

D4 Data and Ethics

Autumn 2022 | Lecture 3 - Part I

Focus: Information security & cybersecurity | Author: Prof. Dr. Petra Maria Aspiron | FHNW



KW	Date	Date	#	Topics	LernSetting WI	Lecturer
38 39	Self Study	First 2 weeks	0	Awareness - Entry Test with Moodle Test (20% counted to course grade)	Virtual	Selfstudy
38		KW38	0 + 7	Coaching Session (according to the information of the respective school)	on site	JRN= Juchler Norman Rerabek Martin Nyfeler Matthias
38	Fr, afternoon	23.09.2022	1	Personal Security	Virtual	Pascal Moriggl
39		KW39	1	Coaching Session	on site	FHNW: Pascal Moriggl ZHAW: JRN
39	Fr, afternoon	30.09.2022	2	Information Security & Cybersecurity I	Virtual	Petra M. Asprien
40		KW40	2	Coaching Session	on site	FHNW: Petra M. Asprien ZHAW: JRN
40	Fr, afternoon	07.10.2022	3	Information Security & Cybersecurity II	Virtual	Petra M. Asprien
41		KW41	3	Coaching Session	on site	FHNW: Pascal Moriggl ZHAW: JRN
41	Fr, afternoon	14.10.2022	4	Data Stewardship I	Virtual	Pascal Moriggl
42		KW42	4	Coaching Session	on site	FHNW: Pascal Moriggl ZHAW: JRN
42	Fr, afternoon	21.10.2022	5	Data Stewardship II	Virtual	Pascal Moriggl
43		KW43	5	Coaching Session	on site	FHNW: Pascal Moriggl ZHAW: JRN
43	Fr, afternoon	28.10.2022	6	Data Ethics	Virtual	Pascal Moriggl
44		KW44	6	Coaching Session	on site	FHNW: Pascal Moriggl ZHAW: JRN
44	Fr, afternoon	04.11.2022	7	Data Privacy	Virtual (Flipped Classroom)	Pascal Moriggl

Moodle Link: <https://mslscommunitycentre.ch/course/view.php?id=113>

MS Teams Link: https://teams.microsoft.com/l/meetup-join/19%3ameeting_YTdhMmU5ODQtZGMxYy00MmY2LWFjNzltMTA3NGU5OThiY2Rh%40thread.v2/0?context=%7b%22Tid%22%3a%229d1a5fc8-321e-4101-ae63-530730711ac2%22%2c%22Oid%22%3a%223fab2c24-f87a-4c23-91d5-b0e1bc7b5892%22%7d

- Part I -- Repetition L1 → SD1
- Part II -- Organization Layer: Relevant References → SD2
- Part III -- Organization Layer: First control - IS Policy → SD3
- Part IV -- Organization Layer: Selective control - GEIGER → SD4
- Coaching Session #3 → SD5

→ SD = Slide Deck

New ransomware tool corrupts data instead of encrypting

1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1
1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1
1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1
1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1

26 SEP 2022 NEWS

A new variation of Exmatter, a popular exfiltration tool used by ransomware affiliate groups, corrupts system files after stealing them, rather than just encrypting them. This way, attackers can bypass security tools, retaining bargaining power since they have the only copy, and ransomware code flaws can't be used to build decryption tools.

Full Story: Infosecurity (U.K.) | <https://www.infosecurity-magazine.com/news/ransomware-affiliates-adopt-data/>

Quantum scientists share Nobel Prize in Physics

Three scientists who laid the groundwork for the understanding of the odd "entangling" behavior of quantum particles have received the 2022 Nobel Prize in Physics. The scientists paved the way for quantum computing and quantum cryptography. The latter is very promising for a new level of secure communication.

Have a look: <https://www.quantamagazine.org/pioneering-quantum-physicists-win-nobel-prize-in-physics-20221004/>

or

<https://www.youtube.com/watch?v=vTS4b4EOI5o>

<https://www.youtube.com/watch?v=uiiaAJ3c6dM>

Future Internet → Quanten Internet

<https://cacm.acm.org/magazines/2022/8/262904-advances-in-the-quantum-internet/fulltext>

<https://www.businesswire.com/news/home/20220707005530/en/2022-Opportunities-in-Quantum-Networks---Researchers-and-Startups-are-Finding-Ways-to-Deploy-Sensors-in-Networks---ResearchAndMarkets.com>



📷 The Nobel committee for physics announces the winners of the 2022 physics prize during a news conference at in Stockholm on Tuesday. Photograph: Tt News Agency/Reuters

Our topic --
Information Security and Cybersecurity (I&CS)

Now more than ever,
every company is a
data company

Data is

- the representations of facts, concepts or instructions in a manner suitable for communication, interpretation or processing by humans or by automated means. In the simplest terms, data are pieces of information (ISACA)
- the qualitative or quantitative-based information that can be recorded, communicated, and analyzed (CMMI)
- information in a specific representation, usually as a sequence of symbols that have meaning (NIST)
- a variable-length string of zero or more (eight-bit) bytes (NIST)
- a subset of information in an electronic format that allows it to be retrieved or transmitted (NIST)

ISACA glossary - <https://www.isaca.org/resources/glossary>

NIST glossary - <https://csrc.nist.gov/glossary/term/data>

Information is ...

