Information Security: History, Technological Basis and International Regulations

Neuroscience Berlin
Ethical Issues and Implications for Sociey

Frank Pallas

Berlin University of Technology – Computers and Society

Berlin, March 21, 2008

In this session, you will...

- ... get the **basics** of information security
- ... learn some vocabulary
- ... understand how the diverse terms relate to each other
- ... get an idea about why organizations do what they do
- ... not fall asleep – hopefully...

An artifact from popular science

„Powers of 10“ (1977)

Quelle: http://www.powersof10.com/

„Powers of 10“

- „A classic!“ (Student A)
- „No idea“ (Colleague B)
- „?“ (Professor C)
- „culturally significant“ (US Library of Congress)
- References, amongs others, in a „Simpsons“ episode

- World of physics: Powers of 10
  → Not really useful for computer scientists

„Powers of 10“

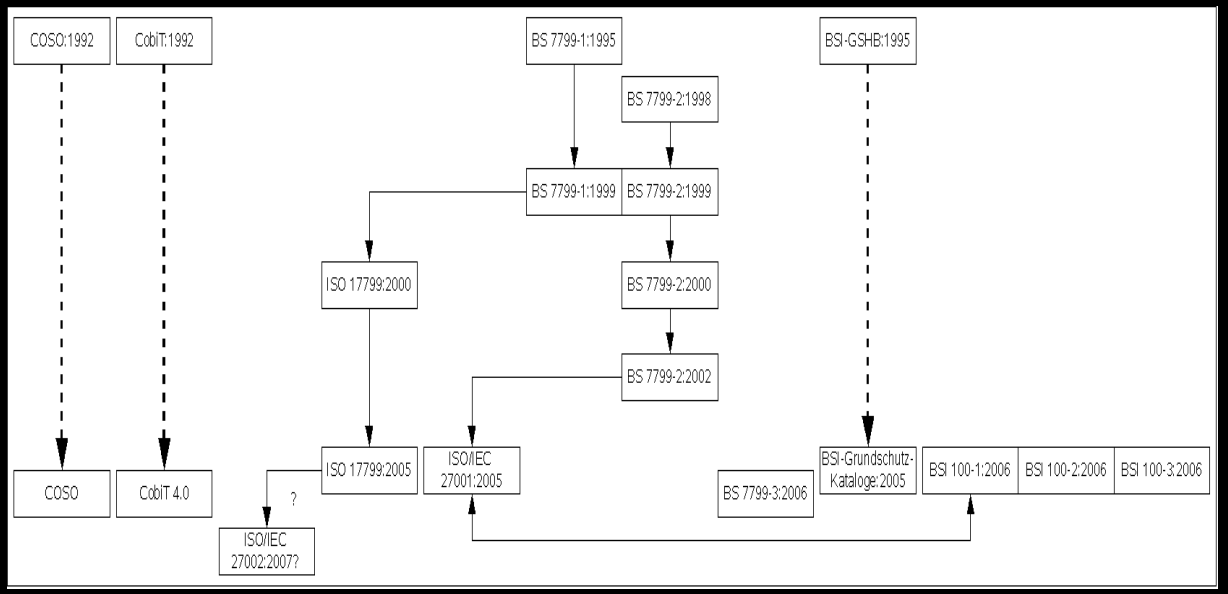
For Computer scientists,
there are only
10
types of people in the world:

Those who understand binary
and those who don't

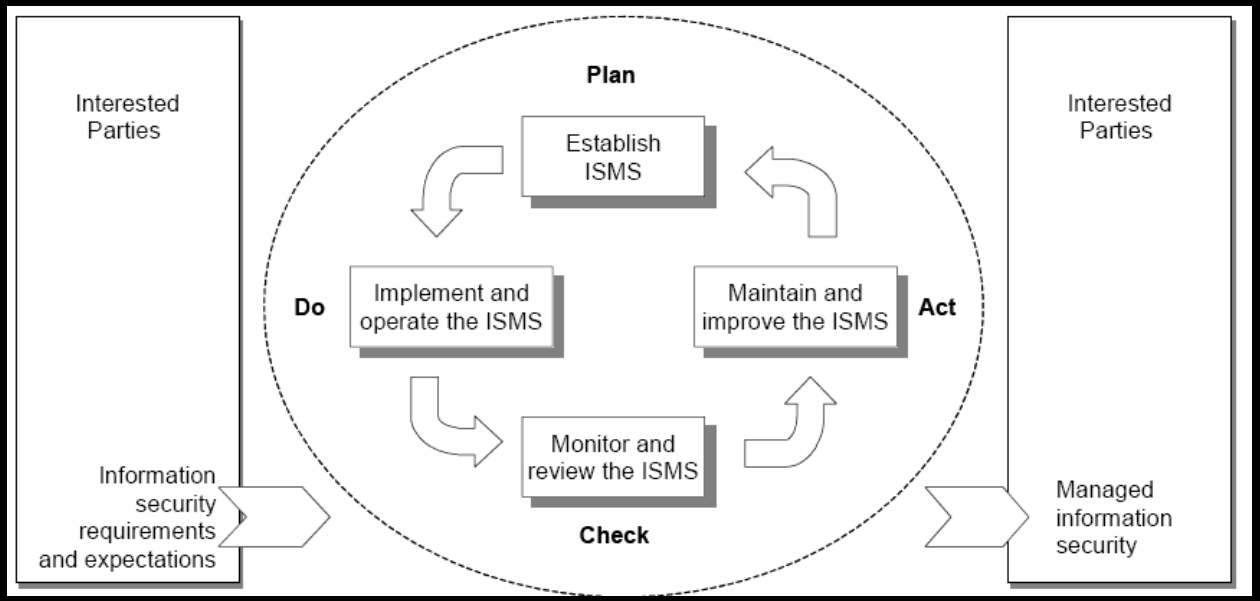
Powers of 2

A short trip through
Information Security history

t – 2^0 years: 2007

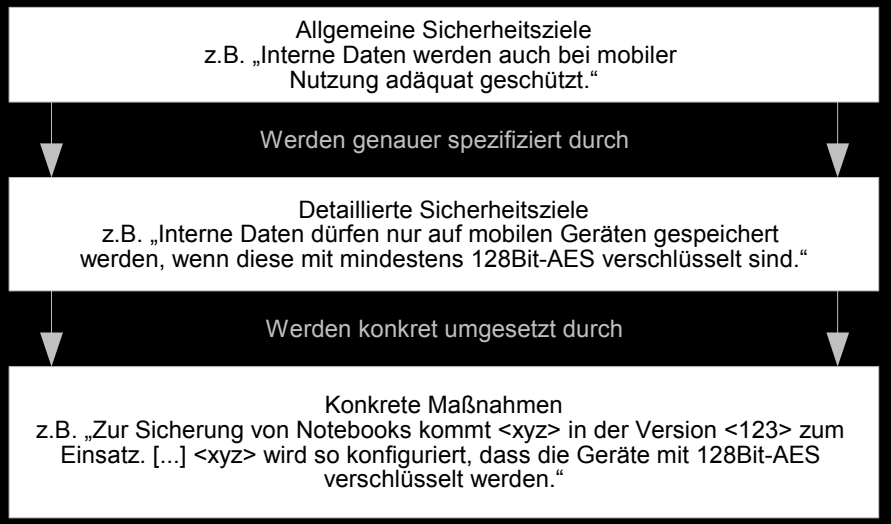


t – 2^1 years: 2006



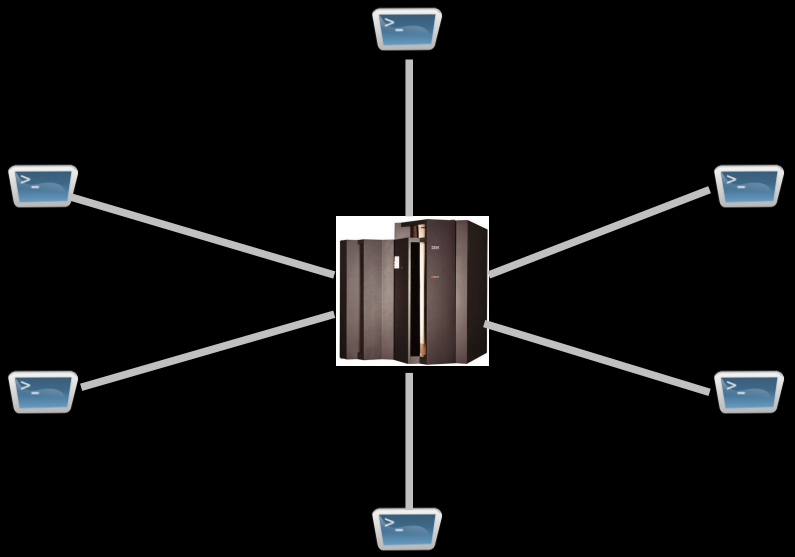
Basel II

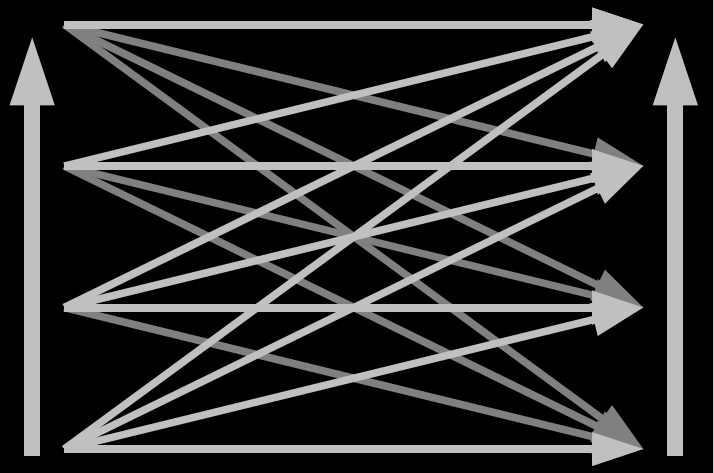
$t - 2^2$ years: 2004



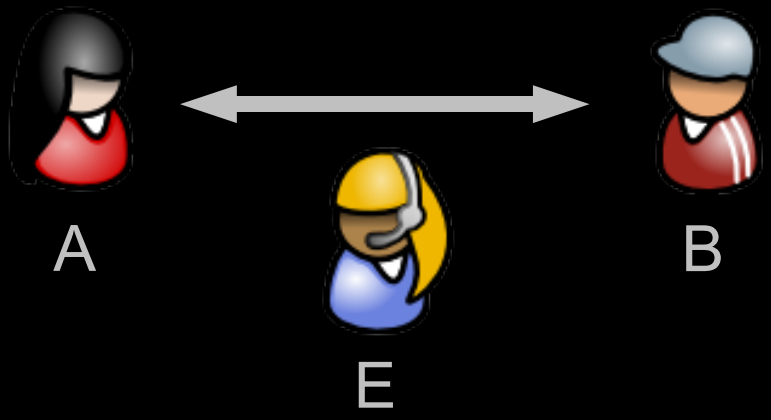
t – 2^3 years: 2000

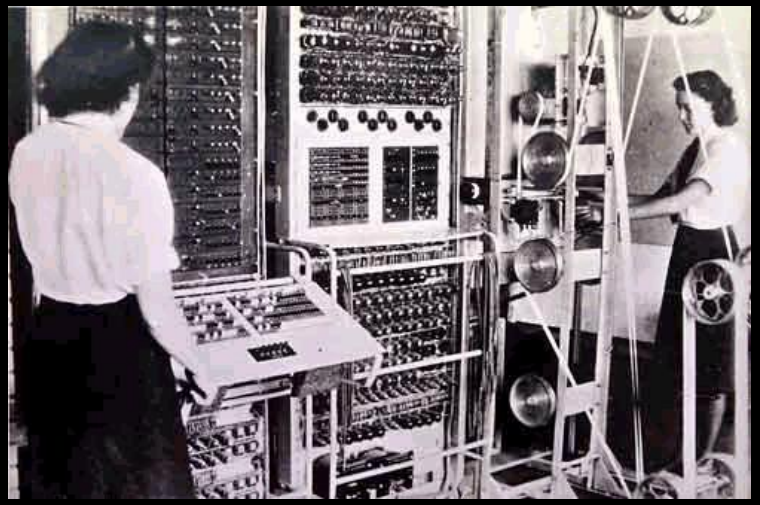
t – 2^4 years: 1992





t – 2^5 years: 1976

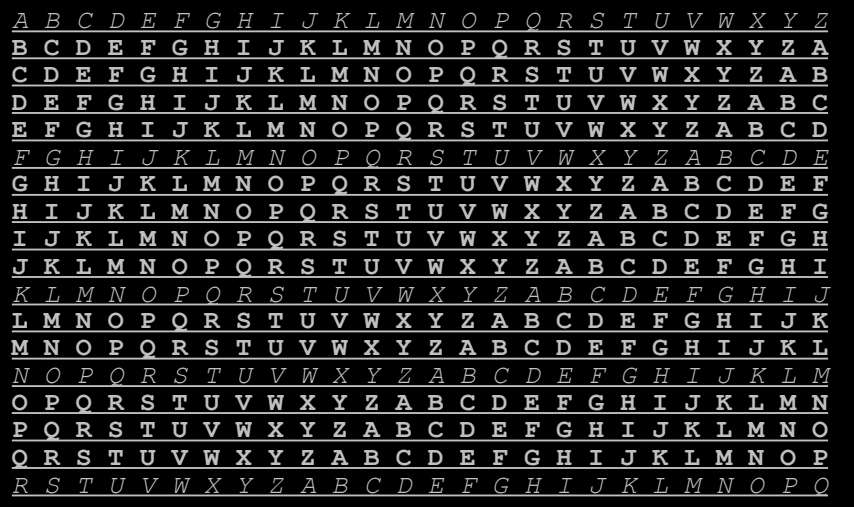




t – 2^6 years: 1944

t – 2^7 years: 1880

t – 2^8 years: 1752

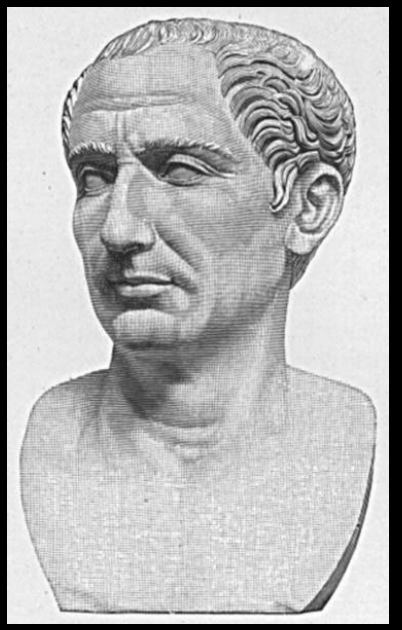


t – 2^9 years: 1496

A	B	C	D	E	…
X	*J*	*K*	*W*	*B*	…
L	*M*	*X*	*V*	*O*	…

t – 2^{10} years: 984

	A	B	C	D	E	…
	~5%	*~2%*	*~2%*	*~4%*	~13%	…



t – 2^{11} years: -40

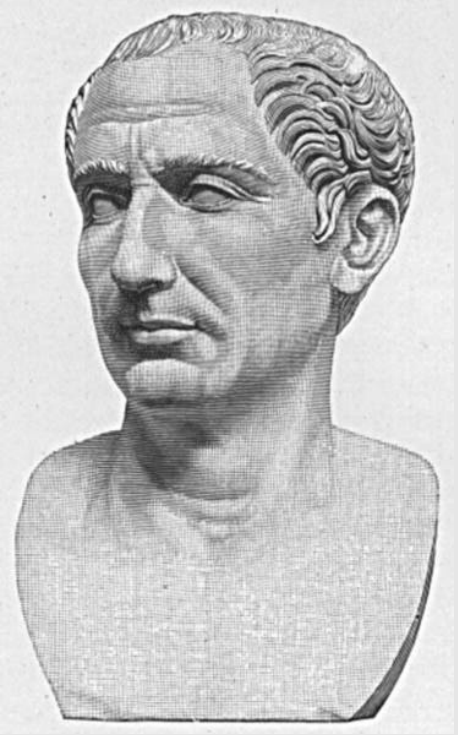
A B C D E …
D E F G H …

~100-44 BC: Caesar

- „Caesar-Cipher“

A	B	C	D	…
D	*E*	*F*	*G*	…

- Special case of a „mono-alphabetic substitution“
- Generalized case:
  a → x, b → k, …, z → i



Quelle: http://de.wikipedia.org/wiki/Bild:Hw-caesar.jpg

Caesar-Cipher: Real world app

Geocaching, anybody?

Additional Hints (Decrypt)

oruvaq/uvagre "Xrzcre Cyngm"

behind/hinter "Kemper Platz"

```
Decryption Key
A|B|C|D|E|F|G|H|I|J|K|L|M
-------------------------
N|O|P|Q|R|S|T|U|V|W|X|Y|Z
(letter above equals below,
and vice versa)
```

$t - 2^{11}$ years: -40

~801-873: Al-Kindi

- Arab polymath
- First mention of crypta-nalysis by frequency analysis
- *„[...] we count the occurences of each letter.“*

A	B	C	D	E	...
~5%	*~2%*	*~2%*	*~4%*	~13%	...

Image source: http://de.wikipedia.org/wiki/Bild:Al-Kindi.jpeg
Quote by Singh: The code book

$t - 2^{10}$ years: 984

~1460: Battista Alberti

- Italian architect, poet, linguist and mathematician
- Also worked for the Vatican
- **Poly**alphabetic substitution

A	B	C	D	E	…
X	*J*	*K*	*W*	*B*	…
L	*M*	*X*	*V*	*O*	…

„[...] the most significant breakthrough in encryption for over a thousand years [...]"

Singh (1999): „The Code Book", p. 46

Image source: http://it.wikipedia.org/wiki/Immagine:LeonBattistaAlberti.jpg

t – 2^9 years: 1496

~1580: Vigenère-Cipher

- Further development of poly-alphabetic substitution
- Vigenère-Square

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q

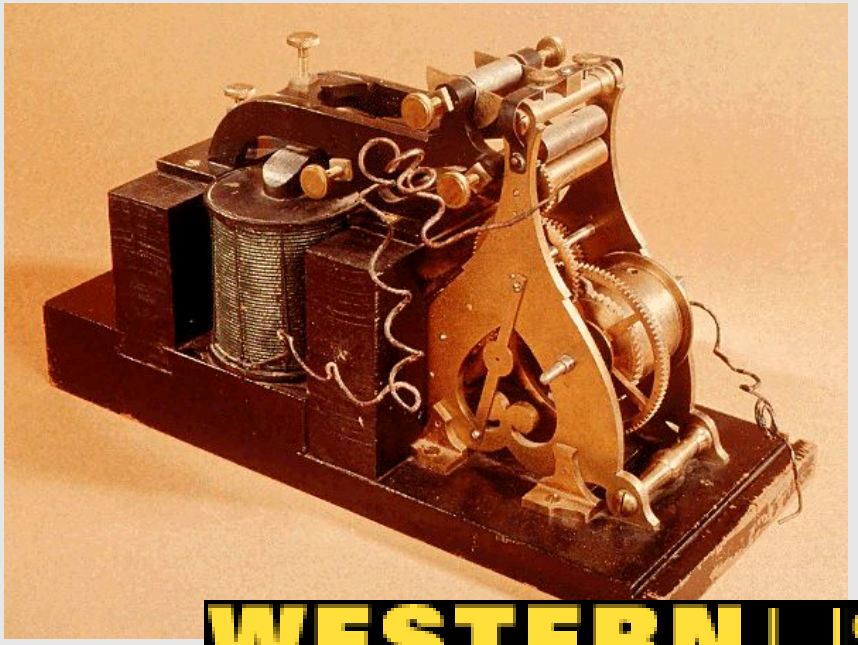
$t - 2^8$ years: 1752

~1850: Charles Babbage

- Developed precursor of current computers
  - Difference Engine No. 1
  - Difference Engine No. 2
- Found method for decrypting Vigenère-Ciphers (~1854)

Since ~1850: Telegraphy

- Fast information transmission
- Also interesting for private sector
- Rapid diffusion
- Problem: Secrecy
- Growing importance of encryption



$t - 2^7$ years: 1880

1883: Kerckhoffs

1883: Kerckhoffs

„Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi"

„The system must not require secrecy and can be stolen by the enemy without causing trouble"

Shannon (1946):

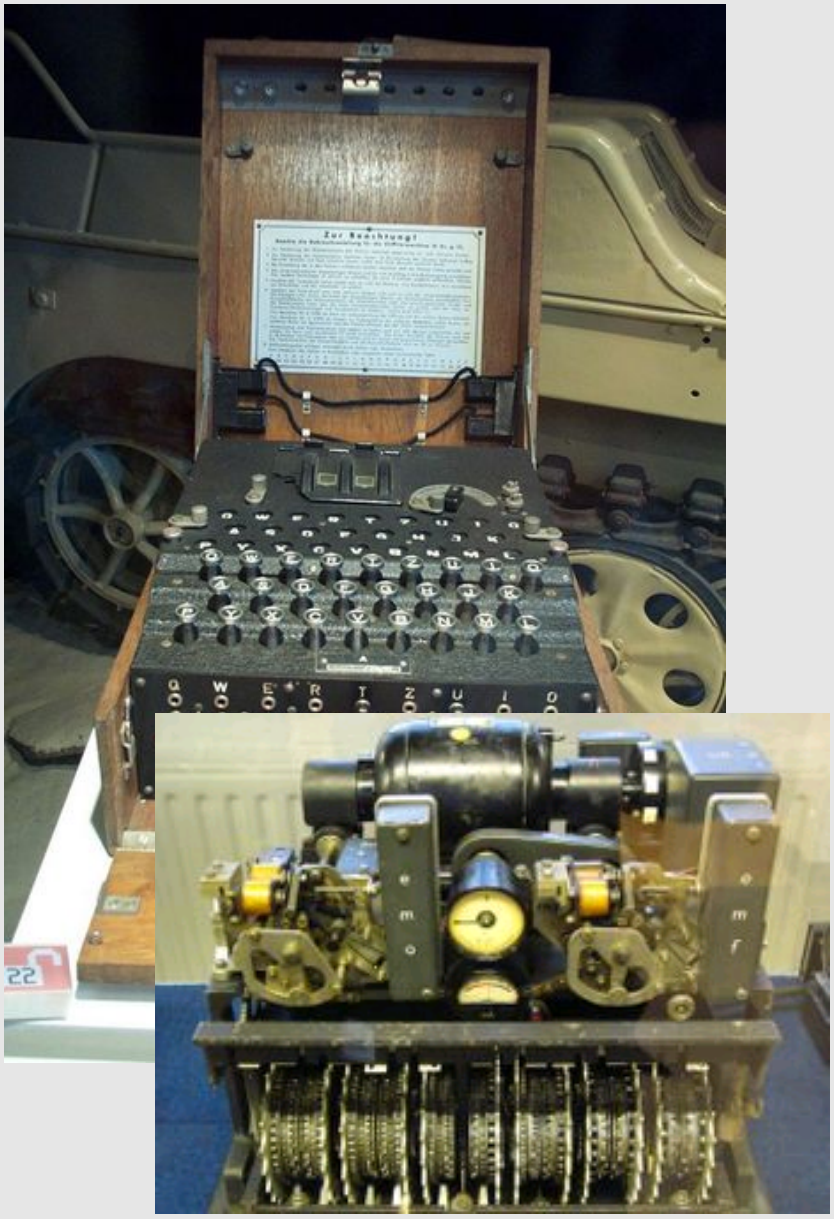
„The enemy knows the system"

Eric Raymond (2004):

*„Any security software design that doesn't assume the enemy possesses the source code is already untrustworthy; therefore, *never trust closed source*."*

Sources: http://petitcolas.net/fabien/kerckhoffs/
http://lwn.net/Articles/85958/

~1923: Enigma (+ Lorenz)



- Cipher **machine**
- Originally designed for private customers
- „Value of confidentiality“
- **Poly- and mono-** alphabetic substitution

