

Incident Management

Trooper 2008
München

Oberstleutnant Volker Kozok

final word on language and nutrition

The Japanese eat very little fat and suffer fewer heart attacks than the British or Americans.

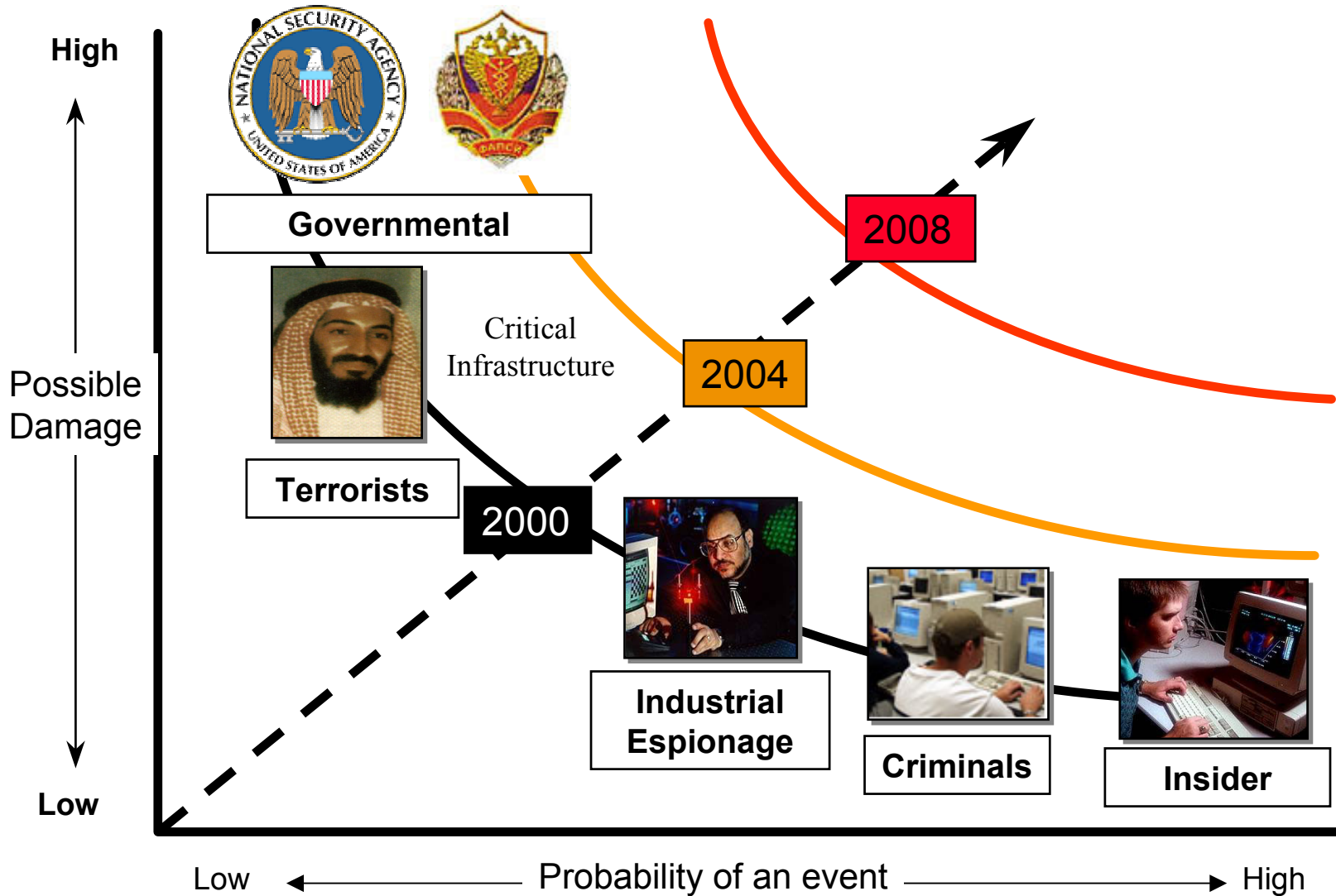
The French eat a lot of fat and also suffer fewer heart attacks than the British or Americans.

The Swedish drink very little red wine and suffer fewer heart attacks than the British or Americans.

The Italians drink excessive amounts of red wine and also suffer fewer heart attacks than the British or Americans.

**CONCLUSION: Eat and drink what you like.
Speaking English is apparently what kills you.**

Cyber Threat Profile



Be prepared!

THE CHRISTIAN SCIENCE MONITOR *BENNETT*

ALWAYS BE
PREPARED



A Question of definition

An incident is any event that deviates from the standard and expected operation of a system or service

Standard - who defines the standard?

Expected operation - I had expected Microsoft Fatal Error!

An incident is the act of violating an explicit or implied security policy.

Security policy – what's that?

My system can't be violated because I have no policy!

An incident occurs, if IT security is impaired/jeopardized by an IT security gap or a breach of IT security.

What is with the loss of credit or reputation?

What is with a breach of duty or infringements?

A Definition with questions

What can be happen?

What is the risk for my division or company?

How can I minimize the risks?

If IT-Security, Personnel Data Protection, Security Service, Disaster Recovery ... doesn't work – what's than?

How can I react if my company is impaired or jeopardized?

What is an incident?

Incident Categorization

- Increased access
- Disclosure of information
- Corruption of information
- Denial of service
- Theft of resources

Increased access

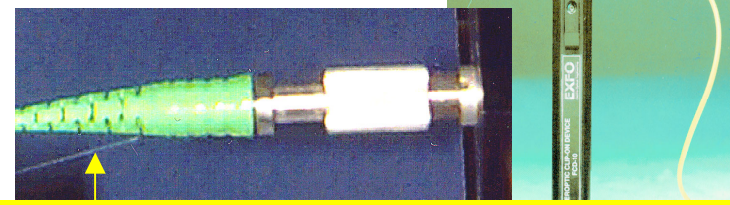
War Driving
Deutsche Ausgabe

Mit einem Vorwort von Jeff Moss
Preskott & CEO, Black Hat Inc.

