- 0

	H	10	0	10	20	30	40	50	60	70	80	90	100
		9	0	9	18	27	36	45	54	63	72	81	90
		8	0	8	16	24	32	40	48	56	64	72	80
		7	0	7	14	21	28	35	42	49	56	63	70
Impact		6	0	6	12	18	24	30	36	42	48	54	60
	M	5	0	5	10	15	20	25	30	35	40	45	50
		4	0	4	8	12	16	20	24	28	32	36	40
		3	0	3	6	9	12	15	18	21	24	27	30
		2	0	2	4	6	8	10	12	14	16	18	20
	L	1	0	1	2	3	4	5	6	7	8	9	10
			0	1	2	3	4	5	6	7	8	9	10
			L					M					H
								Probability					

Overall Risk	Risk level
41-100	High
20-40	Medium
0-19	Low

Operational Controls

Policies:

- No Email from “data digitizing” system (“prohibited use policy”)
- Limitation of USB devices (“prohibited use policy”)
- No camera/mobile phone on premises (“prohibited use policy”)

HR

- Thorough background-screening of employees

IT-Operations

- No CD-RW on “data digitizing” system (“minimal machine”)
- No copier accessible for data-digitizing personnel or in data-digitizing-premises (“least privilege”)

Technical Controls

General Policy Enforcement

No USB support in “data digitizing” system: Easy to disable USB, mature “device control products” available.

No Email from “data digitizing” system (policy enforcement): Easy, no additional products needed. Simple case of suppressing connectivity / can be handled at the network layer.

Targeted Technical Controls

Data Leak/Data Loss Prevention System (DLP): a new technology

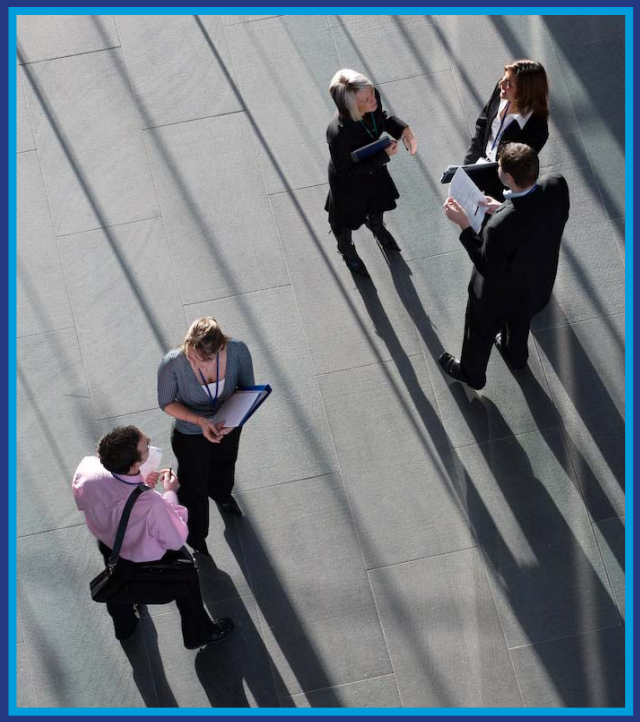
Agenda

1. The Script
2. The InfoSec Incident
3. Risk Management view on the incident
4. Controls with regard to Data Leakage
5. Technical Data Loss / Data Leak Prevention
6. Could Lichtenstein have been prevented?
7. Lessons Learned

