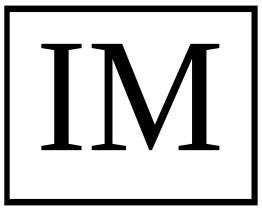


Information Management and Knowledge Management (IMKM)

Lecture 9

Information Security, Privacy and Risk Management

TUM

Chair for Information Systems

Lecture Schedule

Information Systems Strategy

Business Value of IT

- Business IT Alignment
- Guest Lecture: Digital Leadership and the CIO Role
- IT-enabled Strategies
  - Digital Platforms

Information Management

- IT Controlling and IT Governance
- IT Sourcing and IT Offshoring
- **IT Security, Privacy and Risk Management**
- Guest Lecture: Natural Language Processing for IM

Knowledge Management

- Basics
- Tools
- Guest Lecture: Applications

IMKM Lecture 9: Information Security, Privacy and Risk Management

Outline

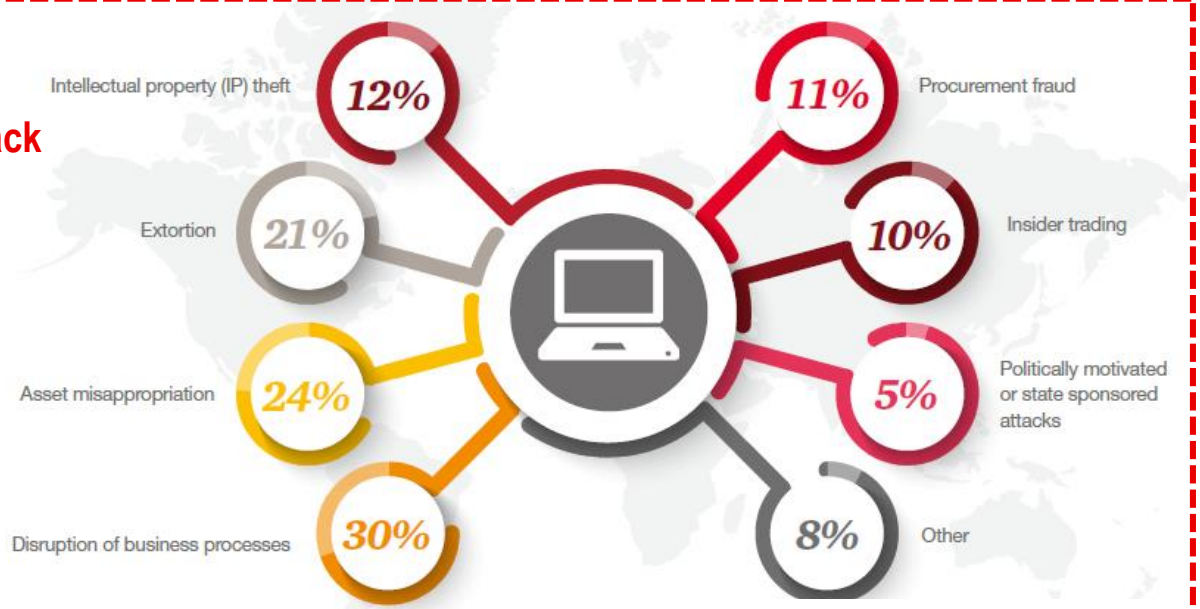
1. **Information Security**
2. Privacy
3. Risk Management
   1. Fundamentals
   2. Risk Management Process
   3. IT Projects

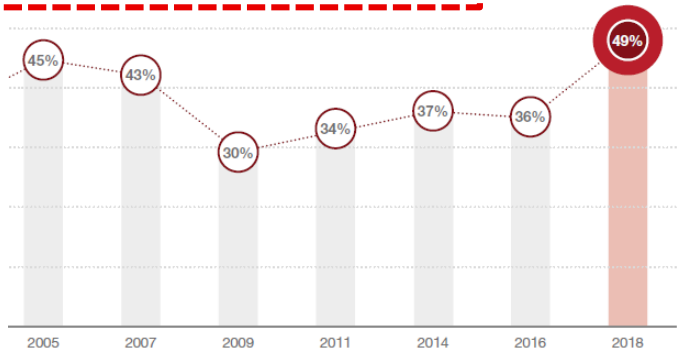
Learning Objectives

- *You understand information security.*
- *You understand the IT security objectives and can distinguish them.*
- *You understand privacy and can discuss the key changes of the GDPR.*
- *You understand and can discuss risk, its categories, and its two strategies.*
- *You can apply the risk management process and know examples for its steps.*
- *You understand and can apply the three characteristics of IT project risks.*