Ch.	WEP	Type	SSID	Name	Vendor	DBP	Stufe	Latitude
220F9022	1	AP	AirView	Higgy Dome	Agere (Lucent)Ornoco	20		
220F9088	3	AP	AirView	airViewChe	Agere (Lucent)Wirel,4H	20		
220F90E8	11	AP	AirView	AP2 Frater's Inc. Apartment	Agere (Lucent)Ornoco	27		
220F909C	3,5	AP	AirView	AP2 Frater's Inc. Apartment	Agere (Lucent)Wirel,4H	46		
90A429BA	6	Yes	Alma2	Class (Airsoft)	20	N27.413520	W1	
90B549FE	10	AP	Alma2	Class (Airsoft)	20	N27.512280	W1	
90A30808	1	AP	alpha	Class (Airsoft)	32	N27.412748	W1	
90A90309	4	AP	alpha	Class (Airsoft)	40	N27.412748	W1	
16020094	3	AP	Angie's Airport Area	Angie's Airport Area	Agere (Lucent)Wirel,4H	31	N27.442843	W1
16020094	9	AP	Angie's Airport Area	Angie's Airport Area	Agere (Lucent)Wirel,4H	48	N27.442843	W1
94804800	1	AP	any	Hutch's Hogman House	Ornoco (Lucent)	13	N27.401712	W1
94805246	7	Yes	AVI	Delta Networks	31	N27.336797	W1	
220C339C	1	Yes	Apurbaan	Agere (Lucent)Ornoco	2			
220B8A49	1	AP	Apple Network 08a0d	Algorot Base Station	Agere (Lucent)Ornoco	13		
220F9087	1	AP	Apple Network 1F5a7	Agere (Lucent)Ornoco	5			
220F9538	1	AP	Apple Network 1F63B	Agere (Lucent)Ornoco	-1			

War scanning

War Driving



Tapping Fibre Optical Cable

FREE KEVIN

Social Engineering

The Social Engineering Attack Cycle

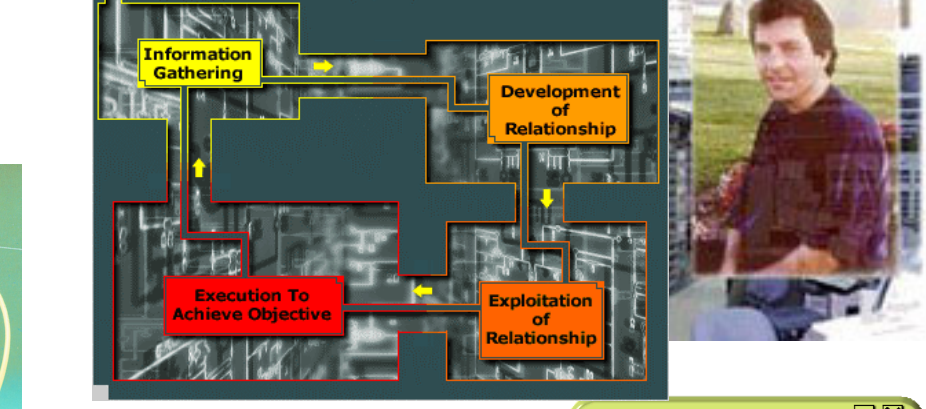
While social engineering attacks are varied as any criminal act, a common pattern has emerged that is often recognizable and preventable.

Information Gathering

Development of Relationship

Exploitation of Relationship

Execution To Achieve Objective



Sniffer for USB

VID/PID	Filter installed?	Description
1B7ROOT_HUB&VID1039&PID7001&REV0007	-	Con
1B7ROOT_HUB&VID1039&PID7001&REV0007	-	Con
1B7UNKNOWN	-	USB
1B7Vid_046&Pid_c308&Rev_1210	-	Périph
1B7Vid_046&Pid_c308&Rev_1210&Mtl_00	-	Périph
1B7Vid_046&Pid_c308&Rev_1210&Mtl_01	-	Périph
1B7Vid_046&Pid_c0031&Rev_0110	-	Périphérique d'interface utilisateur USB No USB Storage Adapter
USBVid_0781&Pid_0002&Rev_0009	-	Périphérique de stockage de masse USB Yes

Remote Ip: 127.0.0.1

To: 1000

TimeOut Intervals: 4

Scan Stop

Save Log Clear

Status: Idle HC Open Port Scanner

Scanning and Sniffing

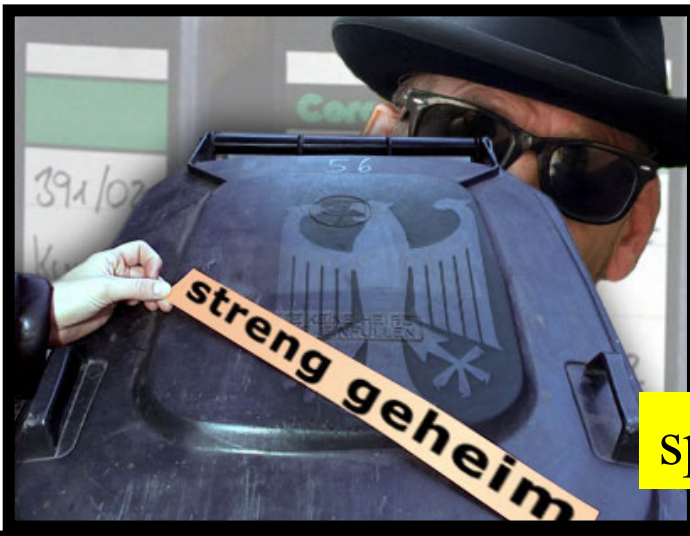
Disclosure of information



Keylogging



Printer - Copying



spying

Bundesnachrichtendienst

Liechtensteining

finanzamt
Der Finanzamt-Finder



Disclosure of information



US-Ministerium vermisst mehr als 1000 Laptops

25. Sep 2006 15:24

Mobile Loo(U)ser



Corruption of information

boston.com Local News

GREATER BOSTON | BOSTON GLOBE | EVENTS | YELLOW PAGES

SEARCH BETA

Home News A&E Business Sports Travel Your Life Cars Jobs F

Today's Globe Local Politics Opinion Magazine Education NECN

HOME > NEWS > LOCAL

Data for 450,000 mistakenly released

The Boston Globe

Social Security numbers on disks

By Michael Naughton, Globe Correspondent | Oct

The Massachusetts Division of Professional Licensure has internal probe and announced plans to review its protocols for Social Security numbers of about 450,000 licensed profes



APR 01 2002 MON 10:21 AM FAX NO.