TROOPERS 08

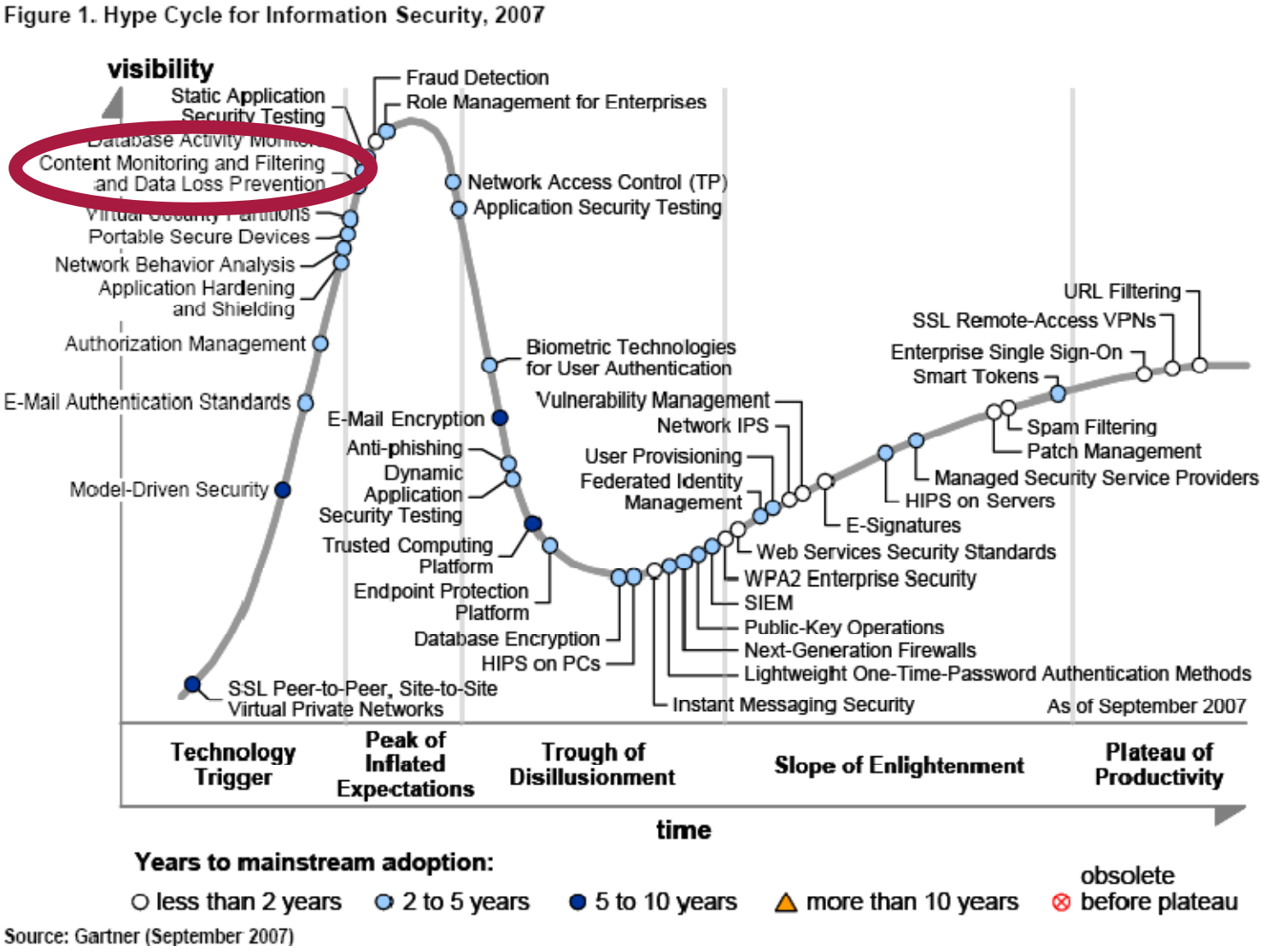
get skilled, or get owned

Technical Data Loss / Data Leak Prevention



How it works

Security hype cycle



DLP vs Digital Rights Management (DRM)

DLP is basically a spin-off of DRM.

The “music industry” wanted to protect music from illegal copying and developed DRM which enables the provider to define rights regarding copying, playing, converting, etc...

Example: Microsoft Zune Player DRM [9]

DLP is “just a flavor” of automatic DRM.

Definition of DLP [10]

"Products that, based on central policies, identify, monitor, and protect data at rest, in motion, and in use, through deep content analysis."

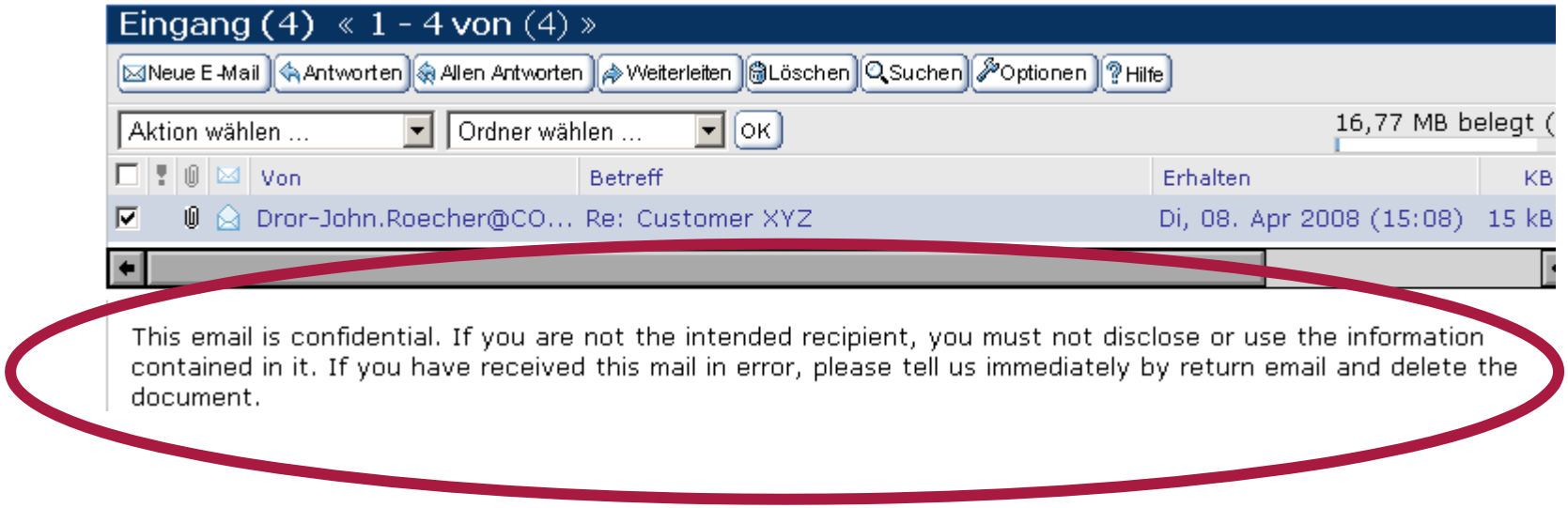
Key concepts:

- Central Policy
- Deep analysis
- Broad coverage across platforms
- Protect data in motion & at rest & in use

Central Policy / Data Classification

Creation, Management and Workflow for the definition of the policy:

Needs data classification scheme and associated actions:



Deep Analysis

Deep Analysis means:

- Look at the *Content* and *Context* of the analyzed data:
  - Content: The actual content of the data
  - Context: Context in which the data is used (source, destination, time/date, meta-data, etc.)