- an asset that, like other important business assets, is essential to an enterprise's business. It can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation (ISACA)

Scope Notes: COBIT 5 and COBIT 2019* perspective*

- any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audio-visual. An instance of an information type (NIST)
- acts and ideas, which can be represented (encoded) as various forms of data (NIST)

ISACA glossary - <https://www.isaca.org/resources/glossary>

NIST glossary - <https://csrc.nist.gov/glossary/term/data>

* COBIT - <https://www.isaca.org/resources/cobit>

Cybersecurity is ... (1/3)

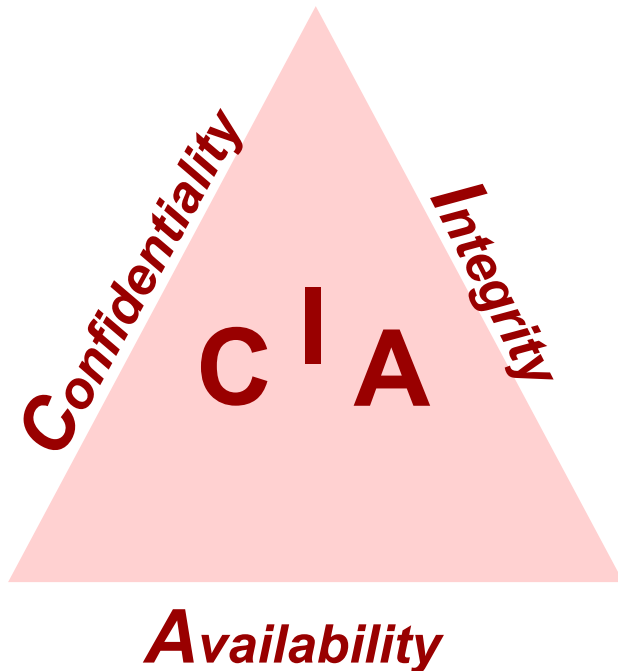
1. the protection of information assets by addressing threats to information processed, stored and transported by internetworked information systems
2. the protection and restoration of products, services, solutions, and supply chain; including technology, computers, telecommunications systems and services, and information; to ensure their availability, integrity, authentication, transport, confidentiality, and resilience. Cybersecurity is a part of information security (CMMI)

ISACA glossary - <https://www.isaca.org/resources/glossary>

Note: There are different spellings of cybersecurity; to get a sound overview the 2015' ENISA paper "Definition of Cybersecurity – Gaps and overlaps in standardisation" is recommended (see also on Moodle). In this course we use the spelling 'cybersecurity'.

The concept of the CIA triad

a well-known model for security policy development, used to identify problem areas and necessary solutions for information security.



Confidentiality -- restrict access to authorized individuals

Integrity -- data has not been altered in an unauthorized manner

Availability -- information can be accessed and modified by authorized individuals in an appropriate timeframe