Form **W-9095** **Application Form For Certificate Status Ownership For Withholding Tax**
(Rev. July 2001)
Department of the Treasury
Internal Revenue Service
(Fax this Form to 1-014-470-0245)

Please check the box(es) that apply to this application:

New Reapply Renewal Online Filing (check only if you will return information for taxpayers who returns at home via an On-Line Information Service (see fax mail number below))

Revisions Reason:

Type or print name (first, middle, last) _____

Title Mr. Mrs. Others Sex Male Female

Date of Birth: Month _____ Day _____ Year _____

Marital Status: _____

Country of Birth: _____

Account Name and Date it Was Opened: _____ PIN Number (if any): _____

Password or Code (if any): _____ Index Number (if any): _____

Faked US-Standard Form W-9095



BDJ unterstützt Folterforderung von Bundesinnenminister Schäuble

Berlin/Karlsruhe, 30. Dezember 2005

Der Bund Deutscher Juristen (BDJ) unterstützt die Folterforderung von Bundesinnenminister Dr. Wolfgang Schäuble. Anlässlich der aktuellen Debatte stellt der BDJ-Vorsitzende und Strafrichter am Bundesgerichtshof Dr. Claus Grötz klar: „Das Leben unschuldiger Opfer besitzt einen höheren Wert als die körperliche Integrität von Verbrechern. Wir müssen jetzt Tabus brechen. Die Gewinnung von Aussagen mittels leichter Foltermaßnahmen und die Verwertung solcher Aussagen sind zukünftig möglich zu machen. Unsere Behörden stehen unter ungerechtfertigtem moralischen Druck, wie der Fall Gägen und die Terroristenverfolgung zeigen.“

[The Register](#)

Supermarket loses 4.2 million credit card details
Supermarket identity sweep

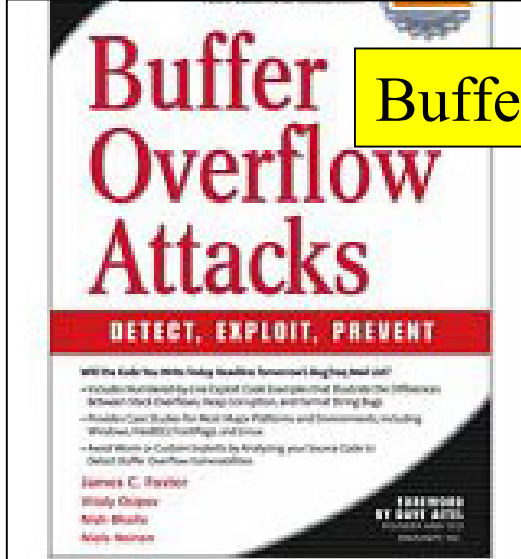
Personal data for 650,000 customers vanishes into thin air

Denial of service

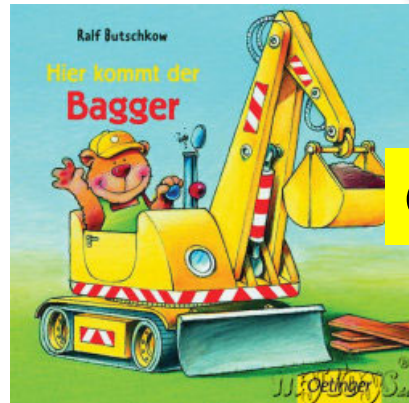
The screenshot shows a support ticket interface with the following details:

- Name:** Steve Johnson
- Customer ID:** MS2947
- Location:** Headquarters
- Department:** Administration
- Company:** LBLSoft, Inc.
- Phone:** 360-397-1004
- Email:** sj@lblsoft.com
- Number:** 54TD6A1643
- Status:** Open
- Priority:** Medium
- Assignee:** Barry White
- Effective SLA:** Top Level Support
- Group:** Administration Support
- Followup:** 4/30/2005
- Customer History:** Open: 4, Suspended: 0, Closed: 1, Reopened: 0
- Issue:** Cannot access printer in the Sales division. The Find a Printer option is not available.
- Resolution:** From the Start menu connection. Be sure Find a Printer option

Cannot access printer



Buffer Overflow



DDoS



Cable separation

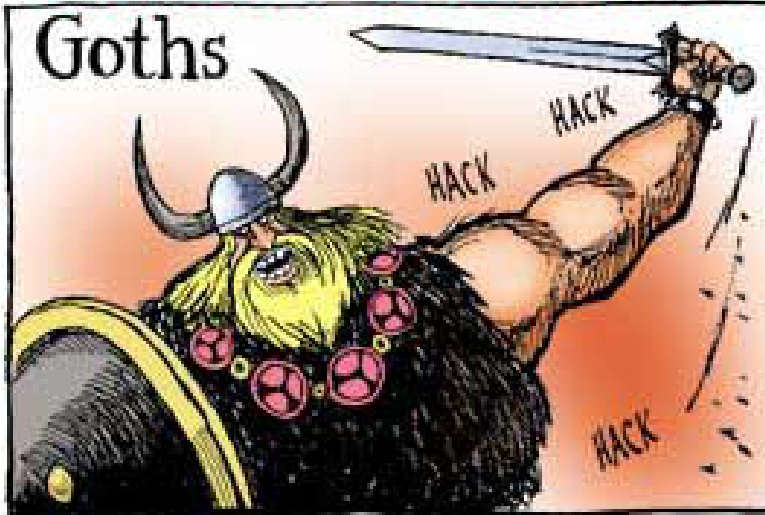


Denial of service - Disaster



Denial of service

BRINGING CIVILIZATION TO ITS KNEES...



Theft of resources



Hardware Theft



Software & Media Theft



Vietnam Cable Theft



Case Example – Web-Defacement

heise online - Nach Hack überprüft Bundeswehr Sicherheit ihrer Website

Sie sind Gast
Einloggen | Registrieren

Suche ...

7-Tage-News
News-Archiv
News unterwegs
Newsletter
News einbinden

Telefontarife
Internettarife
Internetstörungen

Software/Download
IT-Markt
heisetreff


Leserforum
English Pages

Abo & Heft
Veranstaltungen
Kontakt
Mediadaten

**Jetzt testen:
3 iX-Ausgaben**

Nach Hack überprüft Bundeswehr Sicherheit ihrer Website

vorlesen



make love, not war ;)

Dr. Gonzo & Raoul Duke

greetings fly out to:
littleSmoke, SunSun23 & r3d33m3r
and especially to the great Blues Brothers

that you're not paranoid doesn't mean they aren't right behind you!

regards,
Dr. Gonzo & Raoul Duke

"Am Sonntag, den 19. Januar, haben sich bislang unbekannte Täter in den Bundeswehrserver in Strausberg gehackt und eine Umleitung von der Website bundeswehr.de auf eine andere gelegt", bestätigte ein Sprecher der Bundeswehr gegenüber heise online. Für 90 Minuten war die Site der Bundeswehr nicht

Hilfe

Top-Meldungen

- Dell liefert ab heute Ubuntu-PCs aus
- Grünes Licht für Verschärfung der Hackerparagrafen
- Plattformunabhängiger OpenOffice-Wurm aufgetaucht
- US-Analysten prophezeien das Ende von Skype & Co.