Content-Analysis is focus for DLP.

Content Analysis Techniques [10]

Rule-Based/Regular Expression (look for an expression)

Database Fingerprinting / Exact Data Matching (e.g. look for specific CC-Number)

Exact File Matching (look for a specific file via “hashes”)

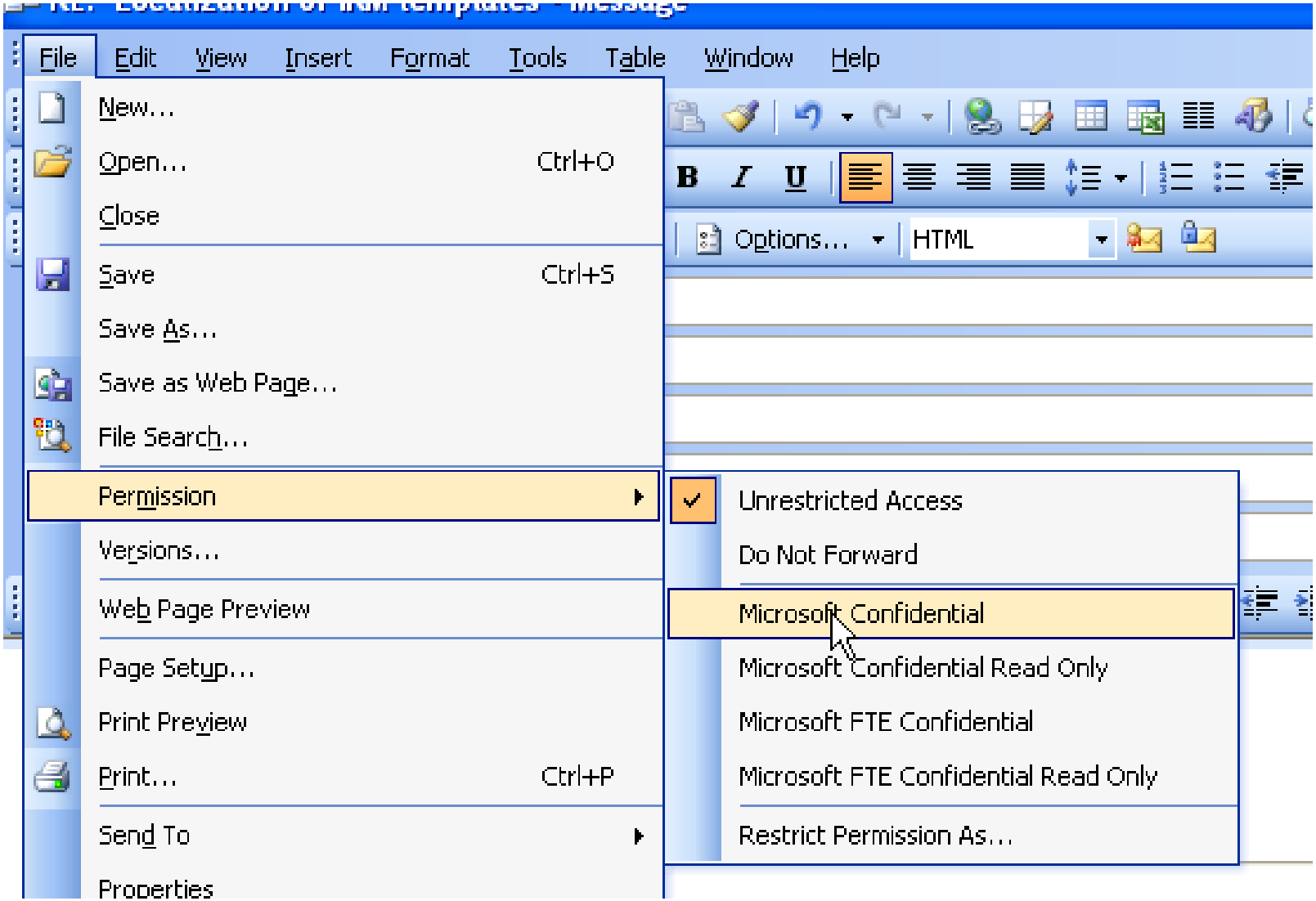
Partial Document Matching (look for specific parts of a document)