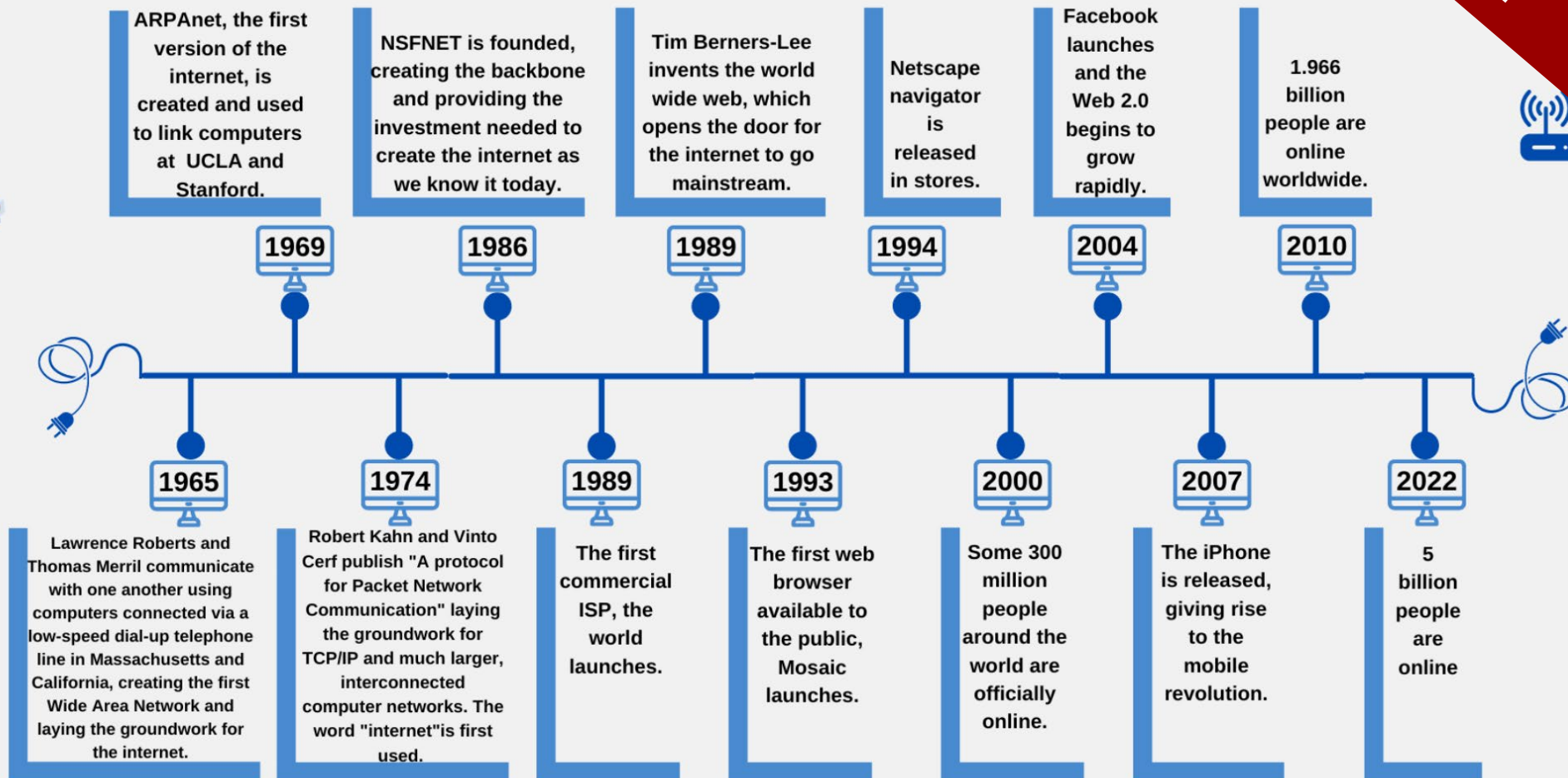
Source: 2012, Perrin, Chad. "The CIA Triad"

Have a look: <https://www.youtube.com/watch?v=bhLbnOa4wno>

Some Leading Organizations *(mentioned)*



The Internet in a timeline ...



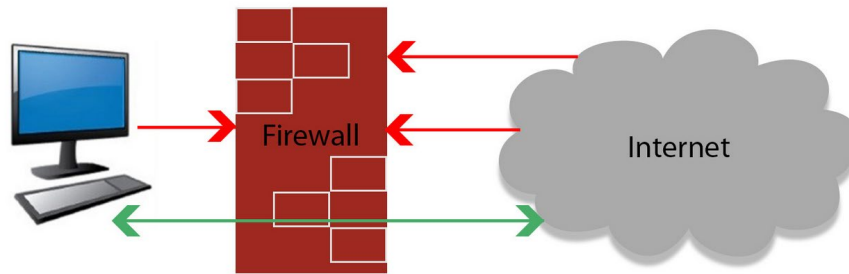
Source. <https://www.broadbandsearch.net/blog/who-invented-the-internet-full-history>

Interesting Links: <https://www.internethalloffame.org/internet-history/timeline>

Have a look: <https://www.scienceandmediamuseum.org.uk/objects-and-stories/short-history-internet>

Risk Management – Important Protection

Repetition
Lecture 2 - II

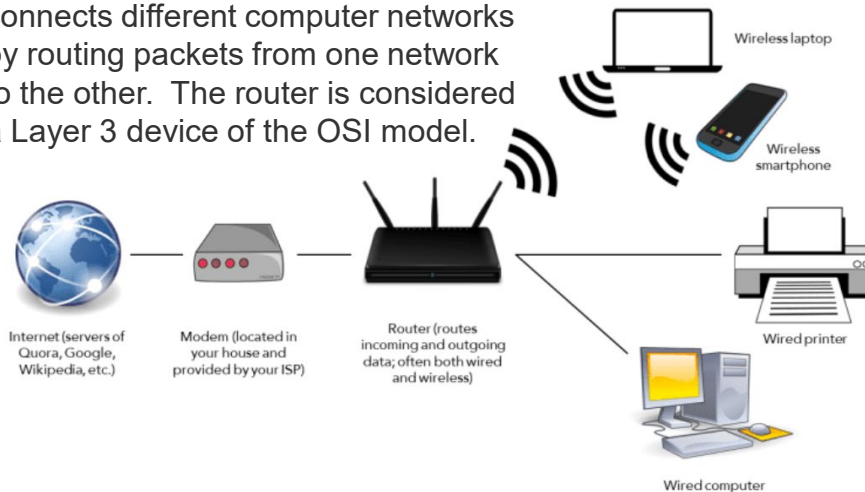


A **Firewall** – the first line of defense in network security - is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