Quelle: http://de.wikipedia.org/wiki/Bild:Enigma_Verkehrshaus_Luzern.jpg

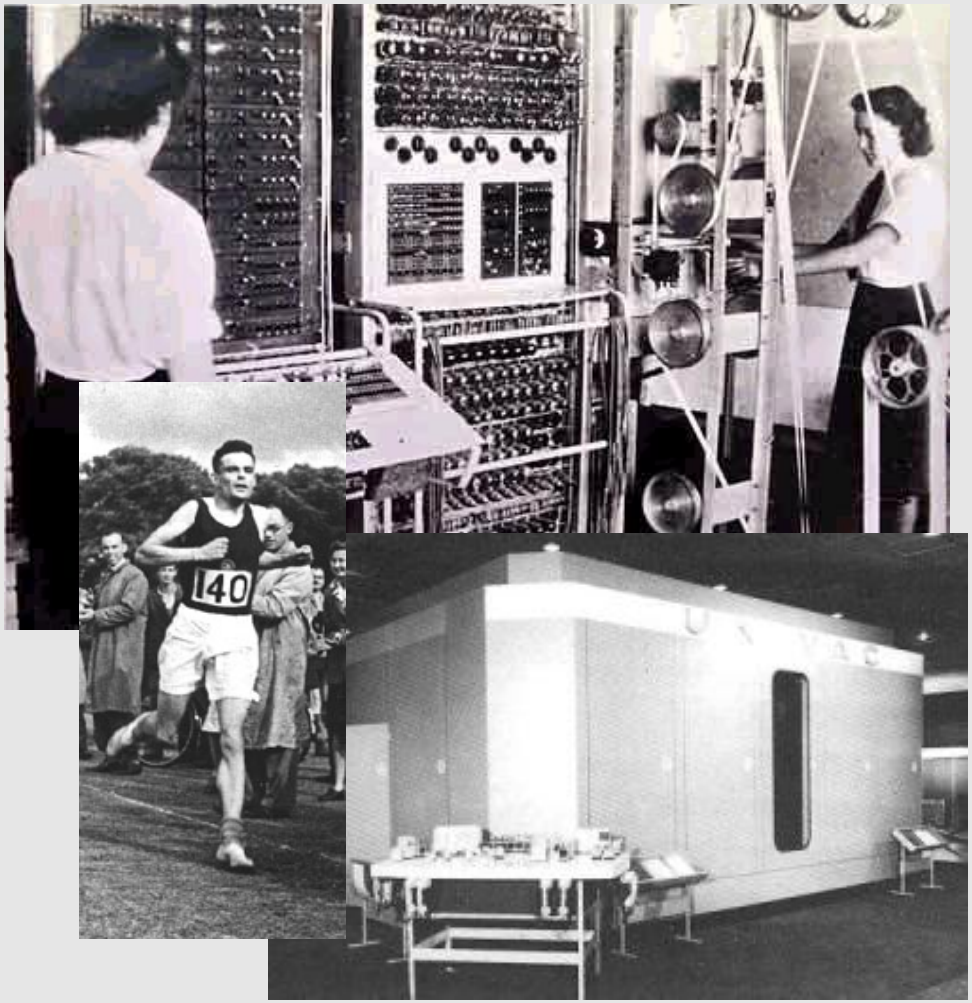
$t - 2^6$ years: 1944

„Computers“

Since 1943: „Computer“

- 1940: Turing-Bombes
- 1943: Colossus
- 1951: UNIVAC
- Since ~1954:
  Also used by
  private sector (GE)
- Since 1964:
  IBM System/360

➔ Security *for* Computers



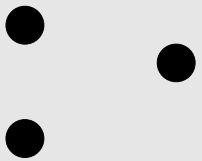
Major shift 1:

From manual to automated „data processing“

Implication:

Physical protection of computers

Shift 1



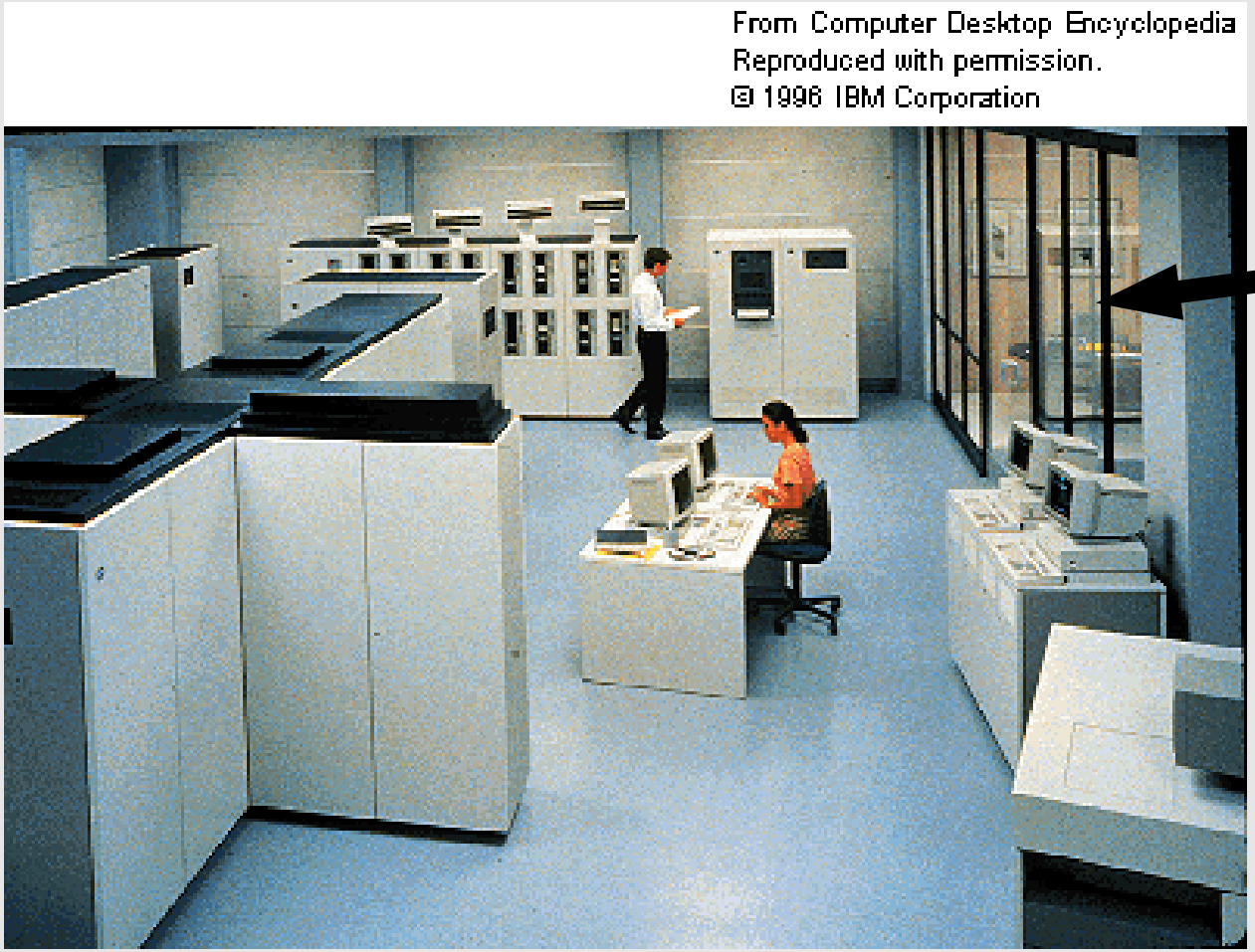
Computing Era	Isolated
Security Measures	Walls Locks etc.
Protection Paradigm	Physical

~1960: Mainframes

„Computer security was simply one aspect of general plant security.“

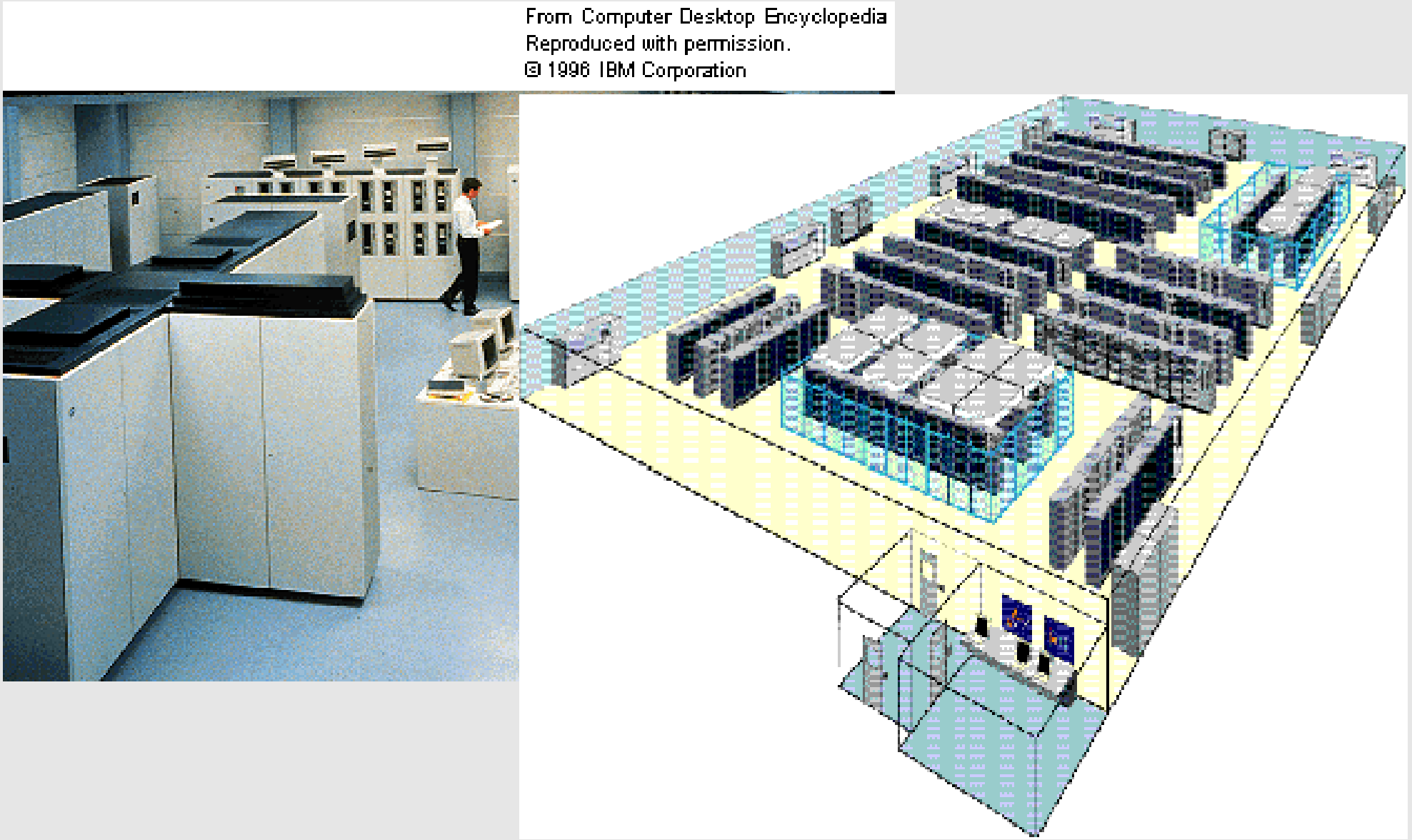
Russell/Gangemi (1991) p. 25

„Computer Security“



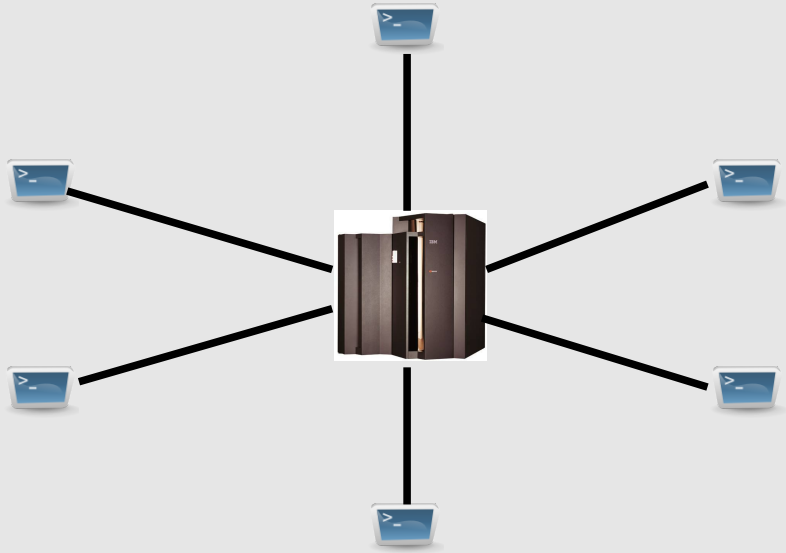
„Glass House“

„Computer Security“



~1970: Introduction of Terminals

- Multiuser
- Time-Sharing
- RAM-Sharing
- Disk-Sharing
- Xyz-Sharing
- ...



- Problem: Multiple processes use the same ressources „simultaneously“
- Different from punchcards, batch-processing, ...