Statistical Analysis

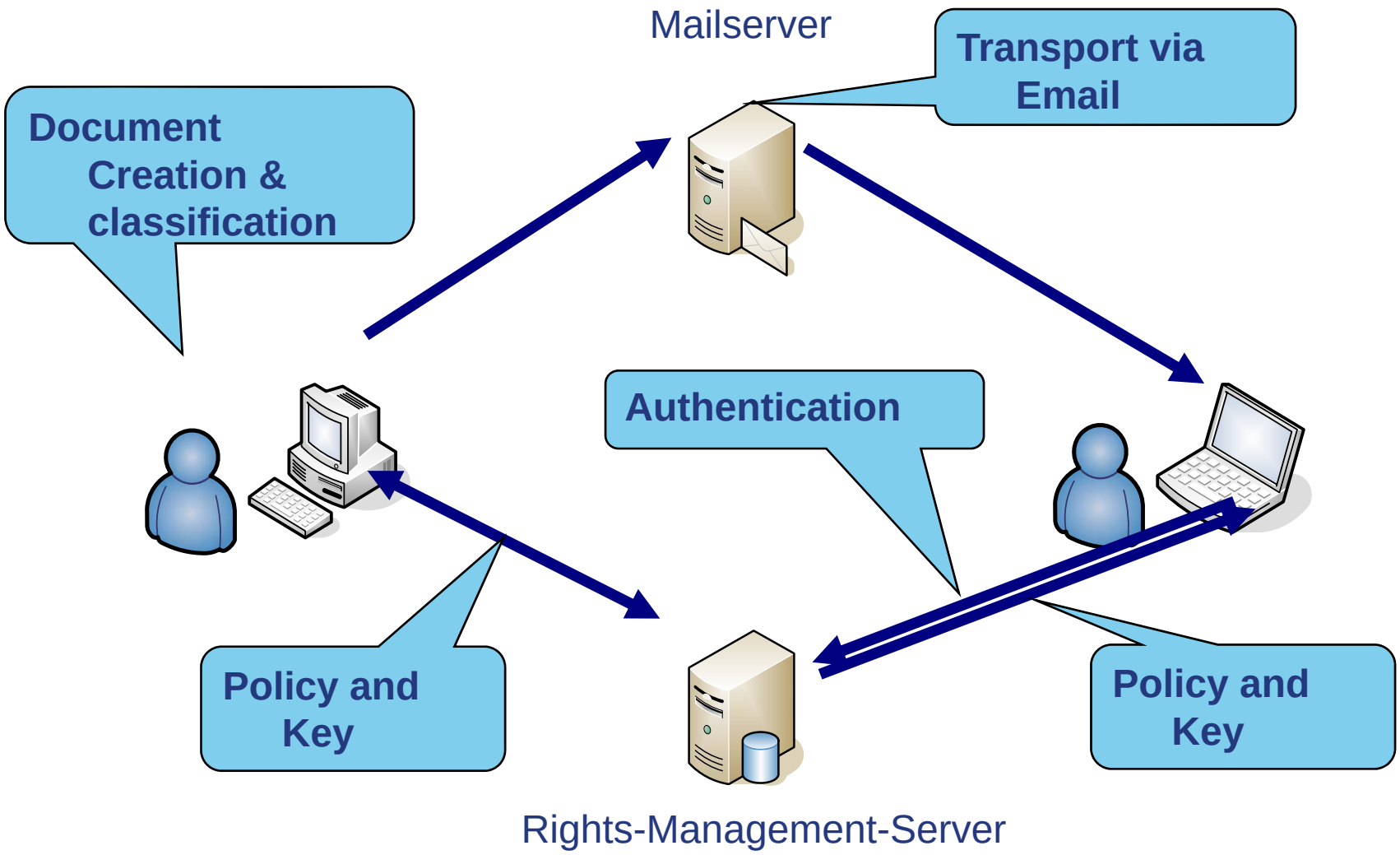
Categories (prebuilt categories with rules & dictionaries for specific types of sensitive data - e.g. HIPAA, PCI).

Manual Classification by originator

Manual Classification Example



An example for „manual classification“

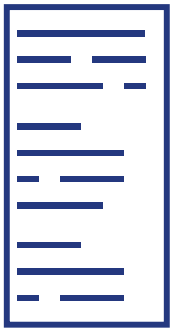


Fingerprinting & Detection

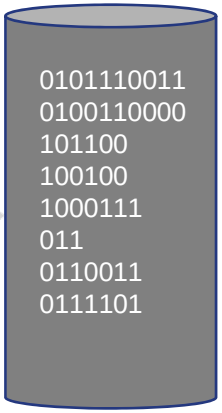
Fingerprinting

Database Record or Document

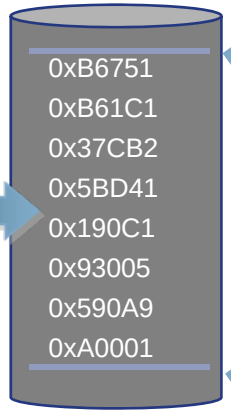
Extract



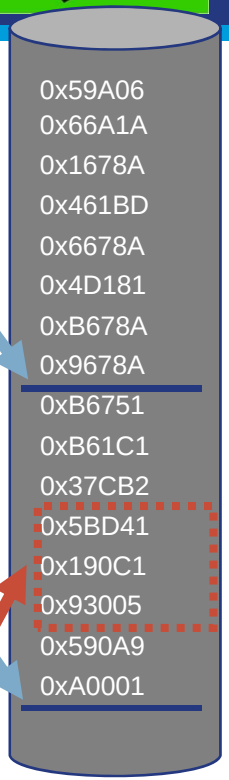
Algorithmic Conversion



Hash



Fingerprint Storage & Indexing



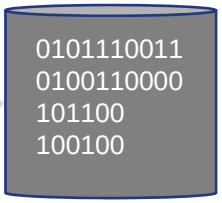
Real-Time Fingerprint Comparison

Detection

Outbound Content (E-mail, Web, Fax, Print, etc.)