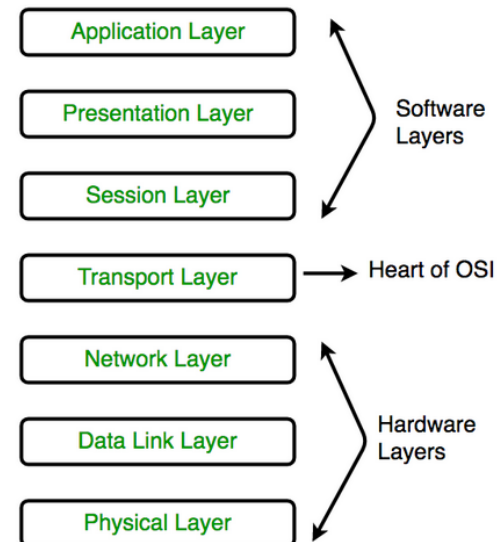


Anti-virus Software looks for patterns based on the signatures or definitions of known malware.

A **Router** is a network device that connects different computer networks by routing packets from one network to the other. The router is considered a Layer 3 device of the OSI model.




The **OSI** model (Open Systems Interconnection) describes the functions of a networking system and characterizes computing functions into a universal set of rules and requirements to support interoperability between different products and software.



Today --- Conclusion ---

With more usage,
it needs more
security!

This learning took place very early ...

A portrait of Edward Snowden, a man with glasses and a slight beard, looking directly at the camera. The image is slightly blurred and has a soft, pinkish tint.

in 2013, Snowden leaked
around 200,000 classified
U.S. documents
confidential data

National Security Whistleblower

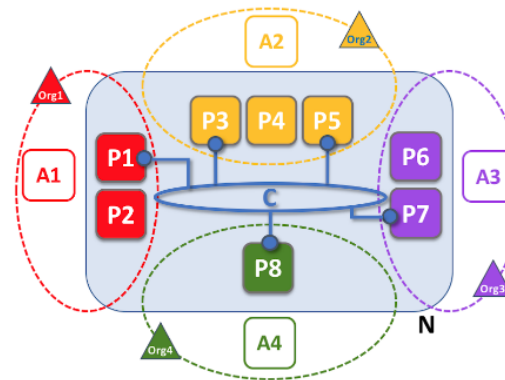
- Edward Snowden copied and leaked classified information from the National Security Agency (NSA), he leaked that the government was 'spying' on the public. He is controversially thought of as a hero to some, and a traitor to others (<https://www.bbc.com/news/technology-54013527>)
 - In 2020, the NSA surveillance of millions of Americans' telephone records was ruled unlawful by the US Court of Appeals. Mr Snowden said afterwards that he felt vindicated by the ruling.
 - *BBC news (2022-09-26): Putin grants Russian citizenship to Edward Snowden - <https://www.bbc.com/news/world-europe-63036991>*

Excuse – Whistleblowing (1/2)

A Blockchain-based Whistleblower Plattform



I@I – Application -- Frontend



I@I -- Underlying Architecture

N	Blockchain Network	L	Ledger
C	Channel	A	Application
P	Peer	PA	Principal PA (e.g. A1, P5) communicates via channel C.
		Org	Organization
		Organization R owns application A1 and peers P1, P2.	

2/2

FHNW HSW:	IWI Competence Center Blockchain Lead: Petra Maria Asprion
Funding:	KBA-NotaSys Integrity Fund, Lausanne
Duration:	2021-05 – 2022-03
Consortium:	FHNW HSW, CC Blockchain
Website:	https://whistleblowersystem.herokuapp.com/
Contact Person:	Frank Grimberg, Hermann Grieder
Student participation:	TOBIT (4 students) BSc Praxis Project MSc BIS Master Thesis

Sources.

- (1) Asprion, P.M., Grieder, H., Grimberg, F. (2022): Blockchain-basierte Meldesysteme. Vorstellung des Projekts Integrity@Inside. In: comply. Fachmagazin für Compliance Verantwortliche, Jhrg. 7, 3/2022, S.18-22.
- (2) Asprion, P.M., Grieder, H., Grimberg, F. (2023): Building Digital Trust to Protect Whistleblowers - A blockchain-based Reporting Channel. HICCS56, 2023. Accepted.

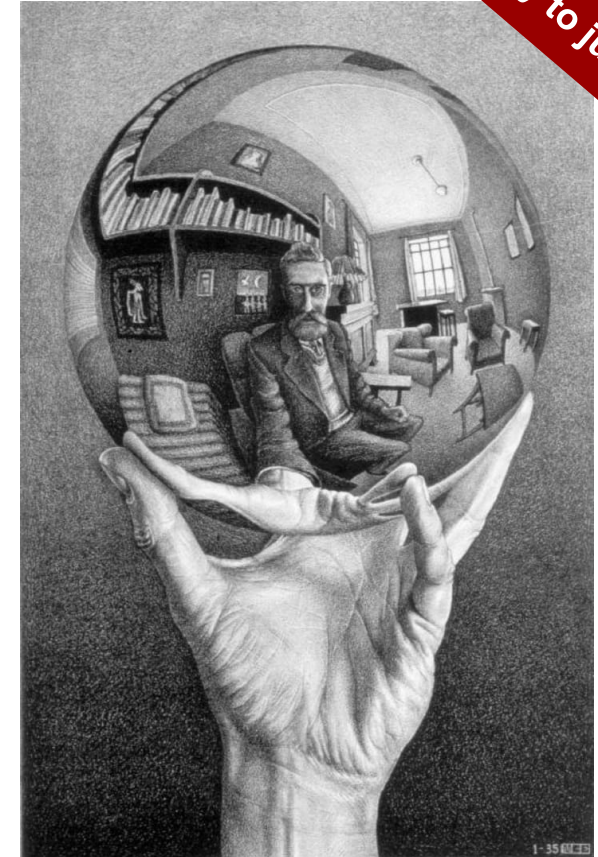
First – try jump over the four walls ...