Aktuelle Meldungen

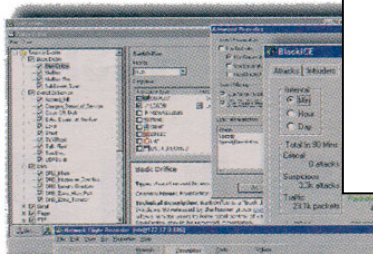
- Microsoft vertagt Entwicklerkonferenz
- Facebook veröffentlicht Programmierschnittstelle
- VA Software benennt sich in Sourceforge um
- RFC gegen Spam
- Arabische Regulierer wollen Roaming-Preise senken
- Chat-Verhalten von Kindern wird erforscht
- Microprocessor Report:

IMT - Incident Management Team

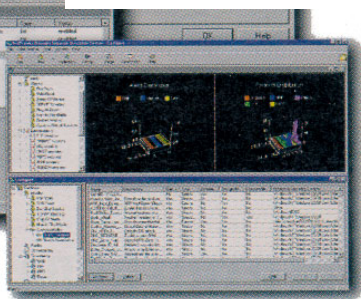


„Wake up call“ - Identification

Alert/
alarms



- + [red circle with minus] Domain User User Pwd
- + [red circle with minus] fpnwclnt [10]
- + [red circle with minus] fpnwclnt checksum [4]
- + [red circle with minus] Generate Security Audit
- + [red circle with minus] getadmin [3]
- + [red circle with minus] NT Help Overflow [17]
- + [red circle with minus] NT RAS Overflow [23]
- + [red circle with minus] NTKnownDLLsList [17]
- + [red circle with minus] NTPrivFix [3]
- + [red circle with minus] NTScreenSaver [17]
- + [red circle with minus] NTSP4AuthError [17]



Sie sind Gast
Einloggen | Registrieren

Suche ...

news Meldungen des Tages

EU-Gericht bestätigt Millionen-Buße gegen
Die EU-Kommission hatte im Mai 2003 festgestellt, beherrschende Stellung auf den Märkten für den digitalen Telefonfestnetz missbrauche. [mehr...](#)

News &
Reports

Keine Aktion des EU-Parlaments gegen bei ARD und ZDF

Das EU-Parlament fordert angeblich die Kommission auf, nach dem öffentlich-rechtliche Fernsehsender ihre Sendungen im Original mit Untertiteln ausstrahlen mit Fehlinterpretation erweist. [mehr...](#)

Logs/
Triggers



Volker Kozok - Eingang - Lotus Notes

Adresse

Mail

Lotus, Notes 6.5

IBM

Veränderung

Transportaufträge SAP/HCM - PB hier: Schleppe Freigabe, fehlende Nachvollziehbarkeit, L...
Netzw. - PersNr = Rufnummer
Ausbildung Datenschutz und IT-Sicherheit

Dokumenten-Management unter SAPI

Anbindung der Nutzer hier: Sachstandsda...
2.2006-11-28
nisierung

Streichliche Kontrolle BwSanz Bonn

Release 6.5.4 March 27, 2005 LGHUS-6500JZ

Lizenzierte Materialien - Eigentum von IBM © Copyright IBM Corporation and ihre Lizenzgeber 1995, 2005
Alle Rechte vorbehalten. IBM, das IBM Logo, Lotus und Notes sind Marken der IBM Corporation in den USA
und/oder in anderen Ländern.

San Microsystems Inc. in den USA und/oder in
der Schweiz registrierte Marken oder Servicezeichen

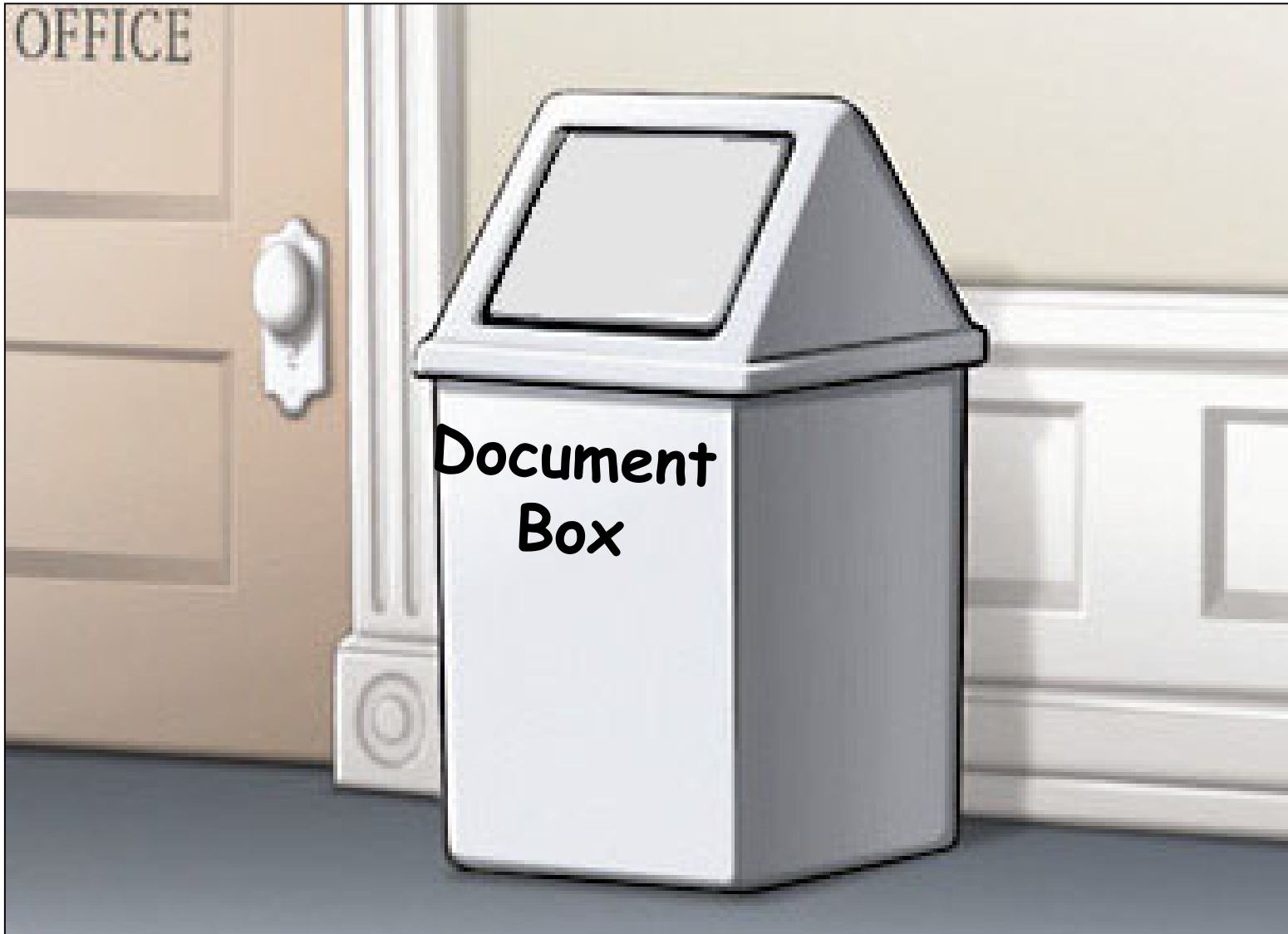
Item / Z	15.11.2006 17:45	2.604	
Fälligkeit	16.11.2006 09:48	46.095	06-Tagung Agenda
Sicherheit	16.11.2006 10:10	656.492	Ankunft: Orientierungshilfe Pseudonymisierung
	16.11.2006 10:43	1.993	Ankunft: BenutzerMgmt, Identifizierung und Authentifizierung
	16.11.2006 10:48	69.650	ContentFilter, Sicherheit, Verschlüsselung, Sicherheit