Extract

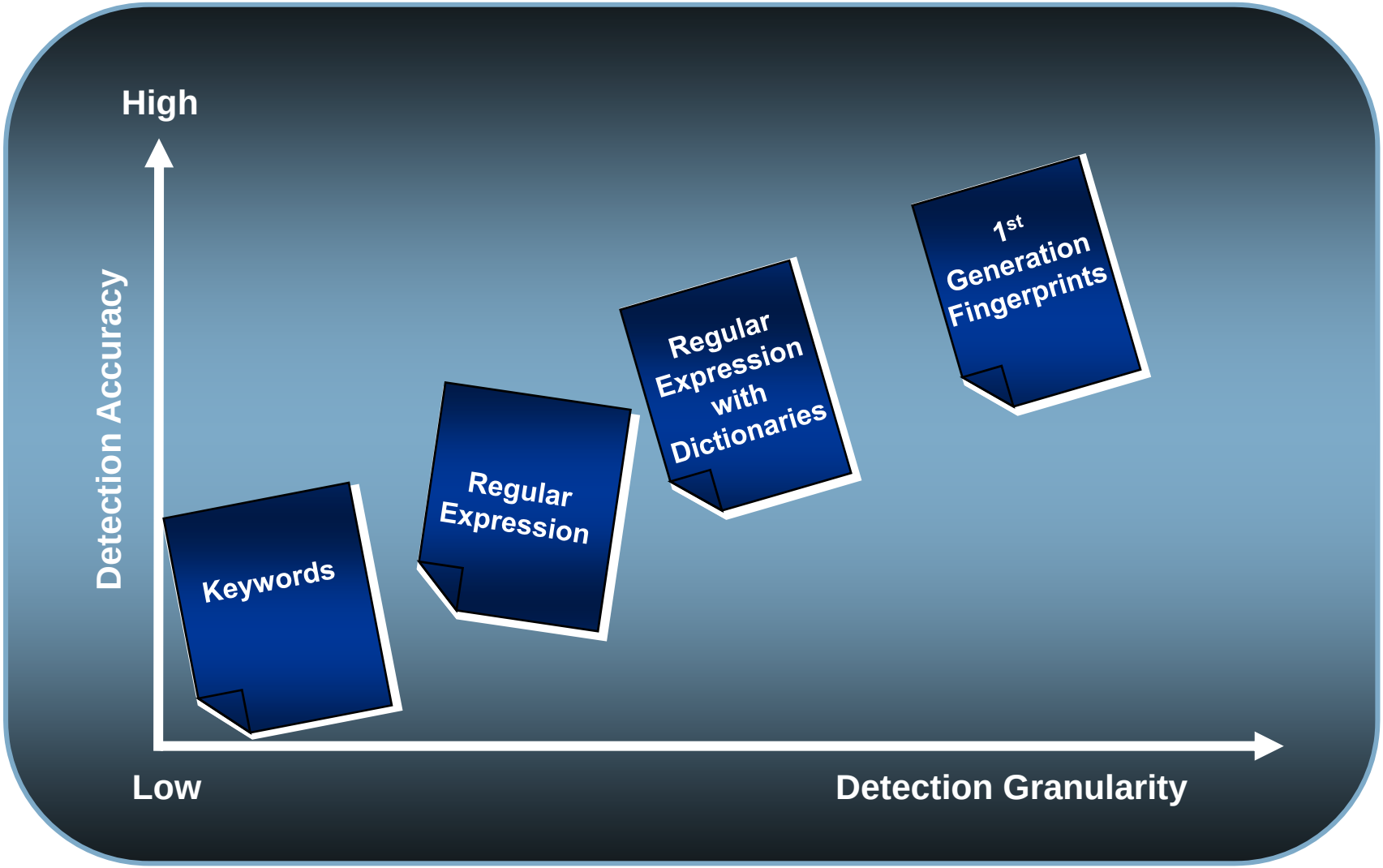
Algorithmic Conversion



Hash

Fingerprint Creation

Analysis Ranking



Broad Coverage

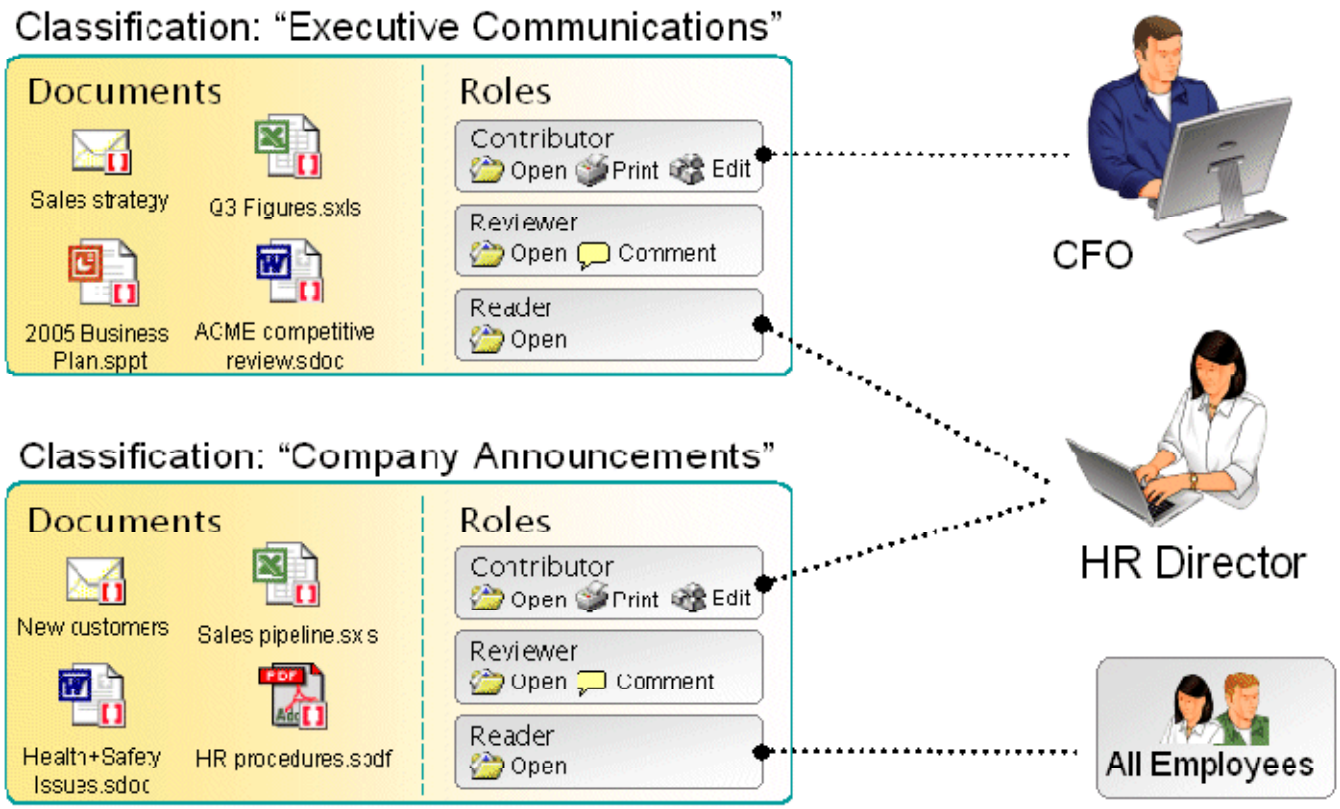
Operating System support (anyone got production data on Win98 boxes? Good luck!)

File type support (the more the better – but the more, the more parsers are needed, which might be used to attack the solution itself)

Nested files (embed a spreadsheet in a Word-Document and zip it – again a parsing problem)

At rest, in use & in motion (so obviously an agent on the clients is needed - and an inline box in the network-path – yet more points of failure)

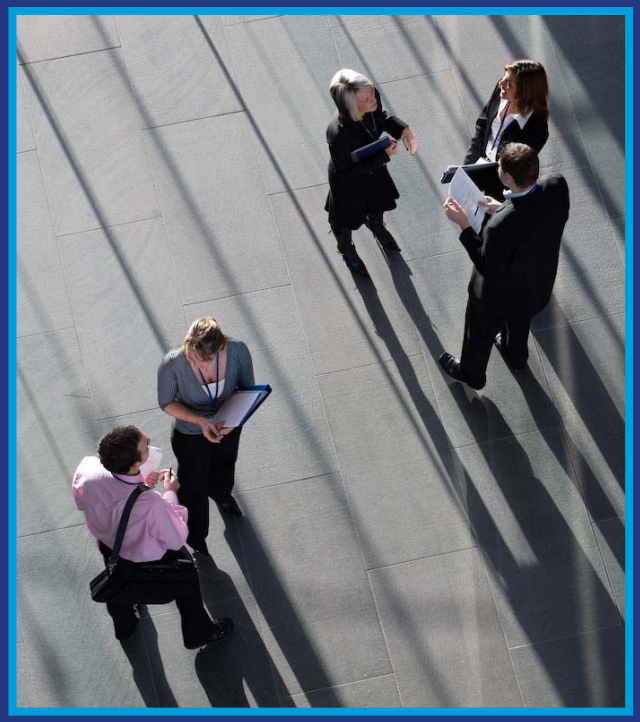
Role Based Access



TROOPERS 08

get skilled, or get owned

A critical view on DLP



Some critical thoughts on DLP

Not yet mature – lots of false positives (think of early-days Intrusion Detection Systems)

Yet another agent with high privileges and a parsing-engine: susceptible to attack resulting in system compromise

Added complexity – contradicts “Keep It Simple” paradigm of InfoSec

One more log-source: Incident Management, Monitoring adversely affected

More critical thoughts on DLP

One more Helpdesk-Problem: “I can’t mail that file!”

Doesn’t address the problem – it is just a fix to the symptoms (thinking of ‘nappies’ when hearing ‘leakage’?)

Needs working data classification – if classification already works, why do you need leak prevention?

How is encrypted traffic handled? With key escrow? (not again!)