Today' – in 2022 – the dynamic geo-political and regulatory landscape shows that traditional cybersecurity approaches are no longer sufficient enough.

Practices established when IT infrastructure components were located within a company's **four walls** are not sufficient in the light of covid and in an era of **Cloud Computing (CC)**, **Internet of Things (IoT)**, **Internet of Everything (IoE)**, **Artificial intelligence (AI)** and **Advanced Analytics**.

The threat situation or cyberattack risks faced by companies using outmoded security methods have increased dramatically during the COVID-19 pandemic. With most employees working remotely, sensitive data needs to be shared outside a company's walls.

This includes **employee data**, **intellectual property**, **corporate financial data**, and **other proprietary information**. It also includes the **supply chain**, data on suppliers, customers, their purchases, and the performance of products in the field.



'Hand With Reflecting Sphere' – M.C. Escher, 1935

The reflection of a mirror, plus the geometric properties of a sphere, makes for a unique self portrait by Dutch artist M. C. Escher

Repetition
Lecture 2 – III
Be informed and try to jump ...

Assessment of your current situation

- **Practitioner approach:** Use established instruments to be informed and to get an initial overview
- **First idea:** Use an easily accessible tool, like ...
 - the **Cyber Risk Index (CRI)*** -- to be informed
 - this comprehensive index aims to measure an **organization's readiness** to respond to different types of cyber threats or cyber attacks

The CRI is composed of two individual indices:

Cyber preparedness index: Representing an organization's readiness to defend against cyber attacks.

Cyber threat index: The state of the threat landscape at the time the CRI was determined.

Key takeaways for businesses

Our findings show that global businesses have a very high chance of being affected by a cyberattack (Note, these are all down from the previous CRI survey in 1H'2021).

- Likelihood of a data breach of customer data in the next 12 months: **67%.**
- Likelihood of a data breach of critical data (IP) in the next 12 months: **71%.**
- Likelihood of one or more successful cyberattacks in the next 12 months: **76%.**

REGIONAL CYBER RISK INDEX TRENDS



THE PRIMARY BUSINESS RISKS

The top cybersecurity risk factors businesses face can be broken down into five categories, based on the top concerns from respondents across the four regions:

Top five cyber threats

1. Ransomware
2. Phishing and social engineering
3. Denial of service (DoS)
4. Botnets
5. Man-in-the-middle attack

Top five data types at risk

- o "My organization is not well prepared to deal with data breaches and cybersecurity exploits"
- o "My organization's enabling security technologies are not sufficient to protect data assets and IT infrastructure"
- o "My organization's IT security function is not able to contain most cyber attacks"

Human capital risk

- o "My organization's IT security leader (CISO) doesn't have sufficient authority and resources to achieve a strong security posture"
- o "My organization's IT security leader does not report to senior leadership (such as the CEO, COO, or CIO)"
- o "My organization's IT security personnel do not have sufficient knowledge, skill, and expertise to protect data assets and IT infrastructure"

Top five infrastructure risks

1. Mobile/remote employees
2. Cloud computing infrastructure and providers
3. Across third-party applications
4. Malicious insiders
5. Mobile devices, such as smart phones