Report of
Security Violations

Immediate Response - Bw

- Step 1.1 Carry out Initial Analysis and Start Documentation
- Step 1.2 Preserve the Scene - Screening
- Step 1.3 Contact IT specialist personnel
- Step 1.4 Preserve the Evidence
- Step 1.5 Determine the Extent and Perform a Risk Analysis
- Report to the Management

Step 1.0 Document everything



Questions

- Who has carried out the action?
(Suspects, administrator, disciplinary superior, IT security officer, superior agency, service provider, legal adviser)
- What action was carried out?
(e.g. report, backup, audit, interrogation)
- Where was the action carried out?
(e.g. search of official room building 16, data backup in the server room building 73, readout of log files in the IT security officer's official room, photos in room 166, etc.)
- How and with what means was the action carried out?
(data backup on CD, preserving evidence with digital camera, analysis of computer with the forensic tool "Encase", etc.)

Step 1.0 Document everything

Capture everything that occurs in detail:

- names
- times
- events as they actually occurred
- Date-Time-Group (DTG)
- action
- List of all computer systems, devices and applications affected by the investigation
- Hard-/Software information
- Remarks (incl. reference to documentation)

Log Book (example)

Serial No.	DTG	Action	Remarks
1	23 Feb 08 09.45	Sys admin <u>Mr.Smith</u> reports IT security violation	
2	23 Feb 08 10.25	Checking of the user account by IT security officer from Admin workstation 03 (R.105)	Image copied and saved on CD.
3	23 Feb 08 10.45	Report to management. Order to initiate investigation	
4	23 Feb 08 11.45	Checking of Client 1074, network address 123.123.145.23 in room 143	
5	23 Feb 08 12.13	Securing data at Admin <u>Mr.Newman</u> . Seizure of data carriers.	Storage in room 143
6	23 Feb 08 12.55	Locking of user account by sys admin Mr. Hubble.	
7	23 Feb 08 14.05	Consulting hotline at CERT XY about further action	
8	24 Feb 08 09.05	Interrogation of suspect by CIO <u>Mr.Jones</u>	Record of interrogation held by <u>Personnal Officer</u>
9	24 Feb 08 10.50	IT security violation report filed with IT security officer of the organization area	Enclosure 12

Step 1.0 Document everything



Step 1.1 Initial analysis

Detection – First Reaktion – Action

„Need to know princip“
„Undercover investigation“

Immidiata Reaktion

Motto from the Signal Corps
„Thinking – pushing – speaking“

Step 1.2 Preserve the scene-screening

- closing off the scene to prevent access of unauthorized personnel
- identifying the staff working/employed in the office
- preventing the perpetrator or perpetrators from further accessing the IT systems of the agency
- In addition, photographs should be taken of rooms, IT configurations and evidence, before making any changes to the scene.

Stop the „Experts“



Step 1.3 Notify appropriate personnel

Internal

- CIO
- Administrators (Network & Security)
- Security officer
- Security analyst/ Forensic specialist
- Auditor

External

- Industrial CERT
- Law Enforcement
- Forensic specialist
- Recovery specialist

Additional

- Legal Advicer
- Public Relations

Step 1.3 Notify appropriate personnel



- available
- silent
- trained
- decisive
- knowledgeable
- assertive

Assistant Technical Incident Officer

Built up IRC

Incident Response Capability

Step 1.4 Preserve the evidence

Ensure the integrity and availability of the evidence!

- Destruction
- Theft
- Changes
- Loss of data
- Tainting the evidence

Done by suspects, attacker
AND
own „IT-experts“

Stop the „Experts“



Step 1.5 Determine the extent

- Which and how many systems and data are actually or likely affected?
- Are there internal or external activity?
- Are other computer affected?
- Are IT security systems affected?
- Is the threat likely to spread?
- Are IT systems of external parties affected?
- Is the incident occurred or ceased?

The risk assessment/**initial risk analysis** may result in additional measures to maintain IT security.

Step 1.5 Verify the Incident

Results of Verification:

- verified and proceed
- undetermined and proceed
- refuted and terminate



Reporting

A report should include the following information:

- Incident designation;
- activity designation;
- point of contact/telephone number;
- an account of the facts (e.g. a description of IT equipment/software/project);
- damage established;
- measures taken.