Economic Crime – A Worldwide Phenomenon

Executed through cyber-attack





PwC (2018)

Foundations

- ***Security*** is the absence of unbearable risks (DIN 2002)
- ***Risk*** is the **probability** of an adverse future event multiplied by its **magnitude**
- ***Risk*** is the probability that a particular adverse event occurs during a stated **period of time**, or results from a particular challenge.

  The Royal Society (1983)

Information Security

- The **information** that companies collect, store, manage and transfer is an organizational **asset**. It adds value to business and consequently needs to be suitably **protected.**

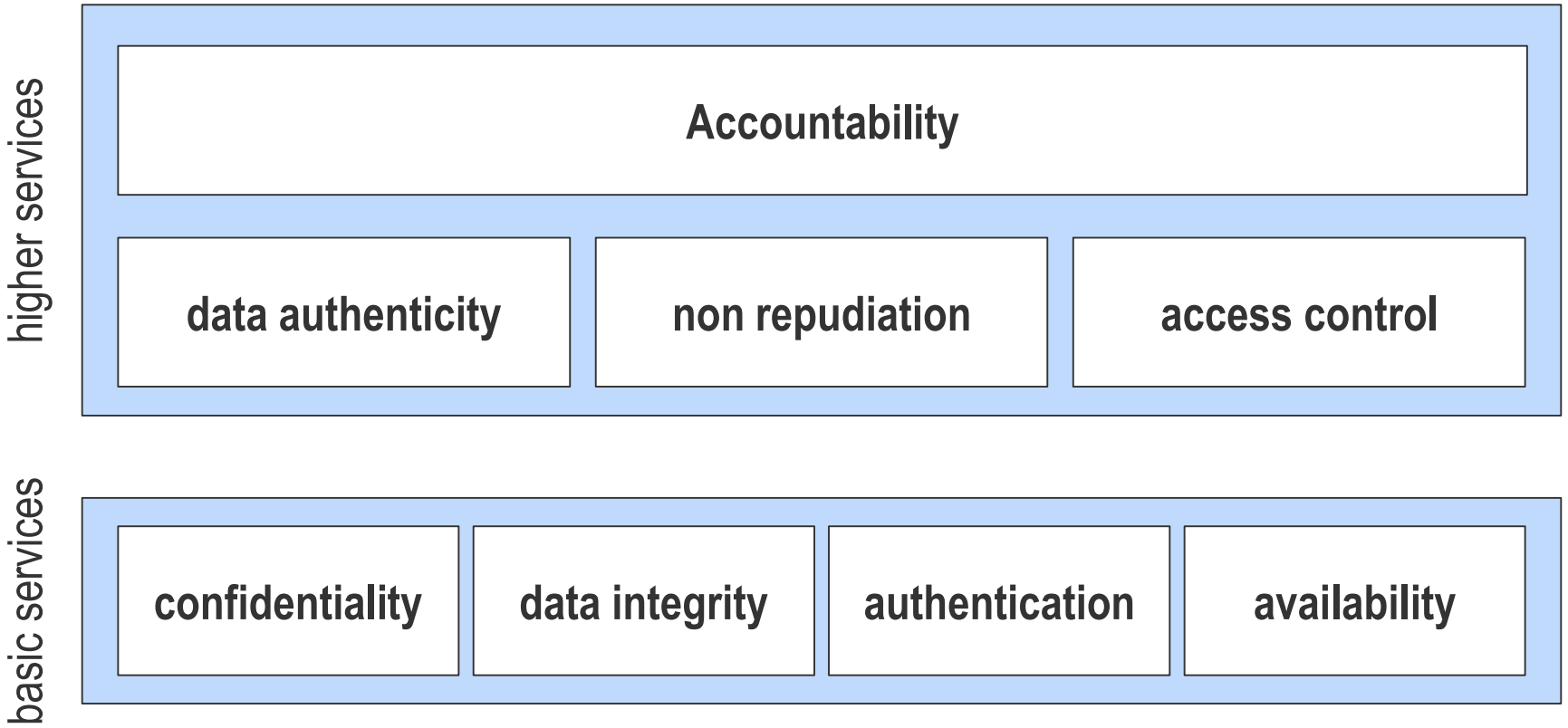
> ***Information security*** *is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical).* [1]