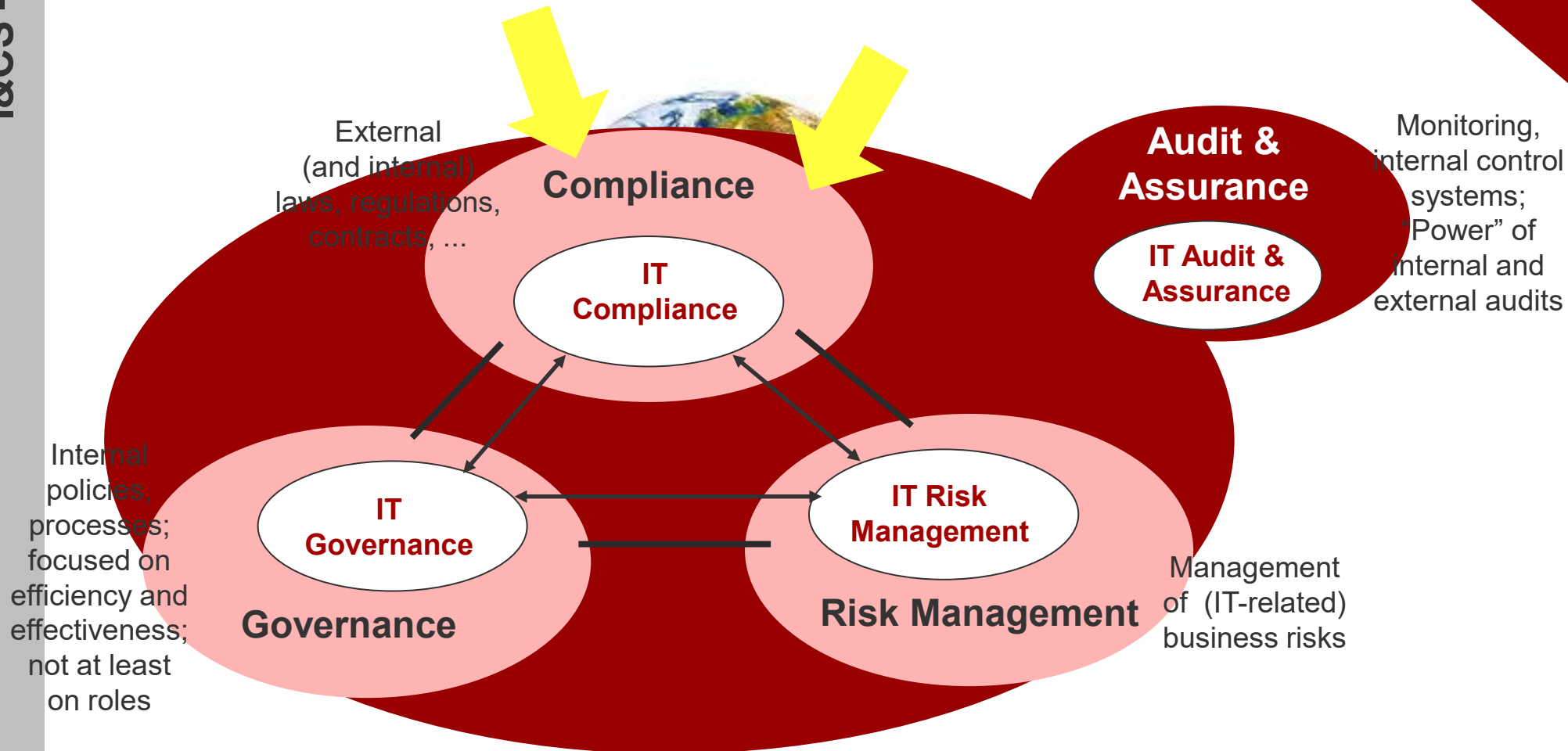
Operational risk

- o "My organization's IT security function lacks support of security in the DevOps environment"
- o "My organization's IT security function does not strictly enforce acts of non-compliance to security policies, standard operating procedures, and external requirements"
- o "My organization's IT security function lacks compliance with data protection and privacy requirements"

Governance, Risks, Compliance Management

→ compliant with legal requirements and supports Risk Management

Repetition
Lecture 2 - IV



Klotz, 2009, p. 11 (adapted)

Authorities and International Organisations



International Organisations

Pharmaceutical Inspection Convention Scheme – PIC/S

International association of 46 GMP-monitoring institutions. Goal: Development, Implementation and fostering of GMP Standards & Quality System.

International Medical Device Regulators Forum (IMDRF)

International forum of medical device regulation

International Society for Pharmaceutical Engineering (ISPE)

ISPE as international operating agency that represents the interests of Pharmacoepidemiology and Pharmacovigilance.

Council for Harmonisation

International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use (ICH) is responsible for the harmonization of human pharmaceuticals as basis for the pharmaceutical admission in Europe, the USA and Japan.



Authorities

Food & Drug Administration (FDA)

U. S. Food and Drug Administration monitors food and pharmaceuticals in the USA

Federal Institute for Drugs and Medical Devices (BfArM)

BfArM is an agency under the Federal Ministry for Health in Germany

European Medicines Agency (EMA)

The European pharmaceutical agency, responsible for the testing and monitoring pharmaceuticals

Medicines & Healthcare Products Regulatory Agency (MHRA)

MHRA is the monitoring and admission authority of medicines in the UK

Swissmedic

Swissmedic is the Swiss admission and control authority for medication.

World Health Organization (WHO)

Coordinating authority of the United States for the international public healthcare.



IMDRF International Medical Device Regulators Forum



ICH harmonisation for better health



Federal Institute for Drugs and Medical Devices



EUROPEAN MEDICINES AGENCY
SCIENCE. MEDICINES. HEALTH.