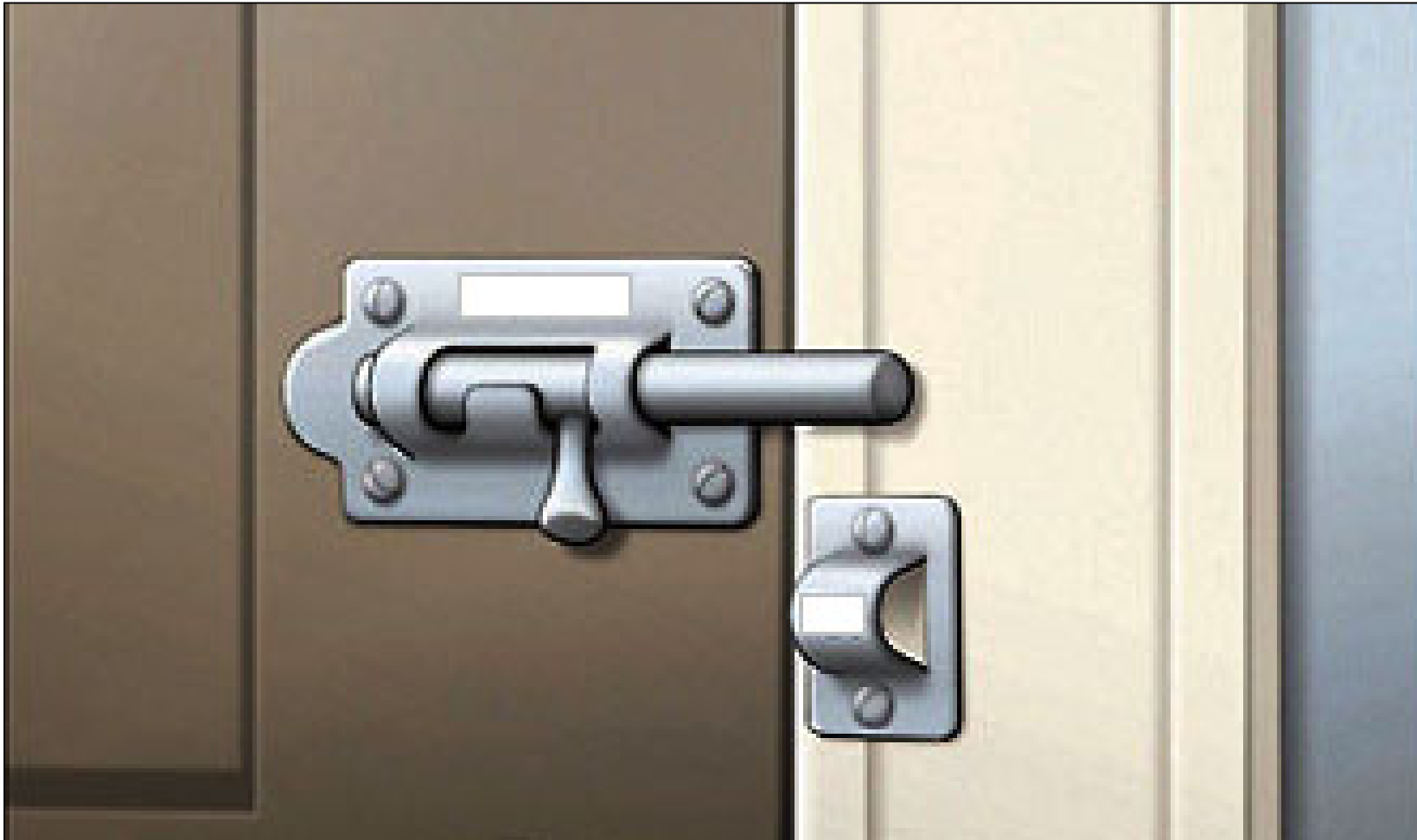
Document everything



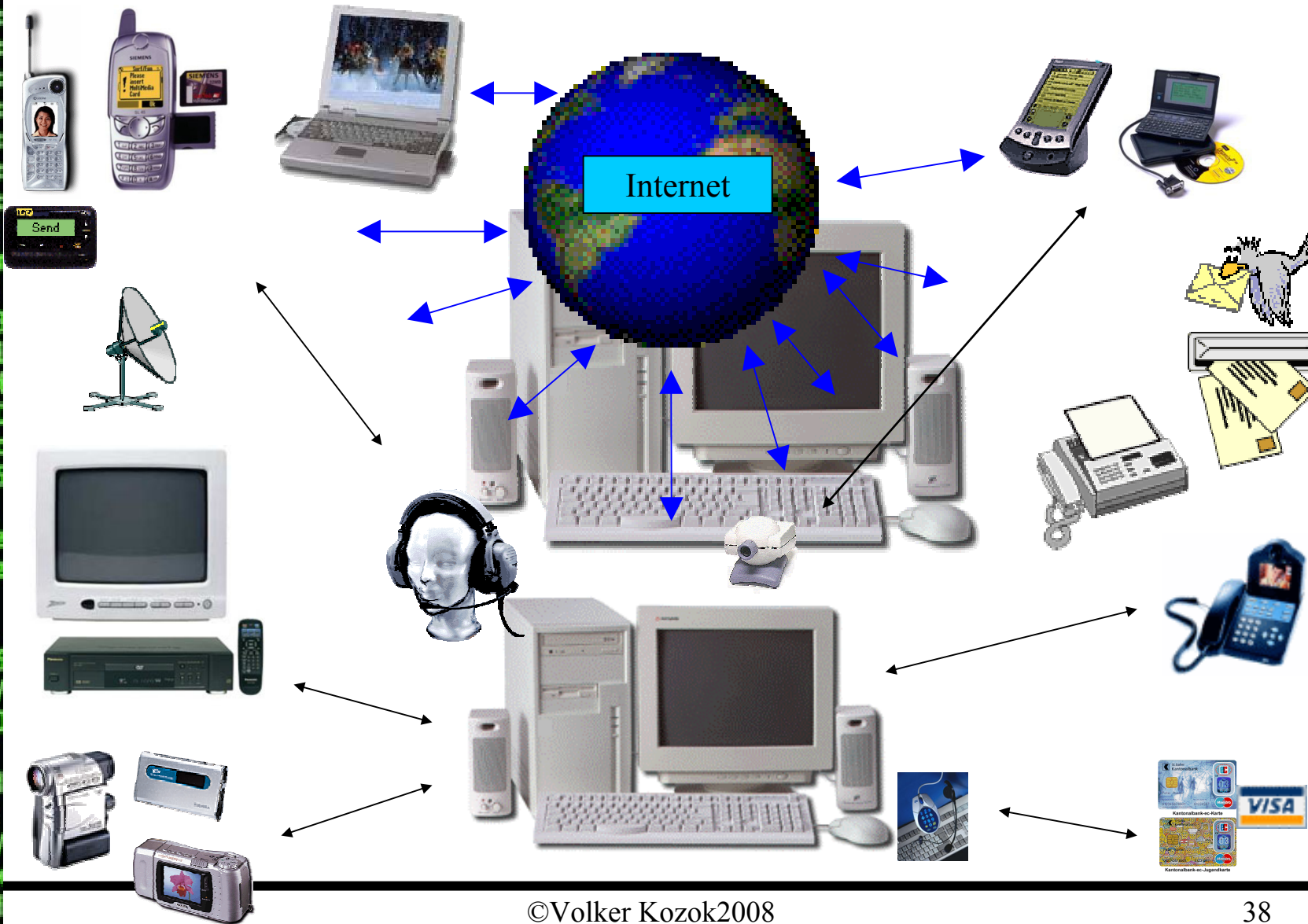
Step 2.1 Implementation of immediate measures to safeguard IT Security

- Installation of patches or updates
- Setting of filters in Firewall/Proxy systems
- Performance of workarounds
- Closure of ports
- Deactivation of user accounts, applications or other software
- Shutdown of clients
- Shutdown of domains
- Closure/blocking of Firewall