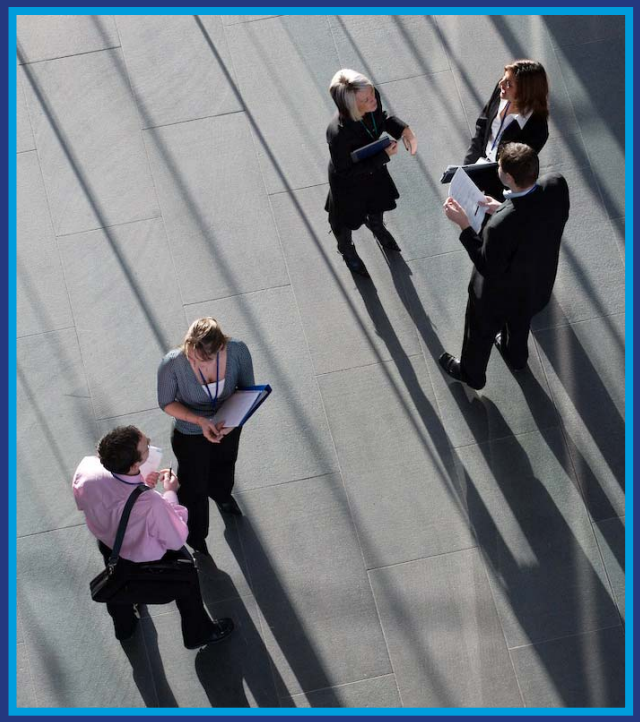
Agenda

1. The Script
2. The InfoSec Incident
3. Risk Management view on the incident
4. Controls with regard to Data Leakage
5. Technical Data Loss / Data Leak Prevention
6. Could Lichtenstein have been prevented?
7. Lessons Learned

TROOPERS 08

get skilled, or get owned

Could the Lichtenstein Data Leak have been prevented?



Prevention with DLP

Lichtenstein may have been preventable with a working DLP under the following circumstances:

- When digitizing the paper, the files are DLP-treated before they are written to disk – which means it needs to integrate into the scanning-application, or run in kernel-space to intercept file-create-operations.
- The DLP policy applies “copy/mail prevention” per default to the newly created files (maybe based on context, rather then content).
- The DLP rights don’t collide with the access-control of the Document Management System (DMS) which is used to store the digitized data.
- The DLP is able to enforce the protection within the used DMS.

Prevention with Classical Controls

Policies would not have worked because the offender was a criminal – criminals don't care about policies (policies are useful in other ways)

Disabling USB support on the machine would have stopped the easy way of copying

Disabling Email support on the machine would have stopped the easy way of copying

Access Control to copiers would have prevented making paper-copies

HR background screening would have prevented the offender being employed first hand (thereby eliminating the root cause of the leakage)

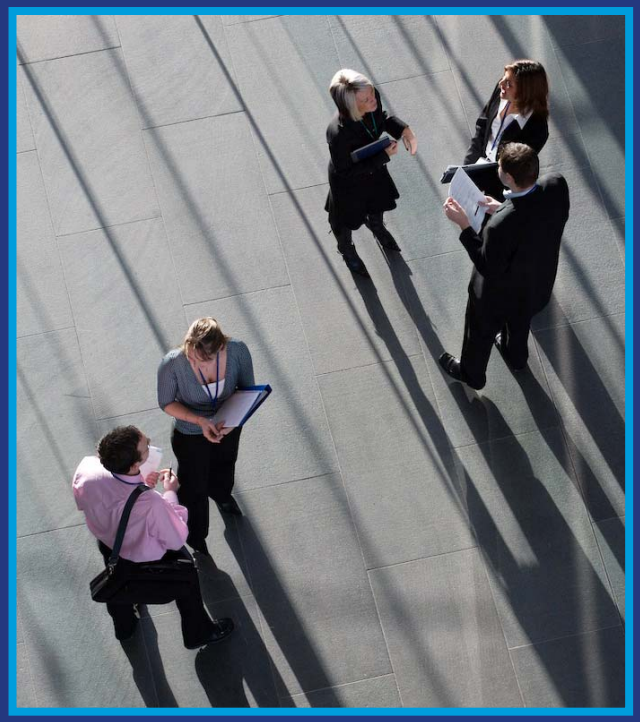
Agenda

1. The Script
2. The InfoSec Incident
3. Risk Management view on the incident
4. Controls with regard to Data Leakage
5. Technical Data Loss / Data Leak Prevention
6. Could Lichtenstein have been prevented?
7. Lessons Learned

TROOPERS 08

get skilled, or get owned

Lessons Learned



More is less…

Even though DLP may have been able to prevent the Lichtenstein InfoSec incident…

- It does not address the root cause (wrong people hired for the job)
- It addresses only some use-cases (what about non-digital data? What about encrypted data?)
- It adds another layer of complexity to security operations
- It requires another manageable agent with high privileges on the clients

Less is more

Classical Controls would have been better suited, because…

- They are able to address the root cause
- They do not add more complexity
- They apply to all data
- They mitigate risk beyond “Data Leakage” threats (e.g. USB enforcement also mitigates malware-infection threats)
- They are more mature and have a history of being manageable

Lessons Learned

Information is a valuable asset – for outsiders too.

Data Leakage has happened, happens today and will happen in the future.

“Interested parties” are willing to spend $$$ to get information.

“Interested parties” include national intelligence agencies.