Medicines & Healthcare products
Regulatory Agency

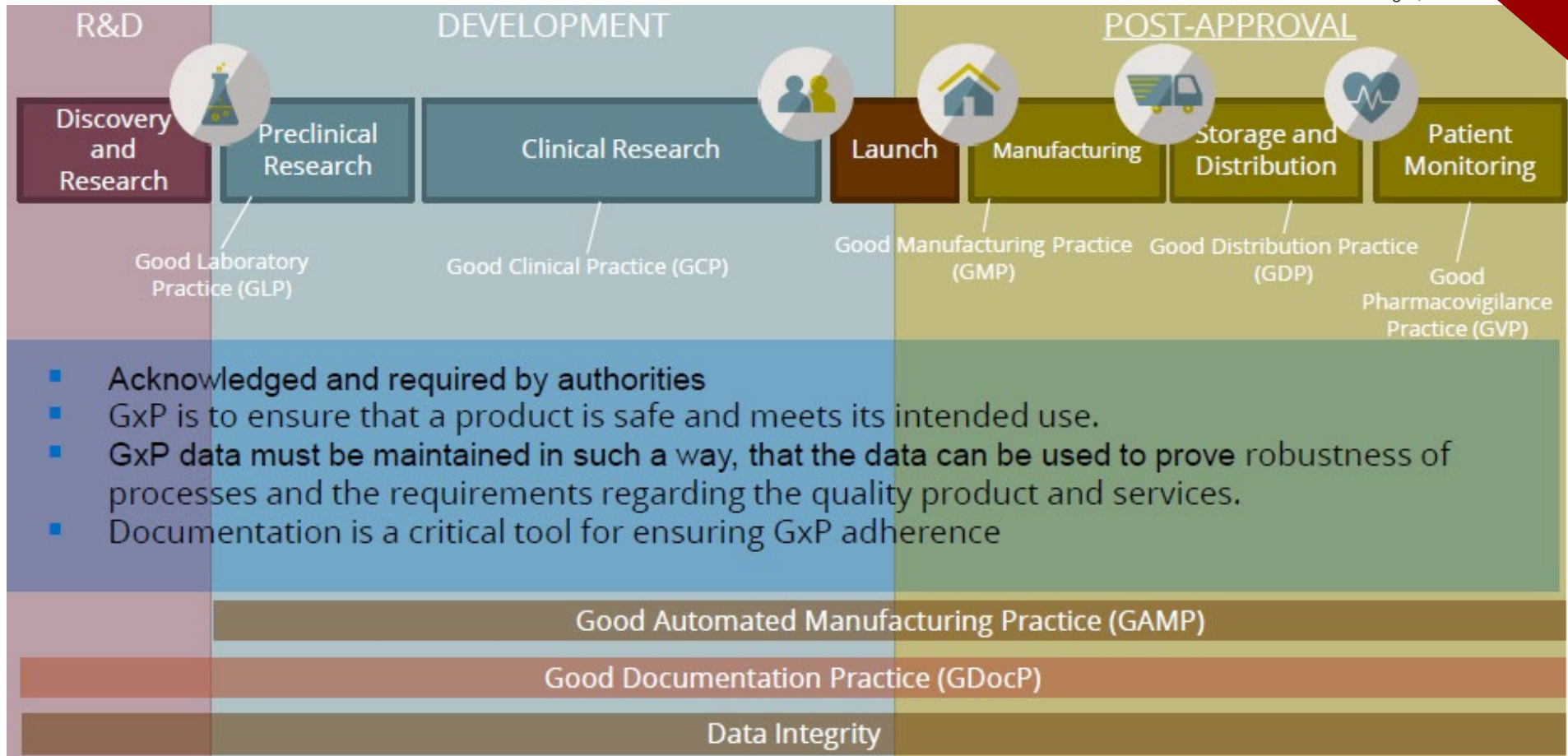


World Health Organization

GxP* – An established standardized good practice

Repetition
Lecture 2 - IV

© Schmiedeberger, 2021



* GxP -- is a general abbreviation for the "good practice" quality guidelines and regulations. The "x" stands for the various fields, including the pharmaceutical and food industries, for example good agricultural practice, or GAP.

In the pharmaceutical industry, the 'x' denotes the following areas: Manufacturing, Distribution, Laboratory, Clinical facilities related, and Documentation

Examples of data integrity problems



Technology

Inadequate or misconfigured IT systems

Missing functionality in infrastructure and applications

Weak technical security controls



Organization & Personnel

- Inadequate business processes
- Weak organizational security controls
- Time pressure on workforce
- Inadequate incentive systems, fear to fail
- Lack of understanding GxP regulations
- Lack of training on IT systems and business processes



And why should you care about data integrity?

The regulators care about data integrity

- Increasing amount of findings in audits/inspections
- Release of guides on data integrity (FDA, MHRA, WHO, PIC/S)
- Sanctions (Recall, Import ban, ...)