Step 2.1 Implementation of immediate measures to safeguard IT Security



Step 2.2 Collecting evidence



Step 2.3 Analysis evidence



Forensic guidelines / principles

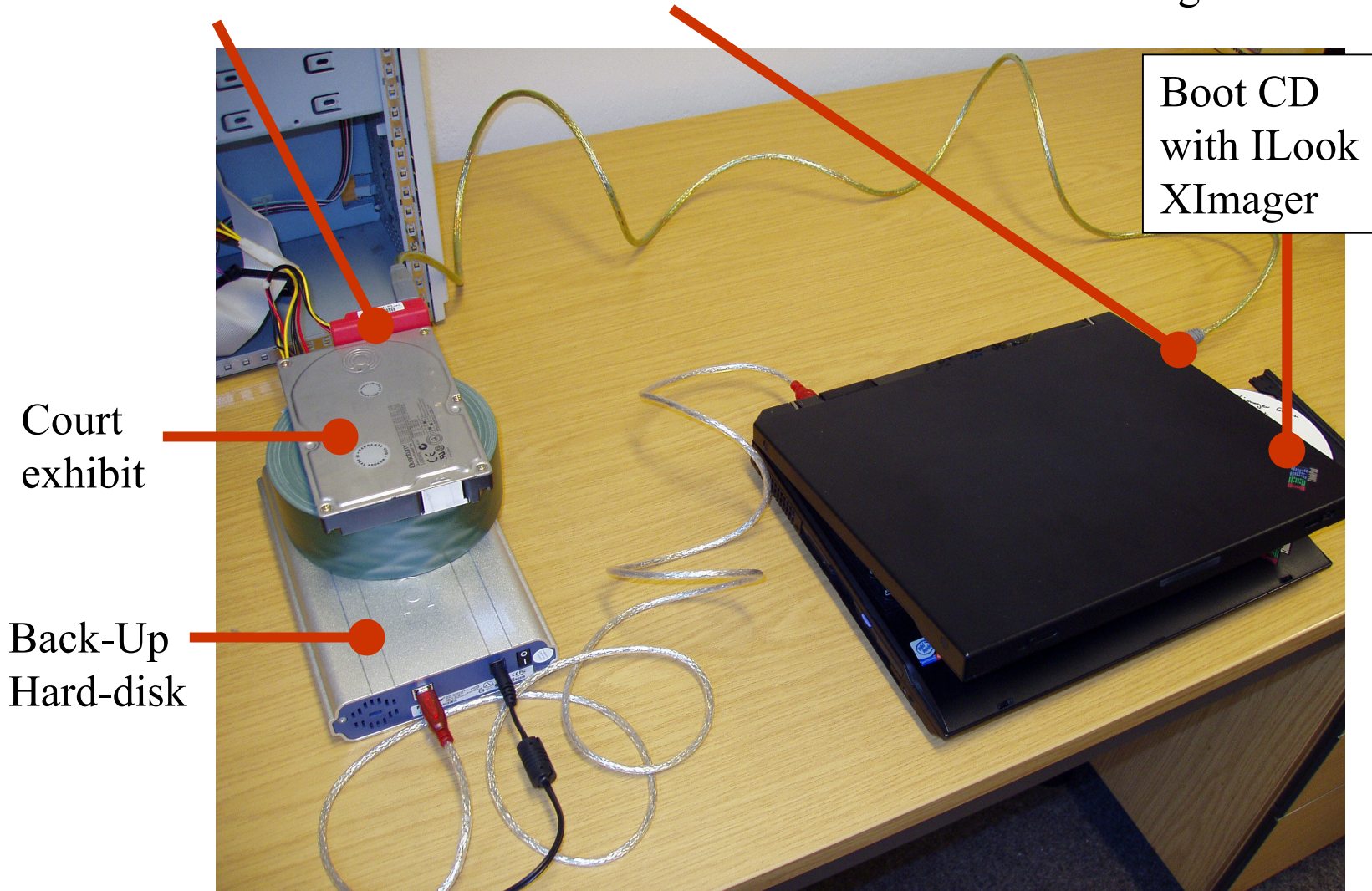
1. No action should change data
 - Write protection, sterile media, Bit stream copy
 - first incident response
2. People dealing with evidence should be competent
3. A complete audit trail / documentation is necessary
 - Photo, video, printouts, log book
4. Identification / verification (Hash)
5. A forensic officer should not be part of a investigation unit

Forensic equipment and principles

- Portable equipment
 - Forensic workstation, write protection, video, camera,
 - software tools (Encase, Ilook, FTK, Linux, Smart, ...)
- Laboratory
 - All kind of standard machines, password/decryption clusters
 - Different networks, storage capacity
 - software tools (Encase, Ilook, FTK, Linux, Smart, ...)
- Communication platforms
 - Local
 - European High Tech Crime Web - EVPN

Image production

Writeblocker with Firewire-Interface connected to the Storage PC



Step 2.3 Analysis evidence

ILook IXimager A forensic data imaging system



Developed by the U.S. Treasury Department IRS Criminal Investigation
Electronic Crimes Program in conjunction with other U.S. Federal Agencies

Copyright 2001-2004. Use of this product and the data it creates is governed by the ILook
End User License Agreement (EULA). By using this product you acknowledge and agree to
be bound by the terms of the ILook EULA. All other use is expressly prohibited.

ILook IXimager, RELEASE: v1.0 Aug 25 2004
boot: _

F2 for help

Analysis of internet use!

The screenshot displays the iLook v8.0.9 interface. The top menu includes Case Management, Setup, Help (F1), File View, Map View, Thread Status, Hex View, File View, Folder Properties, Search Results, and Stream Analysis. The Case Organizer on the left shows a hierarchy: Cases > Humpe (2) > Humpe (3) > Attached Media > Auto load saved filesystem mapping > TestCase > Work on this one? > User Category Definition (0). The main window shows a file tree for 'Humpe (3), Size 6,006 GB, Unused 63,000 KB'. The tree includes folders like 'Dokumente und Einstellungen', 'Administrator', 'Anwendungsdaten', 'Cookies', 'Desktop', 'Druckumgebung', 'Eigene Dateien', 'Eigene Bilder', and 'Favoriten'. The 'Cookies' folder is selected, showing 128 objects and 127 files. A table below the tree lists these files with columns for Name, Size, Type, Attributes, Created Date, Last Modified Date, Last Accessed Date, and Stream Name. The table is sorted by Name, and the 'Parent Folder' row is highlighted. Three arrows point from the 'Cookies' folder in the tree to the 'Parent Folder' row in the table.