Lessons Learned – continued

Offenders do not care about “legal restrictions”.

Risk analysis can help you to identify where the risks are.

HR is part of the overall security program – and needs to be made aware of that.

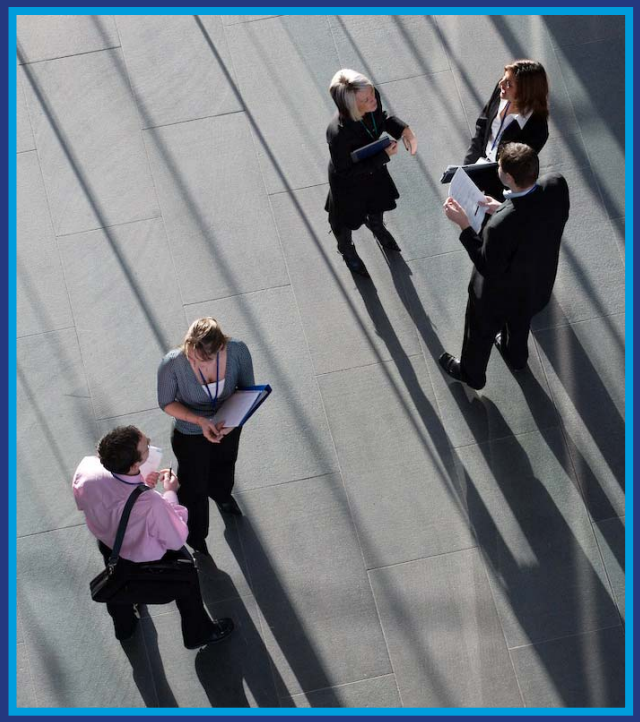
Classical Controls are usually still the better choice to get a grip on data leakage.

Technology (DLP) is not (yet) the answer.

TROOPERS 08

get skilled, or get owned

Questions? And Answers



Thank you for listening…

Dror-John Röcher

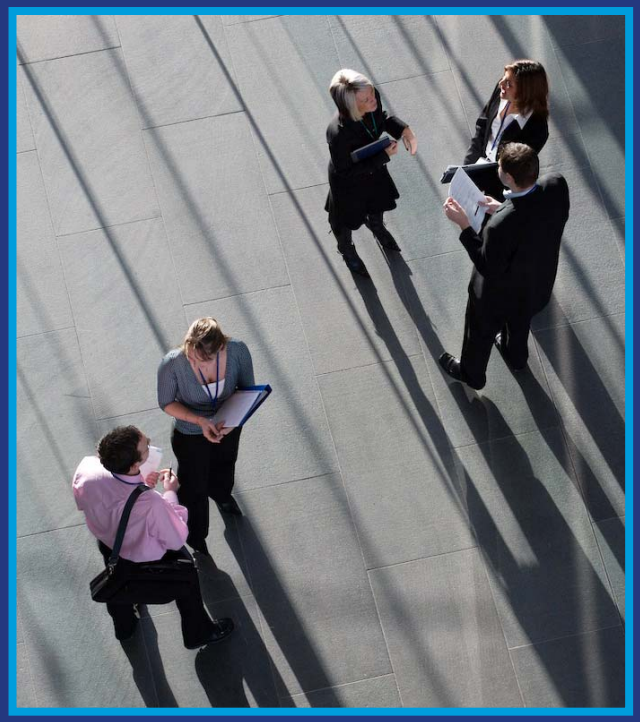
Computacenter
Services & Solutions

Mobile: +49 (0) 172 2382946
E-mail dror-john.roecher@computacenter.com

TROOPERS 08

get skilled, or get owned

References & QR-Codes



References / URLs

[1]: http://diepresse.com/home/wirtschaft/economist/365681/index.do

[2]: http://www.sueddeutsche.de/wirtschaft/special/674/159244/index.html/wirtschaft/artikel/523/161082/article.html

[3]: http://www.focus.de/finanzen/steuern/steuerfahndung/steuer-skandal_aid_262655.html

[4]: http://www.spiegel.de/wirtschaft/0,1518,537742,00.html

[5]: http://www.landespolizei.li/News/Pressemitteilungen/tabid/850/articleType/ArticleView/articleId/263/ffentliche-Fahndung-nach-Heinrich-KIEBER.aspx

[6]: http://www.heise.de/tp/r4/html/result.xhtml?url=/tp/r4/artikel/27/27381/1.html&words=LGT&T=LGT

[7]: http://de.wikipedia.org/wiki/Heinrich_Kieber

[8] http://www.handelsblatt.com/News/Recht-Steuern/Meldungen/_pv/_p/204872/_t/ft/_b/1395561/default.aspx/der-mann,-der-die-steuerdaten-klaute.html

[9] http://en.wikipedia.org/wiki/Zune

[10] http://securosis.com/publications/DLP-Whitepaper.pdf

QR-Codes (ISO/IEC18004)

All referenced Web-sites are available as QR-Codes (visual tags).

A tag-reader for your mobile devices can be downloaded here:

http://reader.kaywa.com/

A tag-reader for your Windows-PC can be downloaded here:

http://www.bctester.de/

URL QR-Codes

[1]

[2]

[3]

[4]

[5]

[6]

URL QR-Codes

[7]

[8]

[9]

[10]