Integrity facilitates evidence-based business decision making

Good data management practice is a good foundation to manage data-centered business requirements such as digital transformation and implementation of data privacy (e.g. GDPR)

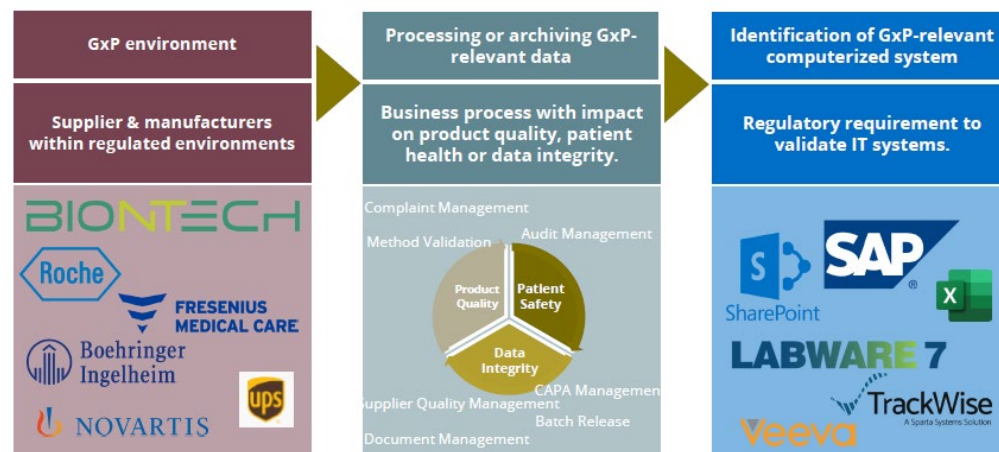
Revelation of data integrity problems has reputational impacts on business

Ensuring data integrity reduces data ownership costs through the data lifecycle

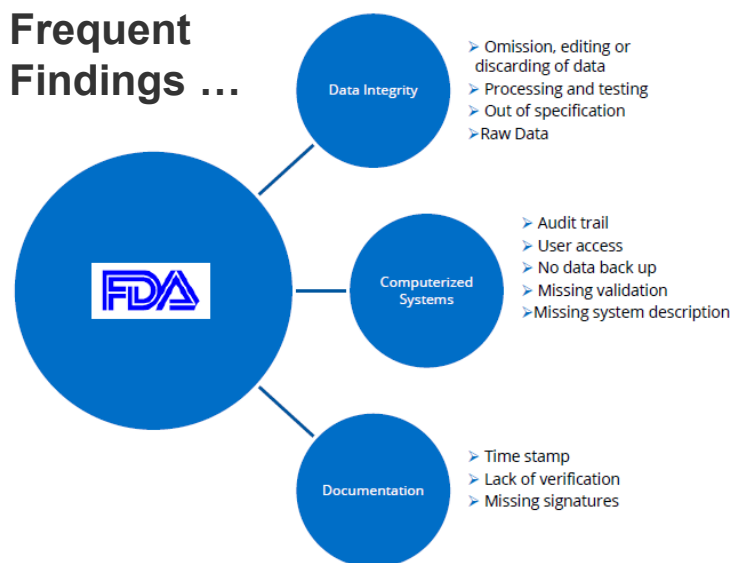
Integrity is the foundation of business excellence and patient safety. Integrity builds trust.

Computerized System Validation

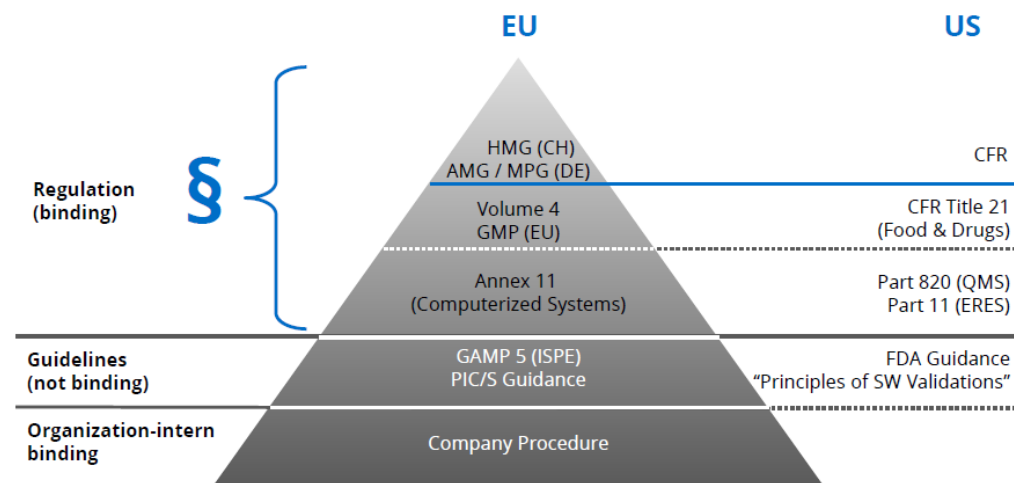
When & Why is Computerized System Validation needed?



Frequent Findings ...



Regulatory Requirements for computerized Systems



What have we discussed so far?

Some News – to emphasise the relevance and actuality of the topic

Relevance and definitions/differentiations of data & information

Concept of CIA – again as one of the most important concepts to secure data

One selective threat situation (Whistleblowing) and a potential control (FHNW research contribution)

GRCM – as a holistic approach to manage (IT) processes ...

Again - influential organisations (you should know)

Again – GxP as an established standardized good practice