- Today this information is often held electronically, and transmitted using electronic means.

  Growing **dependence on information systems**, shared networks and distributed services like cloud computing means organizations are **now even more vulnerable to security threats**.

[1] 44 U.S. Code § 3542

IT Security Objectives



Eckert (2009)

IT Security Objectives

basic services	Confidentiality	The property that information is not made available or **disclosed to unauthorized individuals**, entities, or processes
	Data Integrity	The property that data has not been **altered** or destroyed in an **unauthorized** manner
	Authentication	The process of **verification** of an **identity**
	Availability	The property of a **reliable access** at the right time on information and information systems.
higher services	Data authenticity	The property of **data** being genuine and being able to be **verified and trusted**; confidence in the validity of data itself and its authorship
	Non-repudiation	Way of guaranteeing that the **sender** of message **cannot** later **deny** having sent that message
	Access control	Process of **granting authorized entities** the right to use information, while preventing access to non-authorized entities
	Accountability	The property of being able to **trace activities** on a system to individuals who may then be held **responsible** for their actions

Eckert (2009); BSI 2018, ISO/IEC 2018; Rao & Nayak 2014

Methods to achieve Basic Security Service Objectives

basic services

Confidentiality	**Encryption** of stored and transmitted data Access control Notifications in case of data breach
Data Integrity	**Hash-Functions**, Backups **Access Control**, Email Signatures, Transmission Certificates Validating Inputs, Non-Repudiation
Authentication	User's Access **Credentials** (e.g., passwords, fingerprint, chip cards) Certificates
Availability	Data/Server Replication, **Redundancy** Load Balancing SLAs with external/internal Providers

Methods to achieve Higher Security Service Objectives

higher services

Data authenticity	**Certificates** for the website of the class schedule Keyed-Hash Message Authentication Code (HMAC)
Non-repudiation	Message Authentication Codes and Digital Signatures Auditing and **Logging** (e.g. Time-stamp and verify registrations)
Access control	Definition of roles, attributes or **rules**
Accountability	Auditing and **Logging** Cross-department collaboration Cybersecurity Awareness **Training** on e.g. legal standards

IMKM Lecture 10: Information Security, Privacy and Risk Management

Outline

1. Information Security
2. **Privacy**
3. Risk Management
    1. Fundamentals
    2. Risk Management Process
    3. IT Projects

Learning Objectives

- *You understand information security.*
- *You understand the IT security objectives and can distinguish them.*
- *You understand privacy and can discuss the key changes of the GDPR.*
- *You understand and can discuss risk, its categories, and its two strategies.*
- *You can apply the risk management process and know examples for its steps.*
- *You understand and can apply the three characteristics of IT project risks.*

Privacy

Privacy is best understood through a notion of "**contextual integrity**", where it is not the sharing of information in general a problem, rather it is the **sharing of information outside of socially agreed contextual boundaries.** [1]

Distinction can be made between [2]

(1) **Decision** privacy*: Privacy about person's **decisions** and choices about his private actions. It protects, for example, persons from external **interference** with decisions.*

(2) **Information** privacy: *the ability of a person to control, edit, manage and delete **information about themselves** and to decide how and to what extent such information is communicated to others.*

Example: What if your Fitbit knew exactly what to say on a particular day to motivate you to get off the couch and run a 5K? → It could influence your decisions