1970: „Ware-Report“

*„A secure system must be based on the concept of **isolating** any given individual from all elements of the system to which he has no **need for access**.“*

Ware (1970), p. 8

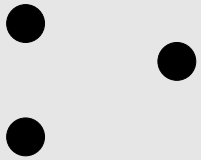
Major shift 2:

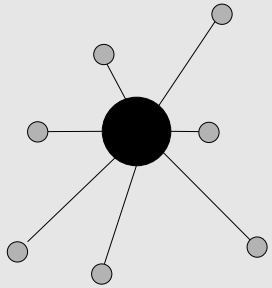
From isolated systems to „shared systems“

Implication:

Isolation of users and (SW-)processes

Shift 2

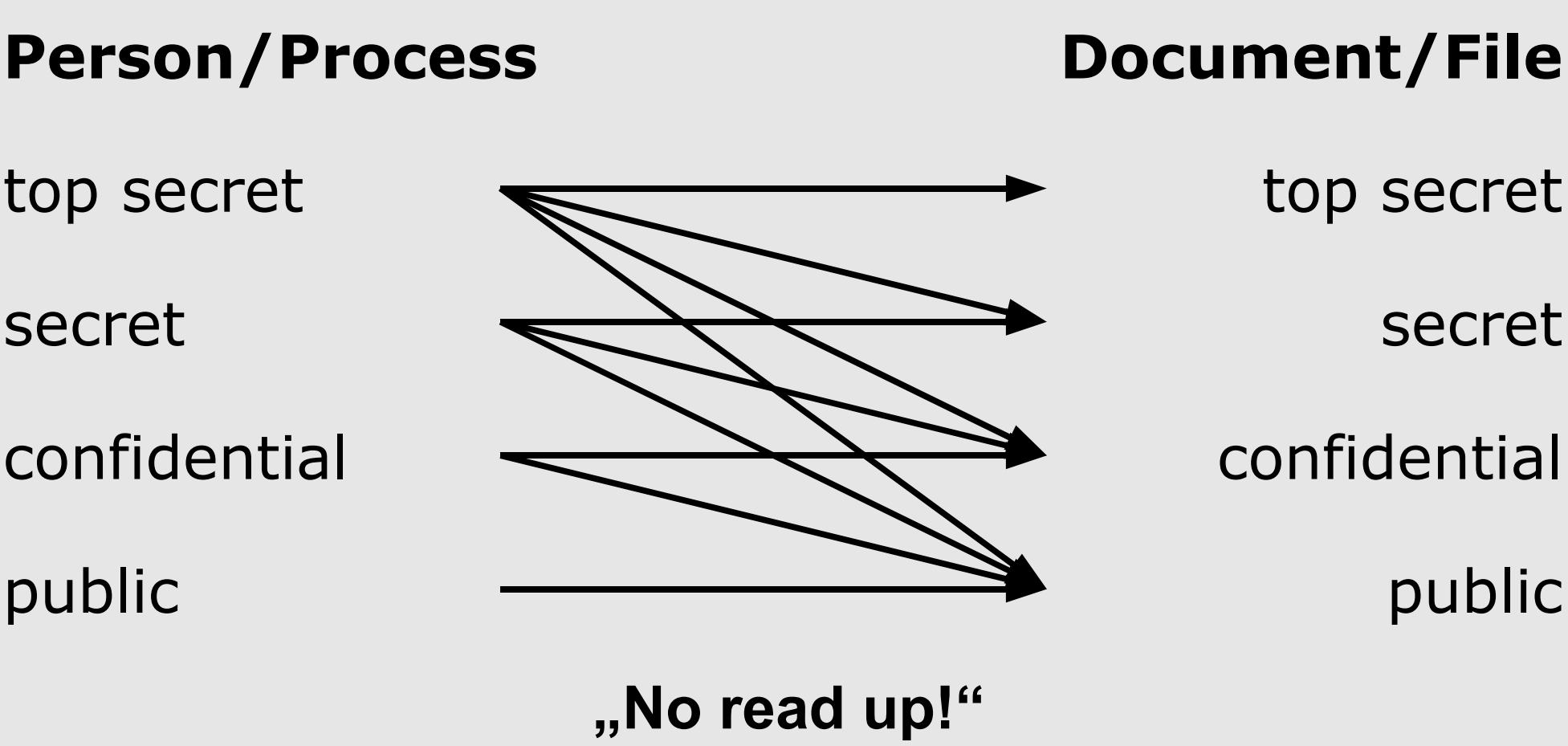




Computing Era	Isolated	Mainframe
Security Measures	Walls Locks etc.	Encryption Access Control etc.
Protection Paradigm	Physical	Technical

$t - 2^5$ years: 1976

1976: Bell-LaPadula – generalized



1976: Bell-LaPadula – generalized

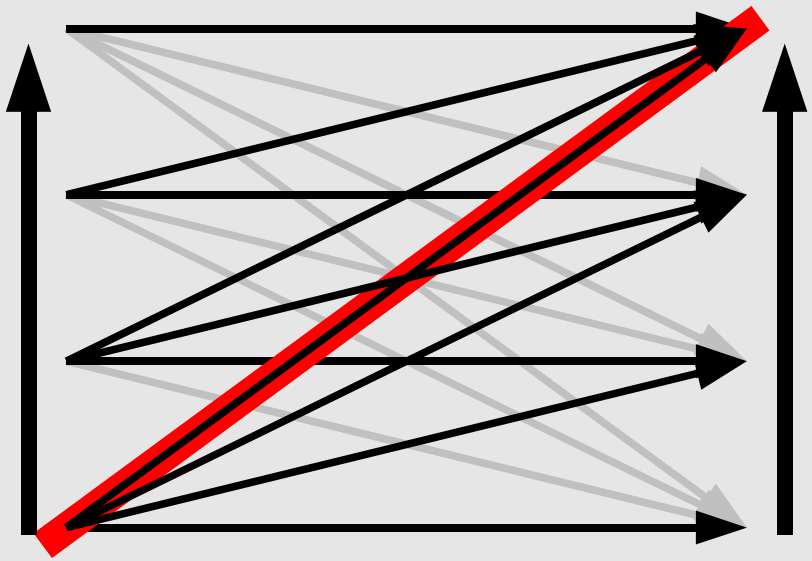
Person/Process

top secret

secret

confidential

public



Document/File

top secret

secret

confidential

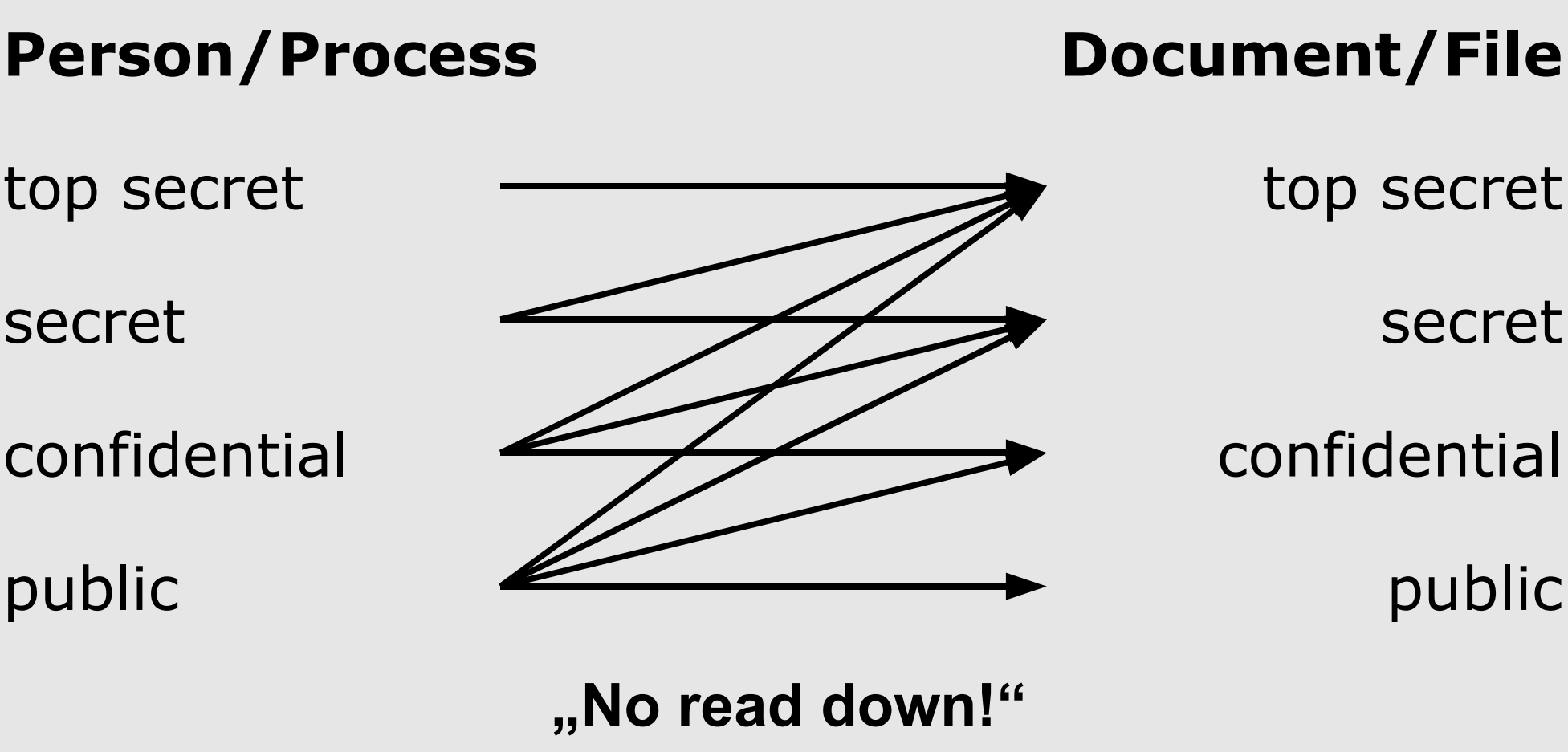
public

„No read up!“
„No write down!“

➔ Ensures **confidentiality**

More mathematical: http://www.albany.edu/acc/courses/ia/classics/belllapadula1.pdf

1977: Biba



„No read down!“

1977: Biba

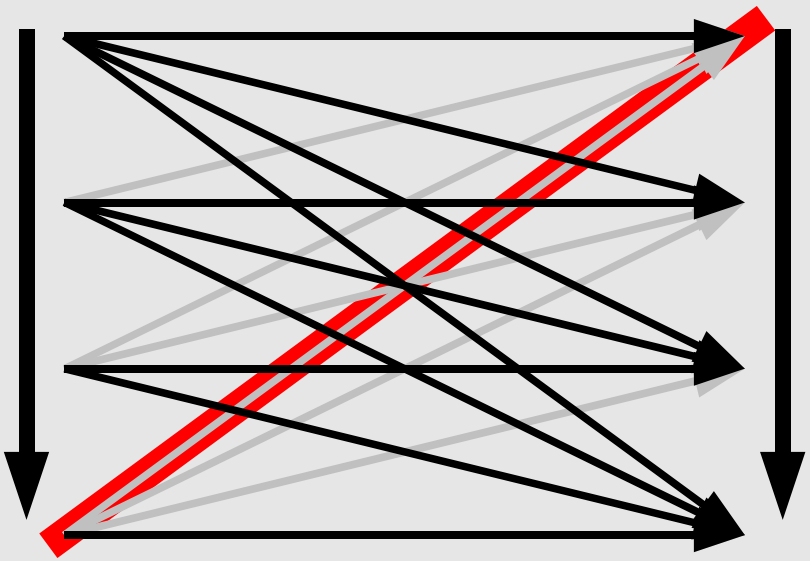
Person/Process

top secret

secret

confidential

public



Document/File

top secret

secret

confidential

public

„No read down!“
„No write up!“

➔ Ensures **integrity**

Objectives of Security - Mnemonic

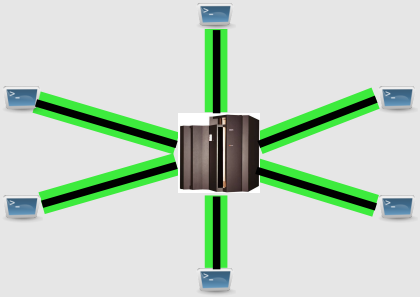
[C] Confidentiality

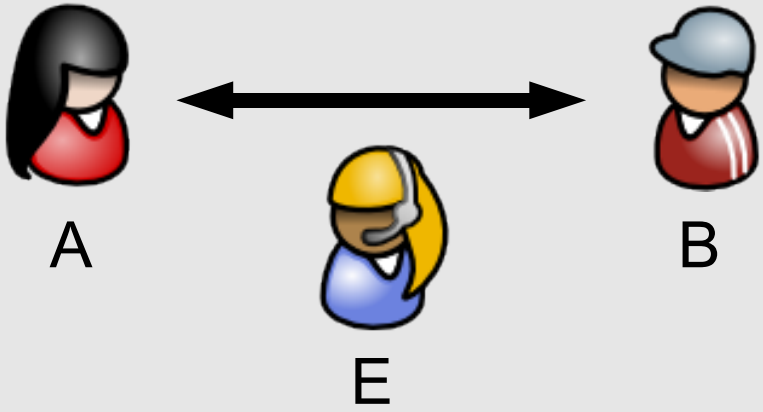
[I] Integrity

[A] Availability

[A] Accountability

1976/1978: Diffie-Hellman / RSA





1977/1979: Apple II + Visicalc

C11 (L) TOTAL C!
25

	A	B	C	D
1	ITEM	NO.	UNIT	COST
2	----	---	----	----
3	MUCK RAKE	43	12.95	556.85
4	BUZZ CUT	15	6.75	101.25
5	TOE TONER	250	49.95	12487.50
6	EYE SNUFF	2	4.95	9.90
7				----------
8			SUBTOTAL	13155.50
9			9.75% TAX	1282.66
10				----------
11			TOTAL	14438.16
12				
13				
14				
15				
16				
17				
18				
19				
20				

➔ Personal computers conquer offices

1986: Security and personal computers

„[PCs have to be protected] the way we protect copying machines."