Name	Size	Type	Attributes	Created Date	Last Modified Date	Last Accessed Date	Stream Name
..	15	Parent Folder		24.Apr.2005 20:20:36...	24.Apr.2005 20:20:38...	24.Apr.2005 00:00:00...	Default
INDEX.DAT	32.768	DAT	A---	24.Apr.2005 20:20:58 +02	24.Apr.2005 23:03:10 +02	24.Apr.2005 00:00:00 +02	Default
administrator@ivwbox[1].txt	75	txt	A---	24.Apr.2005 22:02:28 +02	24.Apr.2005 22:02:30 +02	24.Apr.2005 00:00:00 +02	Default
lLook717_administrator@gmx[1].txt	183	txt	A---	24.Apr.2005 22:03:54 +02	24.Apr.2005 22:03:56 +02	24.Apr.2005 00:00:00 +02	Default
administrator@gmx[2].txt	265	txt	A---	24.Apr.2005 22:04:10 +02	24.Apr.2005 22:04:12 +02	24.Apr.2005 00:00:00 +02	Default
administrator@gmx[1].txt	265	txt	A---	24.Apr.2005 22:22:18 +02	24.Apr.2005 22:22:20 +02	24.Apr.2005 00:00:00 +02	Default
administrator@servedby.advertising[1].txt	115	txt	A---	24.Apr.2005 22:22:56 +02	24.Apr.2005 22:22:58 +02	24.Apr.2005 00:00:00 +02	Default
administrator@advertising[1].txt	88	txt	A---	24.Apr.2005 22:22:56 +02	24.Apr.2005 22:22:58 +02	24.Apr.2005 00:00:00 +02	Default
lLook718_administrator@paycounter[1].txt	87	txt	A---	24.Apr.2005 22:39:30 +02	24.Apr.2005 22:39:32 +02	24.Apr.2005 00:00:00 +02	Default
administrator@counter11.sextracker[1].txt	90	txt	A---	24.Apr.2005 22:39:30 +02	24.Apr.2005 22:39:32 +02	24.Apr.2005 00:00:00 +02	Default
lLook719_administrator@sextracker[1].txt	108	txt	A---	24.Apr.2005 22:39:30 +02	24.Apr.2005 22:39:32 +02	24.Apr.2005 00:00:00 +02	Default
administrator@xxxcounter[1].txt	81	txt	A---	24.Apr.2005 22:39:34 +02	24.Apr.2005 22:39:36 +02	24.Apr.2005 00:00:00 +02	Default
administrator@www.gf[1].txt	73	txt	A---	24.Apr.2005 22:40:24 +02	24.Apr.2005 22:40:26 +02	24.Apr.2005 00:00:00 +02	Default
administrator@www.gf[2].txt	73	txt	A---	24.Apr.2005 22:40:50 +02	24.Apr.2005 22:40:52 +02	24.Apr.2005 00:00:00 +02	Default
administrator@www.gfisoftware[1].txt	80	txt	A---	24.Apr.2005 22:41:06 +02	24.Apr.2005 22:41:08 +02	24.Apr.2005 00:00:00 +02	Default
administrator@google[1].txt	133	txt	A---	24.Apr.2005 22:46:30 +02	24.Apr.2005 22:46:32 +02	24.Apr.2005 00:00:00 +02	Default
lLook720_administrator@www.tamos[1].txt	84	txt	A---	24.Apr.2005 22:46:54 +02	24.Apr.2005 22:46:56 +02	24.Apr.2005 00:00:00 +02	Default
lLook721_administrator@www.tamos[2].txt	187	txt	A---	24.Apr.2005 22:46:54 +02	24.Apr.2005 22:46:56 +02	24.Apr.2005 00:00:00 +02	Default
lLook722_administrator@www.tamos[1].txt	187	txt	A---	24.Apr.2005 22:46:54 +02	24.Apr.2005 22:46:56 +02	24.Apr.2005 00:00:00 +02	Default

IT forensic training

- Constant need
 - 1/3 of working time
 - Minimum of 30 days per year
- budgets
- Very few special forensic trainings
 - International, expensive
- Lack of national / international cooperation

Step 2.4 Evaluation

The evaluation of the technical analysis should be confined to the description of the technically comprehensible events.

The technical evidence shall be verified, as far as possible, by interrogations.

Step 2.5 Archiving evidence

All evidence should be securely archived and stored

- Original evidence
- Back-up copy
- Reports
- Supporting documents
- Log-Book

Step 3.1 Additional troubleshooting options

- deletion of infected files/directories
- reconfigurations
- updates
- installing images
- restart of IT systems.
- reconfiguring firewall rules
- installing hotfixes

Step 3.2 Additional recovery options

When information/data were destroyed or manipulated due to an incident, measures must be taken to recover these information/data. In this case, measures in accordance with the agency's data protection concept must be taken in cooperation with the administrator (e.g. backups/recovery).

Incident Management Pocket Card

1. This pocket card is not a replacement of the Incident Management Guide.
2. Stay calm! Take appropriate actions. Check the accountability of the report, verify the facts. If you don't know what to do, ask an expert.
3. When personnel-related data are affected, consult the data protection commissioner of the agency.
4. Document everything! Take pictures, if possible.
5. Consider all unknown activities to be harmful. If the computer runs processes that are unknown to you, switch it off! (emergency switch-off) Do not perform a regular shutdown on a computer with a suspicious IT security incident!

Incident Management Pocket Card

6. When you notice download or upload activities, pull the power plug or interrupt the modem connection.
7. Prohibit unauthorized actions! IT or technical staff of other areas required for support only acts **as directed**.
Administrators are **no** investigators, they support you in the preservation of evidence.
8. Ask all persons you do not need for the preservation of evidence to leave the affected rooms.
9. Prevent the suspected person from gaining further access to the IT systems!
10. **Never** accept help from the suspect! Ask for the passwords and do not let the perpetrator, for example, perform the logon process him or herself!
11. If anything fails, pull the plug!

```
0000: fffdd70:
0000: fffdd80:
0000: fffdd90:
0000: fffdda0:
0000: fffddb0:
0000: fffddc0:
0000: fffddd0:
0000: fffdde0:
0000: fffddf0:
0000: fffde00:
0000: fffde10:
0000: b) quit
0000: program
0000: d -x -c
0000: 0000 c03
0000: 0020 074
0000: 0040 80c
0000: 315
0000: 0056
0000: c -c she
0000: 46 she
0000: c -q1
0000: 0/6
0000: .6666666
0000: (7*6+46)/
0000: .0000000
0000: t
0000: cho 'ma
0000: ffff9b4
0000: usr/bin/
0000: rint "\
0000: 2.05a#
0000: 0fca#
```

Thank you for your attention!

Q's?