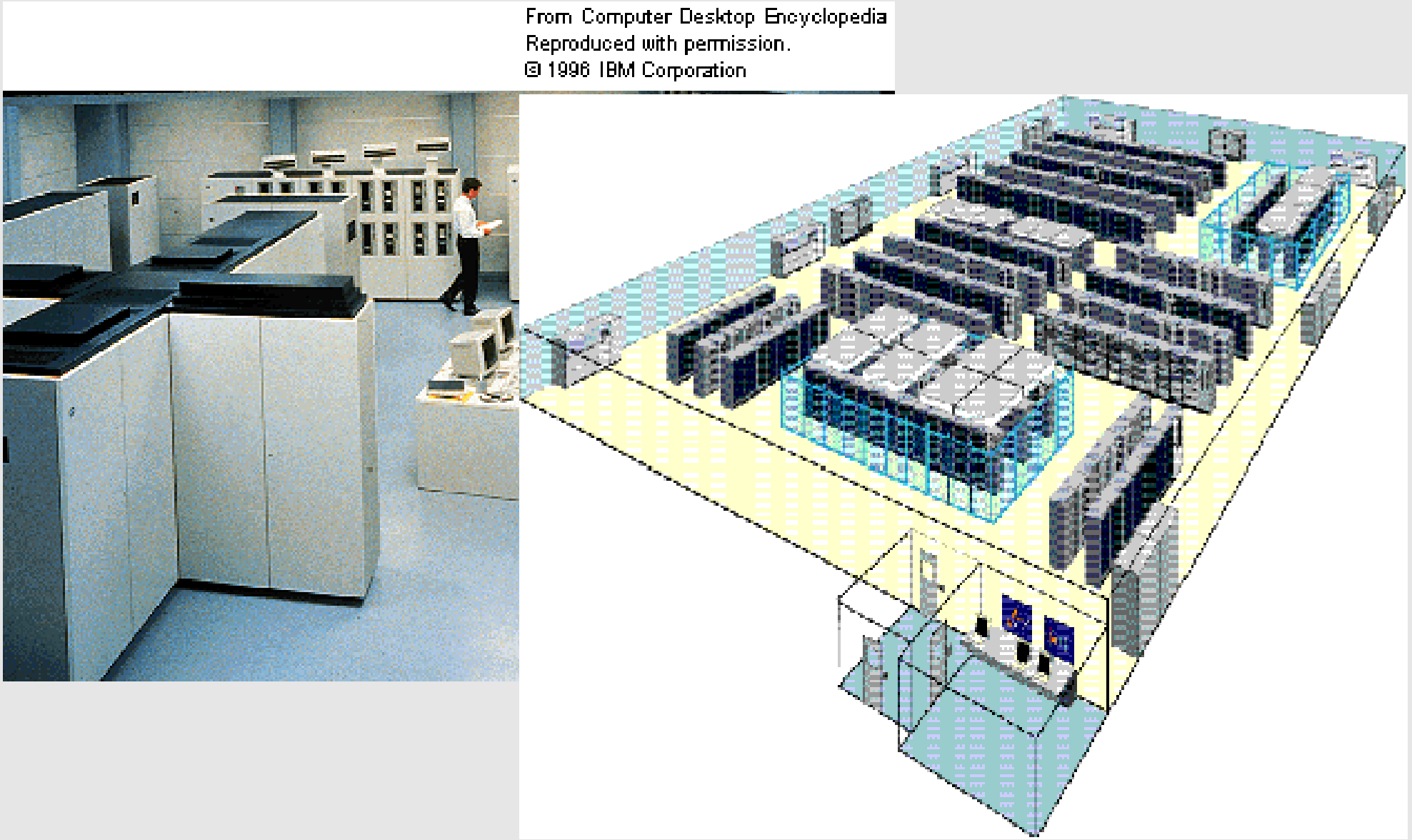
„[S]ometimes that surprises people because their first identication of the personal computer is not as a piece of equipment but rather as a computer."

„And everybody knows how you protect a computers right?"

„You place computers in highly specialized environments."

Murray (1986):
„Good security practice for personal computers."

„Computer Security“



1984: Security and personal computers

„The ideal of controlled information in an office seems to clash with the traditional view of what an office should be.“

*„A lack of **awareness** among office systems users"*

*„Lack of **managerial emphasis** [...] to the need for protecting information in the office"*

Schweitzer (1984):
„Information Security and Office Automation...“

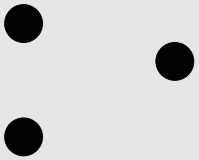
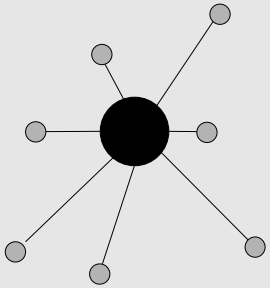
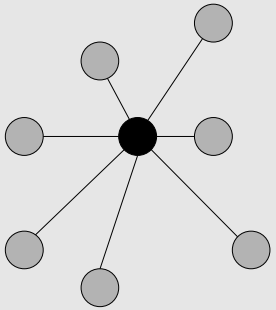
Major shift 3:

From „shared systems“ to decentralized processing

Implication:

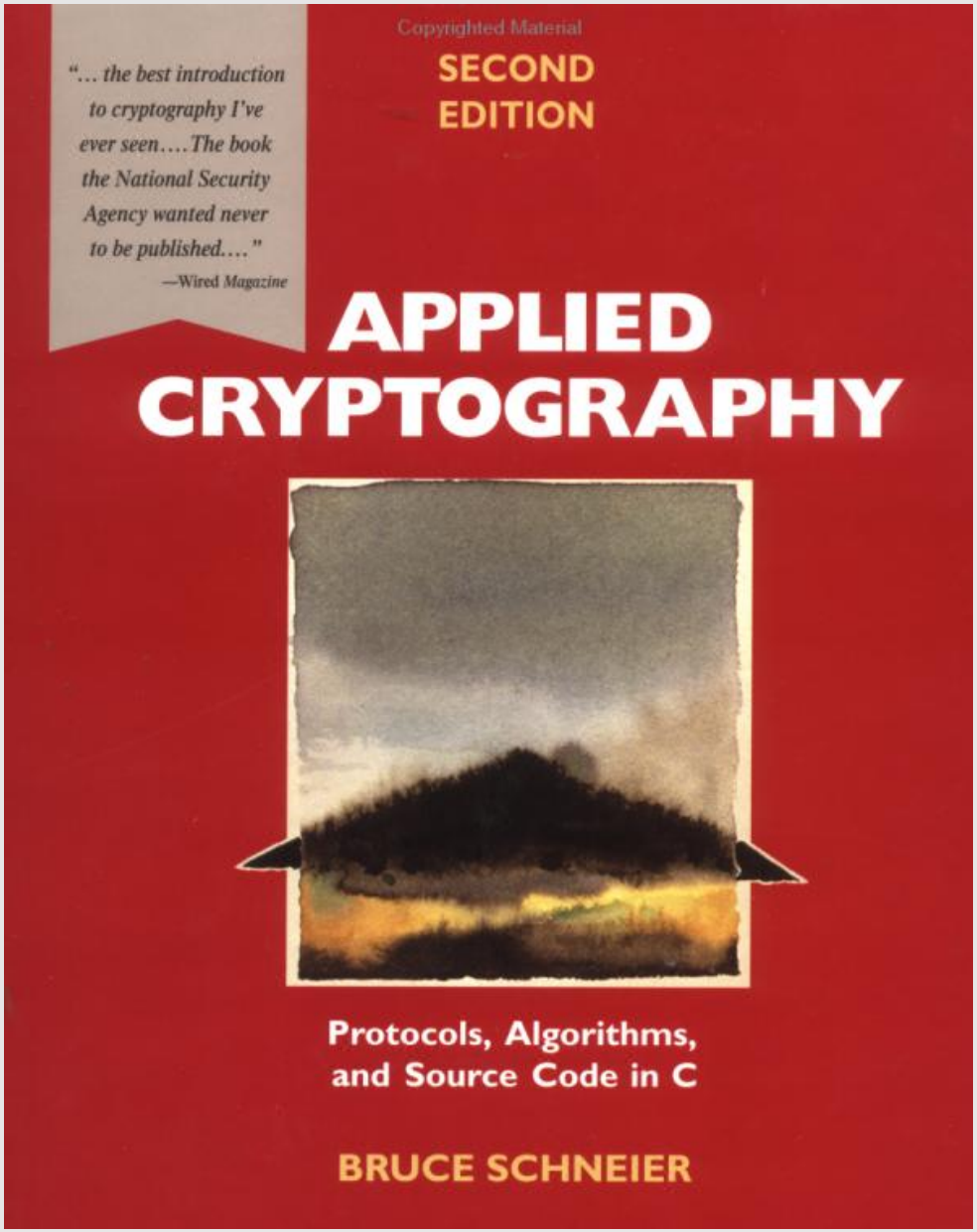
„awareness“, „managerial emphasis“, ... - At least, something different...

Shift 3

			
Computing Era	Isolated	Mainframe	Distributed
Security Measures	Walls Locks etc.	Encryption Access Control etc.	???
Protection Paradigm	Physical	Technical	???

$t - 2^4$ years: 1992

1995: Applied Cryptography



„The book the NSA wanted never to be published"

Wired Magazine

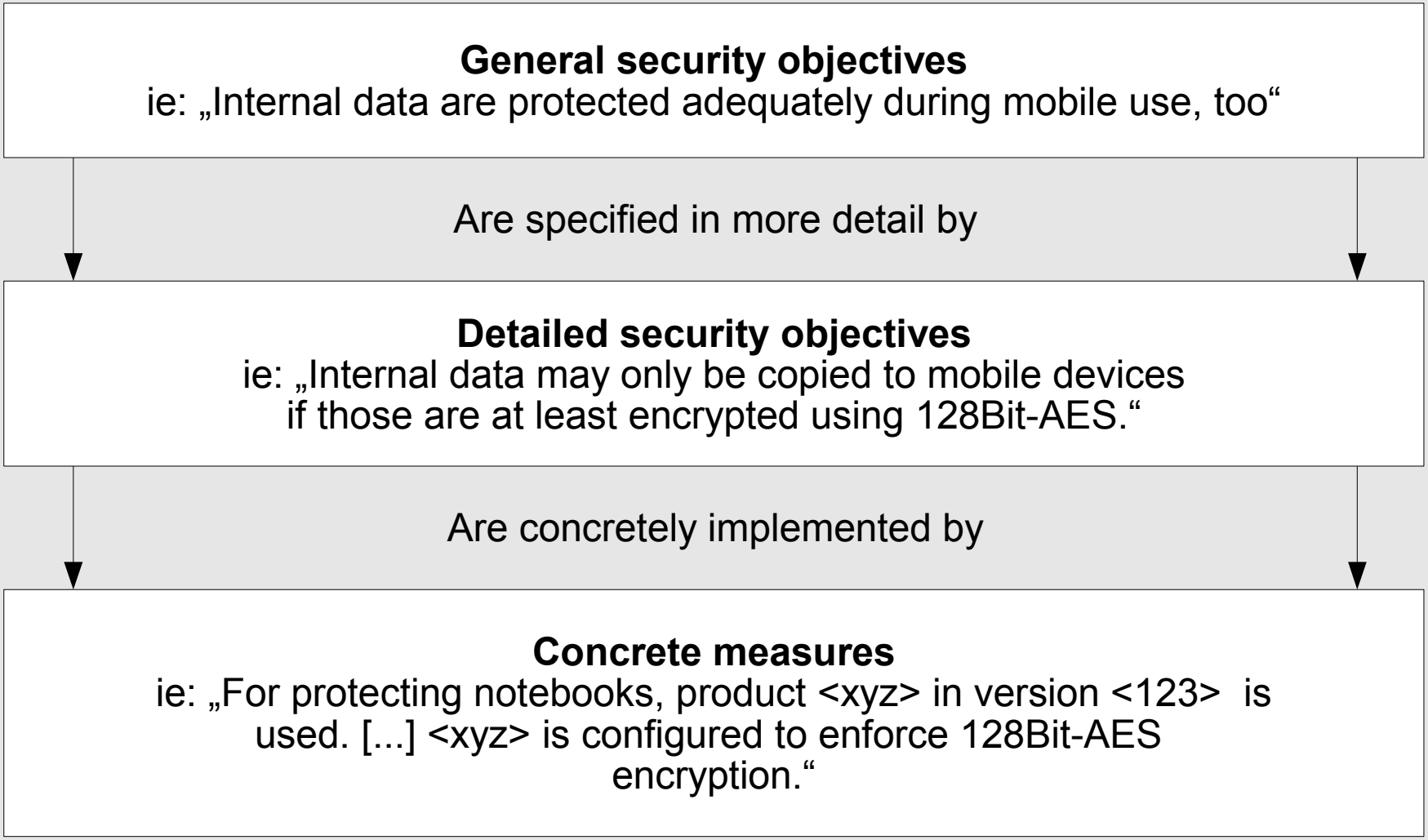
Since 1995: BS 7799

- British standard
- **Best practices!**
- 1995: Additional BS 7799-2 – „Information Security Management Systems“
- Complete update in 1999
  - BS 7799-1:1999 + BS7799-2:1999

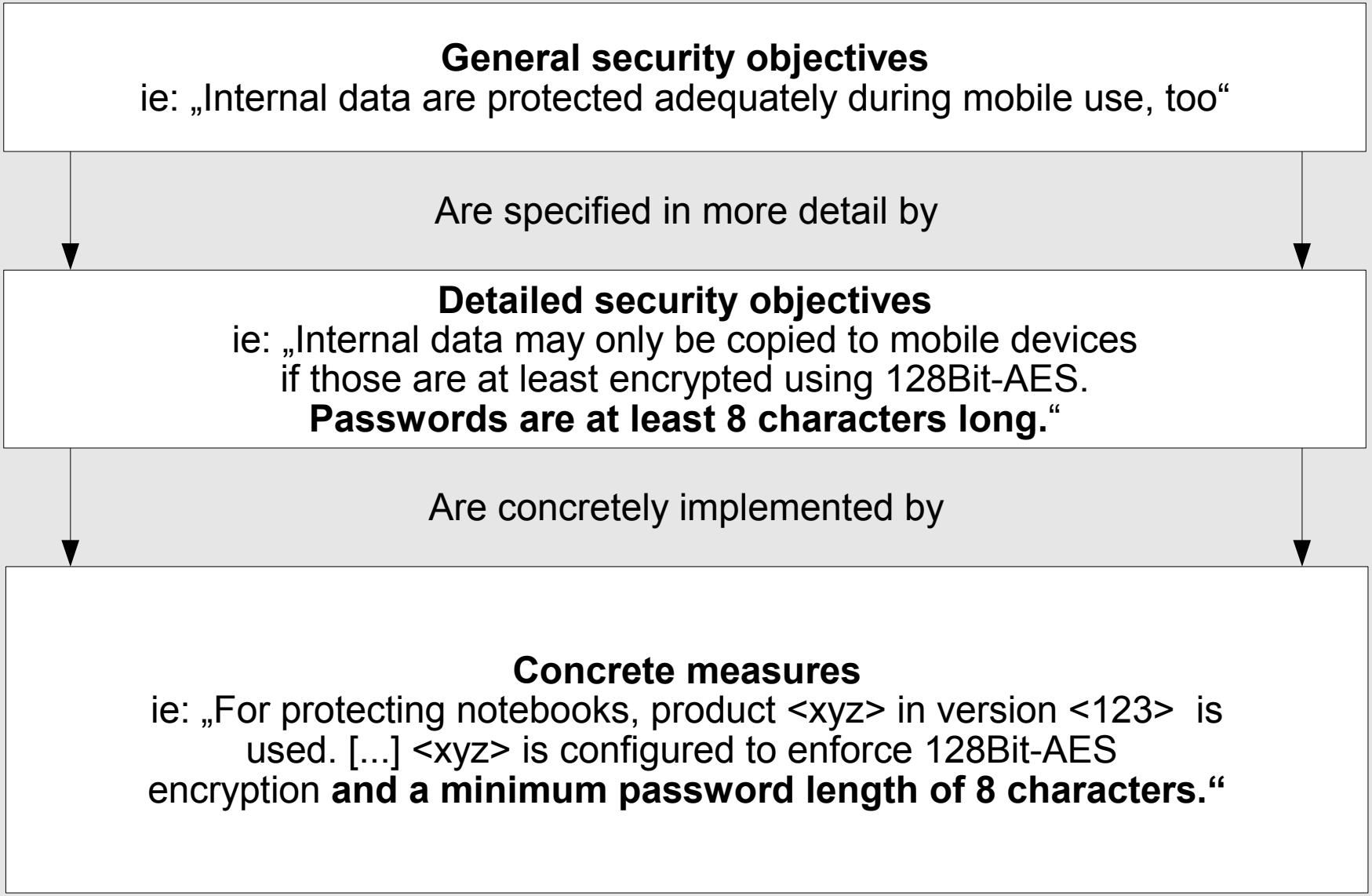
Since 1995: BSI-GSHB

- German Federal Office for Information Security (BSI)
- *G*rund*S*chutz*H*and*B*uch
- English: Baseline Protection Manual (BPM)
- Consists of different modules
- Should help to meet „medium protection requirements“
- Thousands of pages
- Rather reference book than manual or guide

Since ~1999: Security Policies



Since ~1999: Security Policies



Since ~1999: Security Policies

General security objectives
ie: „Internal data are protected adequately during mobile use, too“

Are specified in more detail by

Detailed security objectives
ie: „Internal data may only be copied to mobile devices if those are at least encrypted using 128Bit-AES. **Passwords are at least 8 characters long.**“

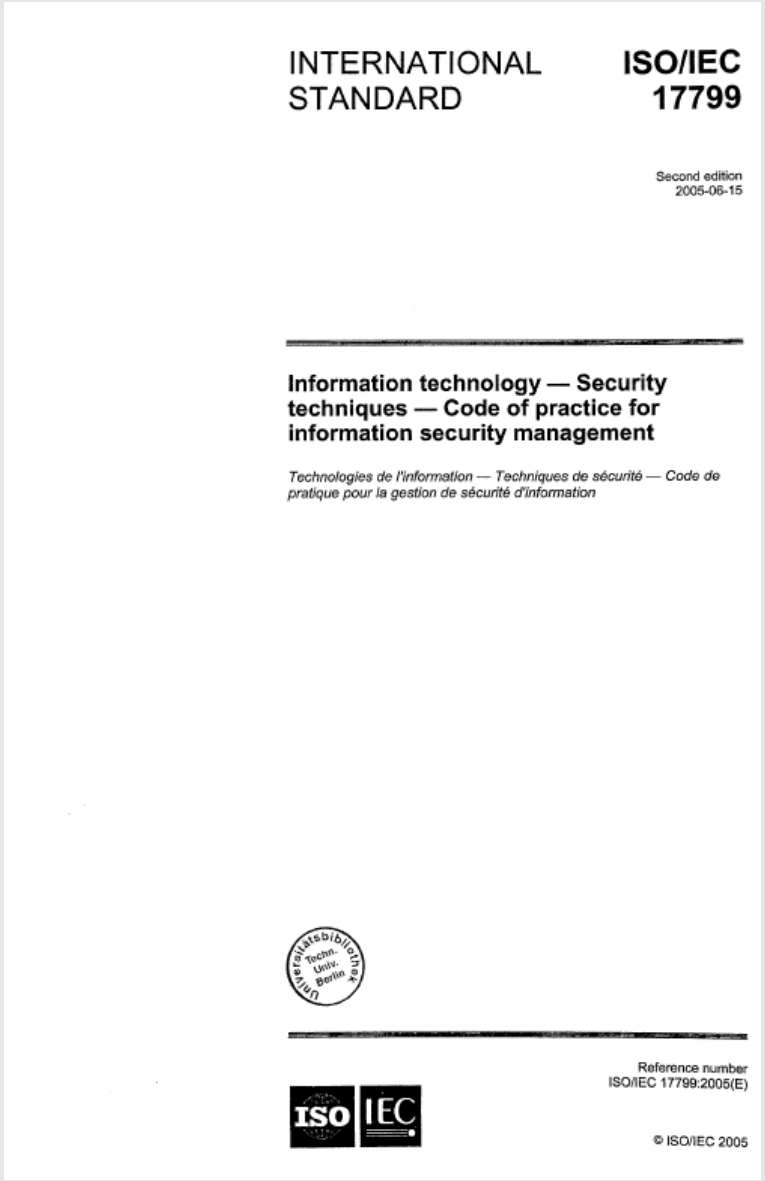
Are concretely implemented by

Concrete measures
ie: „For protecting notebooks, product <xyz> in version <123> is used. [...] <xyz> is configured to enforce 128Bit-AES encryption. **Employees are obligated to choose passwords with 8 or more characters.“**

$t - 2^3$ years: 2000

Since 2000: ISO / IEC 17799

- „Information technology – security techniques – Code of practice for information security management“
- one-to-one-copy of BS 7799-1:1999 (not -2!)



INTERNATIONAL STANDARD

ISO/IEC 17799

Second edition
2005-06-15

Information technology — Security techniques — Code of practice for information security management

Technologies de l'information — Techniques de sécurité — Code de pratique pour la gestion de sécurité d'information

Reference number
ISO/IEC 17799:2005(E)

ISO IEC

ISO / IEC 17799: An example

10.5.1 Information back-up

Control

Back-up copies of information and software should be taken and tested regularly in accordance with the agreed backup policy.

Implementation guidance

Adequate back-up facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure.

The following items for information back up should be considered:

a) the necessary level of back-up information should be defined;

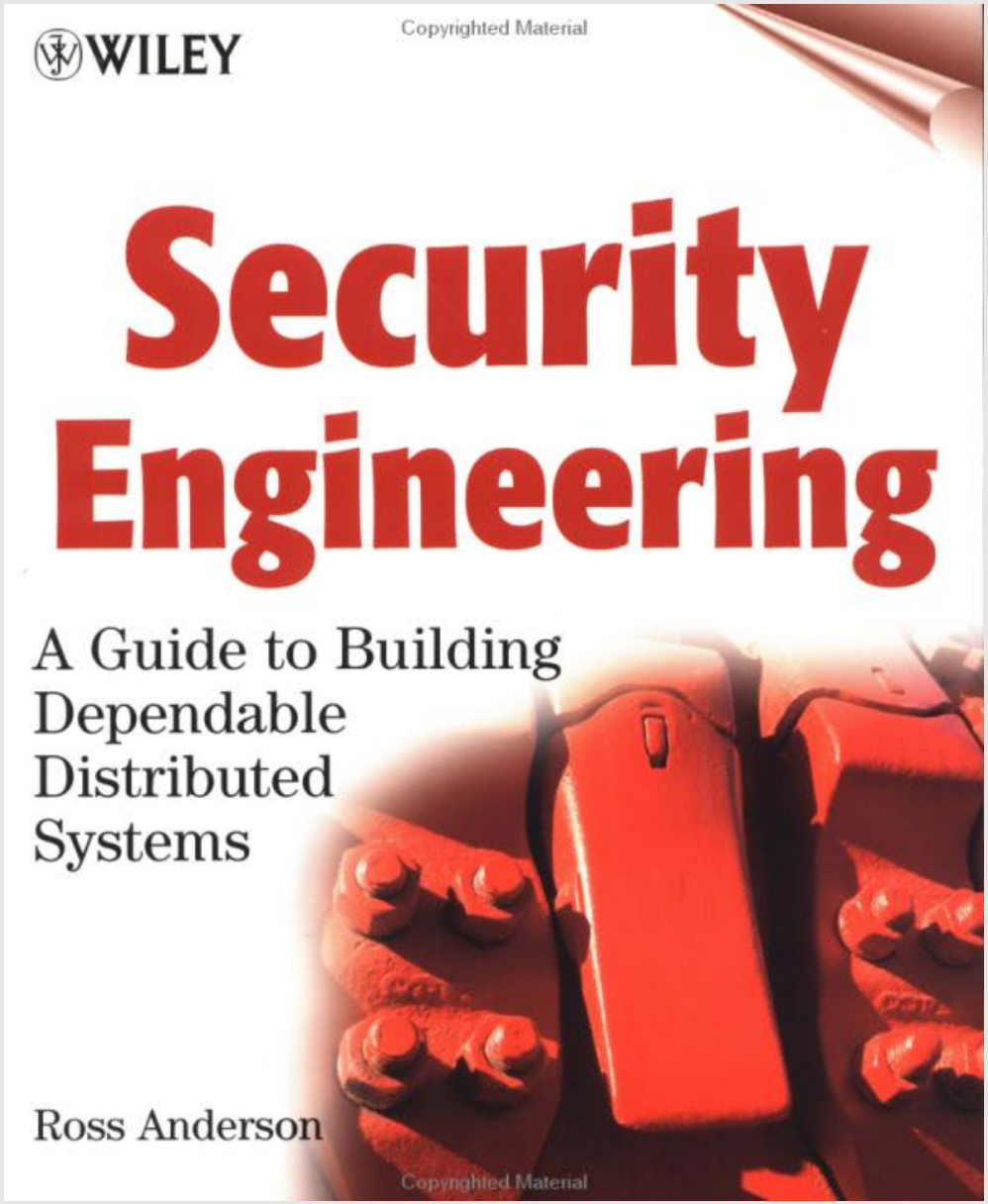
b) accurate and complete records of the back-up copies and documented restoration procedures should be produced;

c) the extent (e.g. full or differential backup) and frequency of backups should reflect the business requirements of the organization, the security requirements of the information involved, and the criticality of the information to the continued operation of the organization;

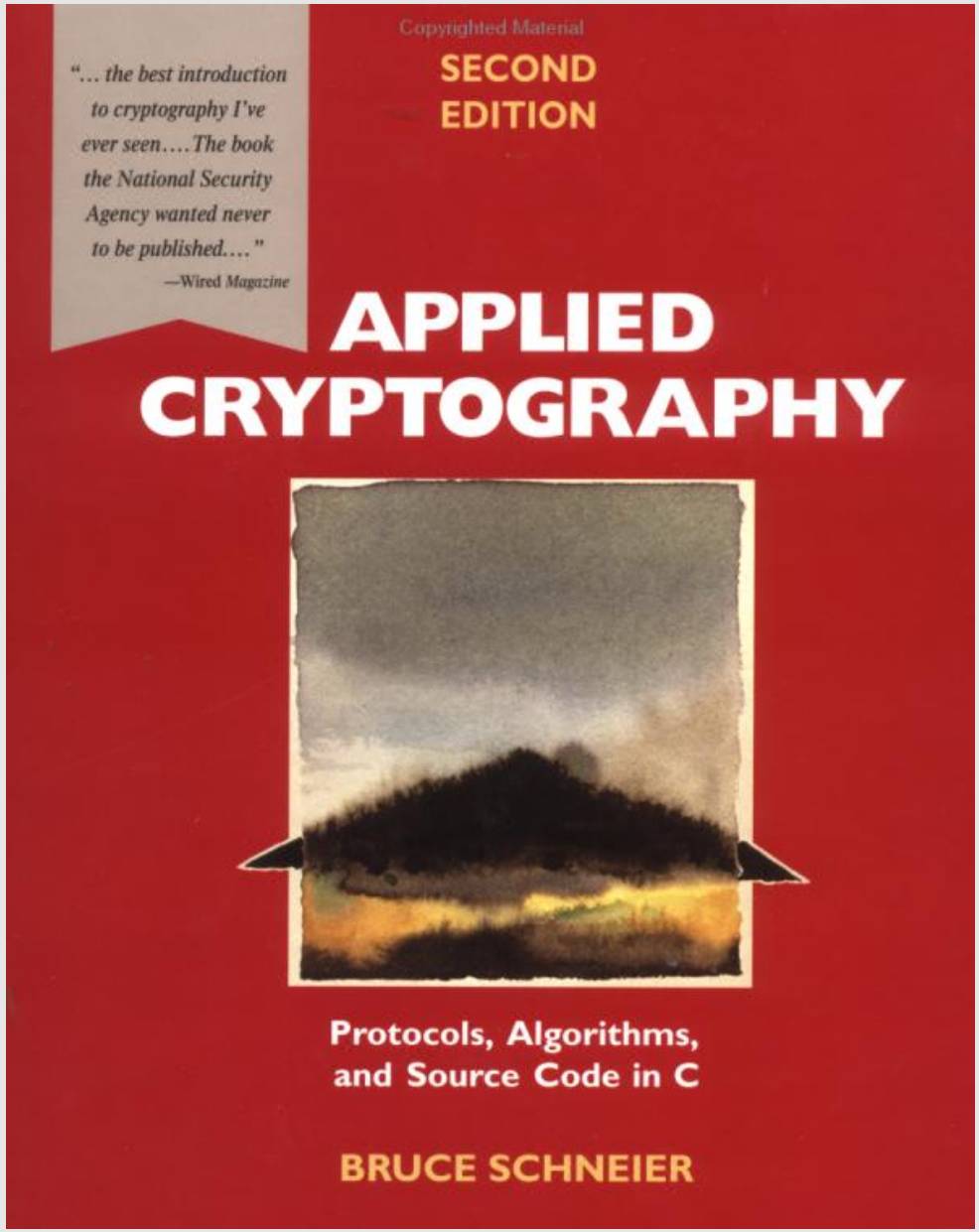
Since 2000: ISO 17799

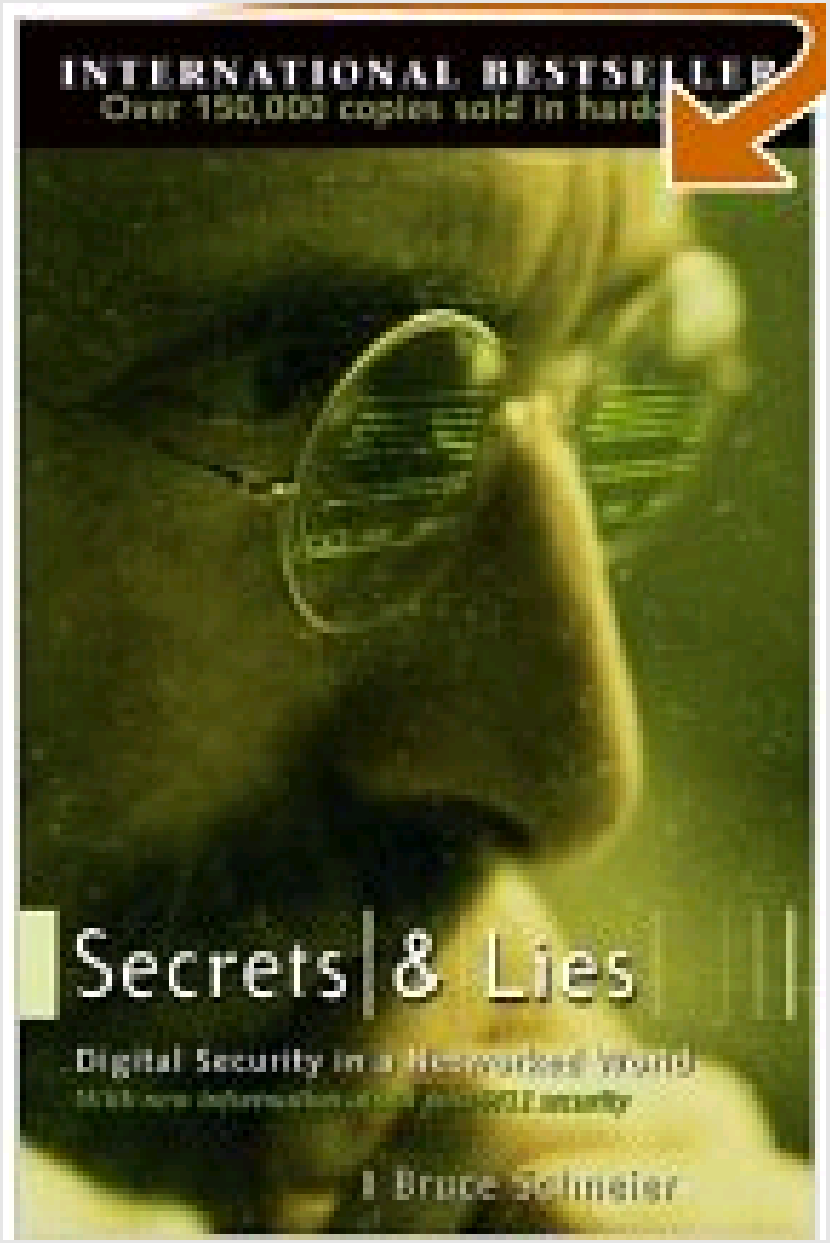
- „Information technology – security techniques – Code of practice for information security management“
- one-to-one-copy of BS 7799-1:1999 (not -2!)
- **Best practices! Recommendations!**

2001: Security Engineering



2000: Schneier again





2000: Secrets & Lies

„I have written this book partly to correct a mistake.“

„The error of *Applied Cryptography* is that I didn't talk at all about the context. I talked about cryptography as if it were The Answer™.“

„I was pretty naïve.“

„If you think technology can solve your security problems, then you don't understand the problems and you don't understand th technology.“

Comparably, already 1996

„No viable secure system design can be based on the principles of policy, integrity, and security, because in the modern world integrity and secrecy are not achievable and policy is not manageable.“

Bob Blakely, IBM:
The emperor's old armor

2000-2002: Enron etc.

- Several cases of accounting fraud
- Serious impact on US-Economy
- Insufficient revision by accounting firms
- Solution approach: Sarbanes-Oxley-Act (SOX, SOA, ...)

Quelle: http://upload.wikimedia.org/wikipedia/

2002: Sarbanes-Oxley-Act

Section 101:

*„There is established the Public Company Accounting Oversight Board to **oversee the audit** of public companies [...]"*

Section 302:

„[...] the principal executive officer [...] certify each [...] report that [...] the signing officers [...] have designed such internal controls to ensure that material information is made known to such officers [...]"

Section 404:

„[...] responsibility of management for establishing and maintaining an adequate internal control structure [...]"

„[...] contain an assessment of the effectiveness of the control structure"

PCAOB - SOX-Interpretation

„COSO's publication (also referred to simply as COSO) provides a suitable framework for purposes of management's assessment"

PCAOB (2004):
„Board Considers Adopting Standards..."

- ➔ Concretion/expansion/interpretation of the law by PCAOB
- ➔ Use of COSO + CobiT or similar frameworks effectively becomes obligatory for many companies
- ➔ „SOX by proxy" (Pinder, 2005)

Major shift 3:

From shared systems to decentralized processing

Implication:

Security Management, maybe?

Distributed Systems

„As soon as you have distributed systems, you have people responsible for security in all sorts of places [...]“

Roger Needham, MS Research (2002):
„Mobile Computing versus immobile Security“

2000-2004: <nil>

Viruses

Worms

Spam

WLAN

Trojans

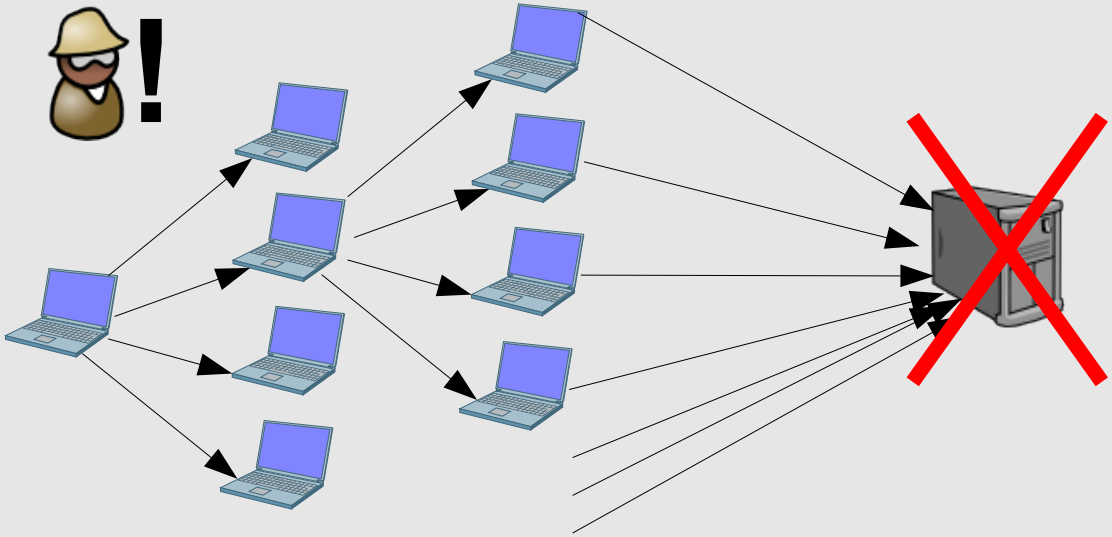
...

Bluetooth

Malware etc.

The Shmoo Group

AirSnort Homepage



t – 2^2 years: 2004

2004: Basel II passed

„For Basel II, in the UK [...] risks must be identified and mitigating controls must also be put in place for ***People, Processes and systems***"

„The FSA handbook [...] states that 'Security should have regard to established security standards such as ***ISO 17799*** *[...]'"*

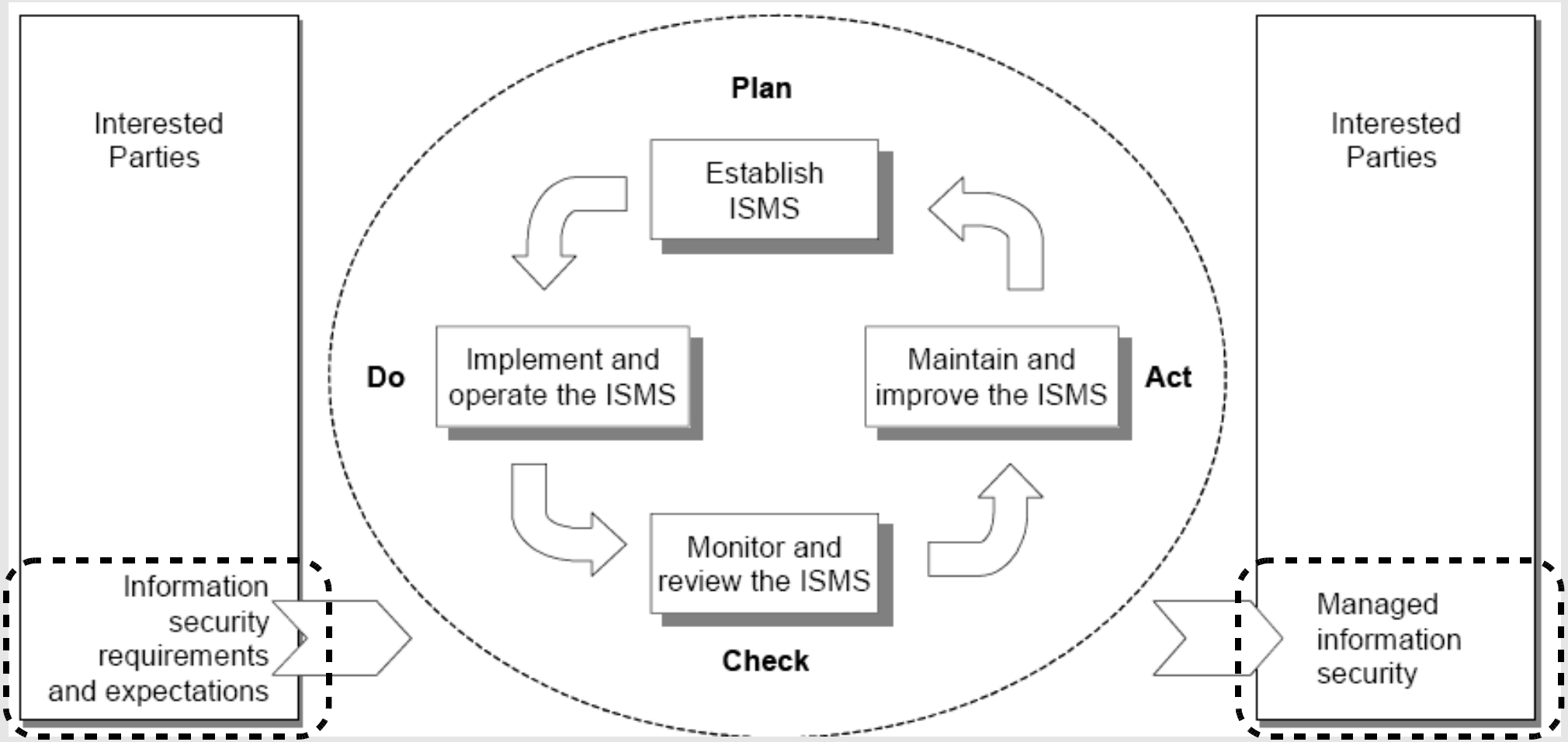
„This then raises the question of whether the role of Information Security [...] should be incorporated into the ***Risk Function***"

Pinder (2005):
„Preparing Information Security for legal and regulatory..."

2005: Updating Standards

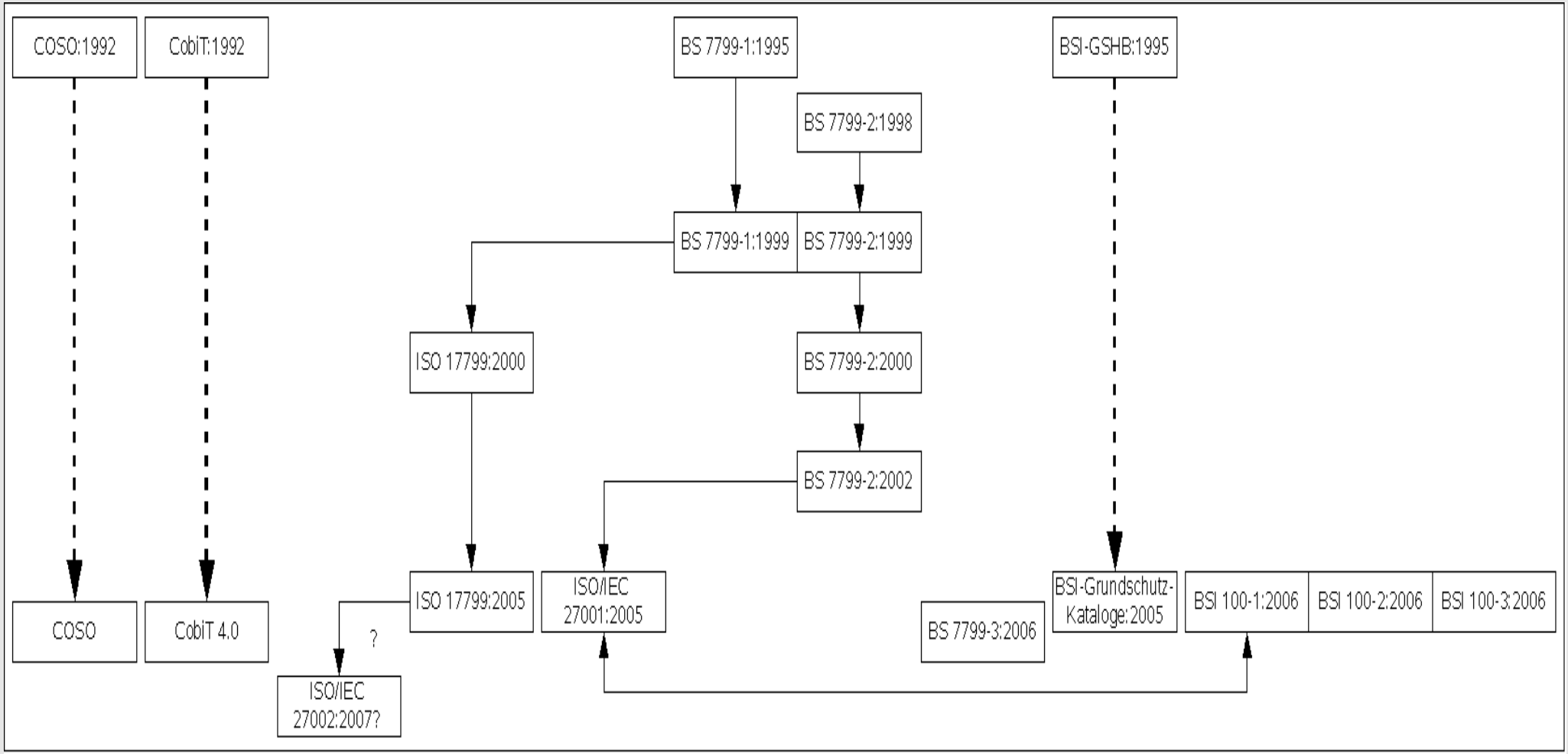
- BS 7799-1:2005
- ISO 17799:2005
- New Standard ISO/IEC 27001: 2005
  - Based on BS 7799-2
  - Certification possible / intended

ISO/IEC 27001 - Excerpts



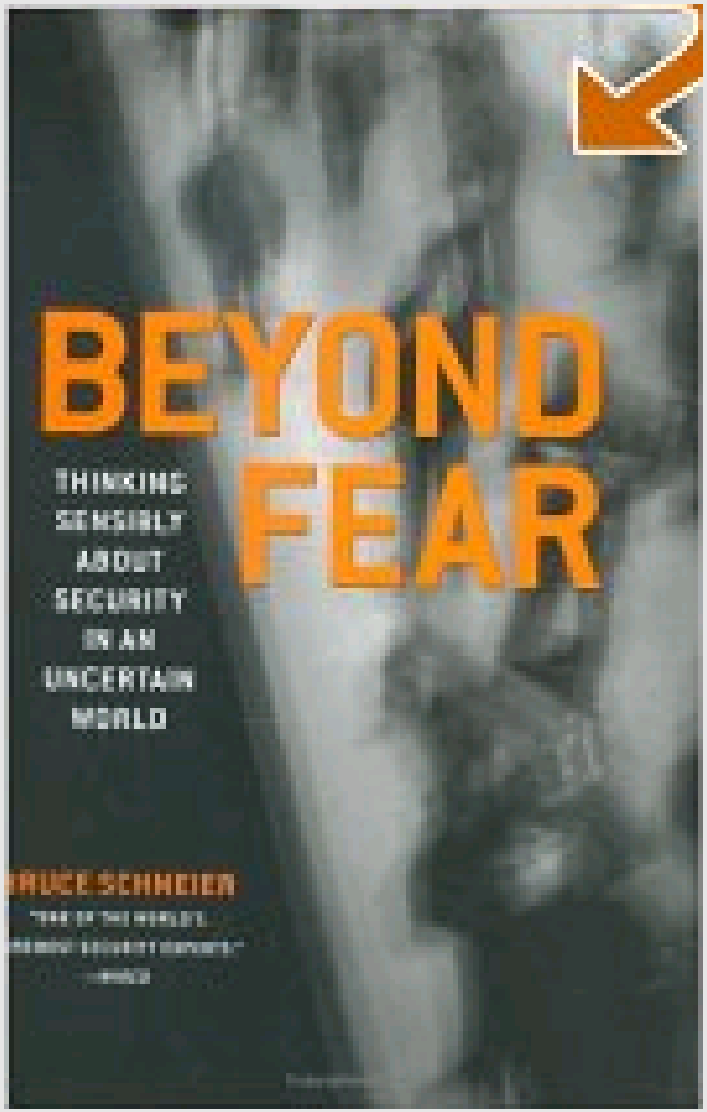
$t - 2^1$ years: 2006

Standards, Standards, ...



$t - 2^0$ years: 2007

2007/2008: Schneier, Once More



Bruce Schneier

The Psychology of Security

By Bruce Schneier
January 18, 2008

PDF version
Spanish translation by seguridaddigital.info
Italian translation by Agatino Grillo

Introduction

Security is both a feeling and a reality. And they're not the same.

The reality of security is mathematical, based on the probability of different risks and the effectiveness of different countermeasures. We can calculate how secure your home is from burglary, based on such factors as the crime rate in the neighborhood you live in and your door-locking habits. We can calculate how likely it is for you to be murdered, either on the streets by a stranger or in your home by a family member. Or how likely you are to be the victim of identity theft. Given a large enough set of statistics on criminal acts, it's not even hard; insurance companies do it all the time.

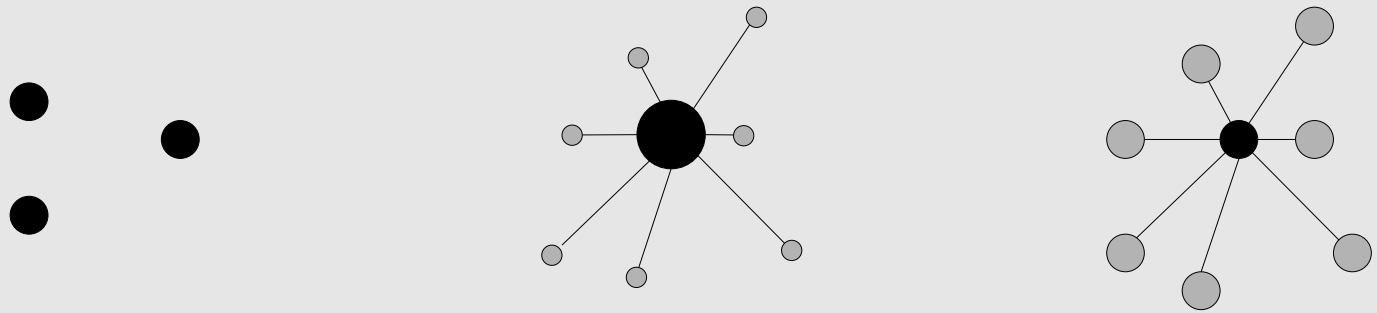
We can also calculate how much more secure a burglar alarm will make your home, or how well a credit freeze will protect you from identity theft. Again, given enough data it's easy.

But security is also a feeling, based not on probabilities and mathematical calculations, but on your psychological reactions to both risks and countermeasures. You might feel terribly afraid of terrorism, or you might feel like it's not something worth worrying about. You might feel safer when you see people taking their shoes

Conclusion

- Security has been important topic for centuries
- Businesses „make“ Information Security
  - because of self-interest (trade-secrets etc.)
  - because they have to (SOX etc.)
  - because they have to for self-interest (Basel II, ...)
- New paradigms of computer use lead to new approaches
- Recently:
  - Standards, Standards, Standards
  - Structured „Information Security Management“
  - „Security Awareness“, „Security Culture“

Conclusion II



Computing Era	Isolated	Mainframe	Distributed
Security Measures	Walls Locks etc.	Encryption Access Control etc.	Security Policies Awareness Programs etc.
Protection Paradigm	Physical	Technical	Managerial

Outlook

Major trends in academia:

Economics of Information Security

Psychology of Information Security

Both together

The End