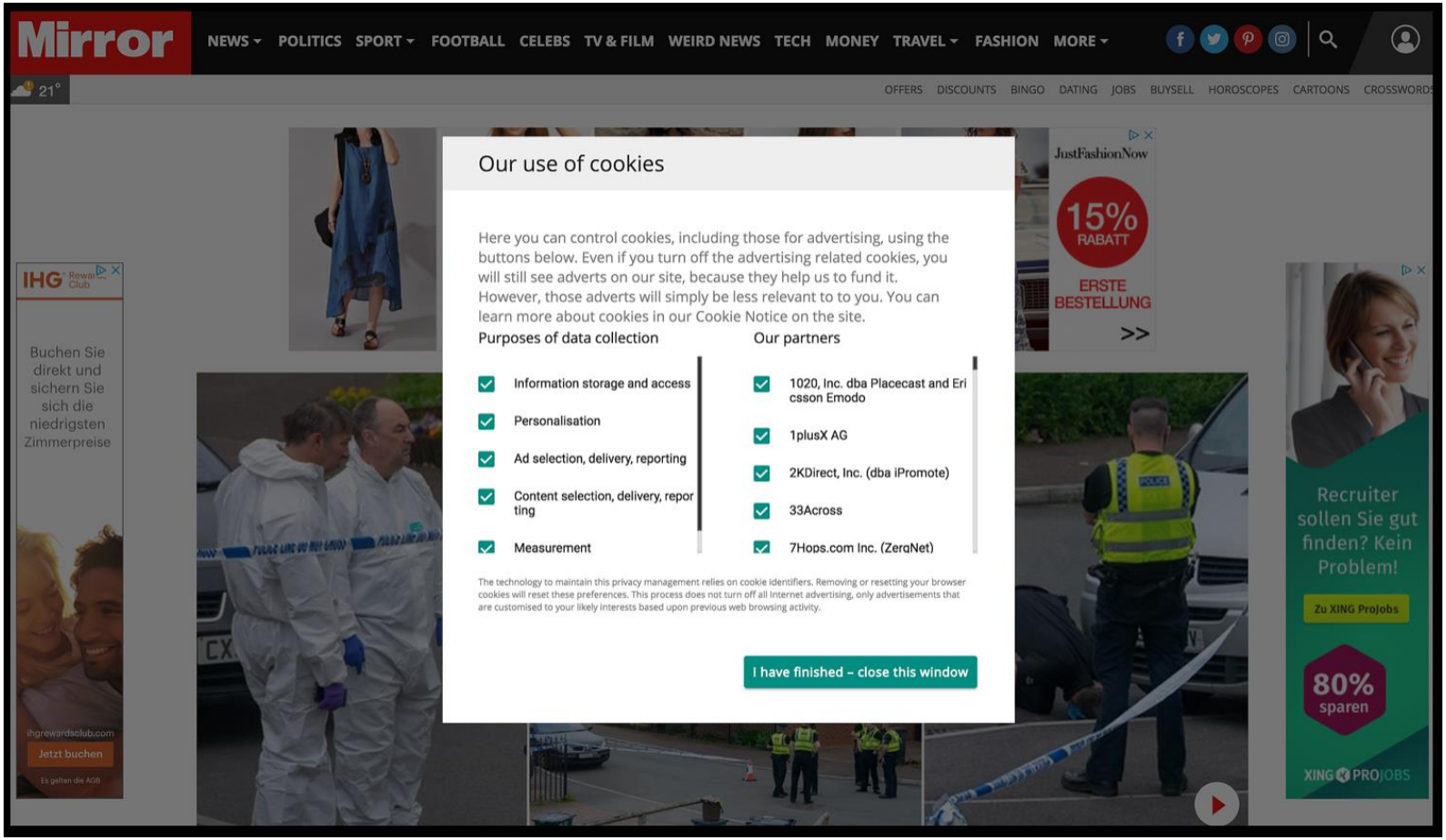
[1] Nissenbaum (2004) [2] DeCew (1997)

Impacts and issues by certain threads

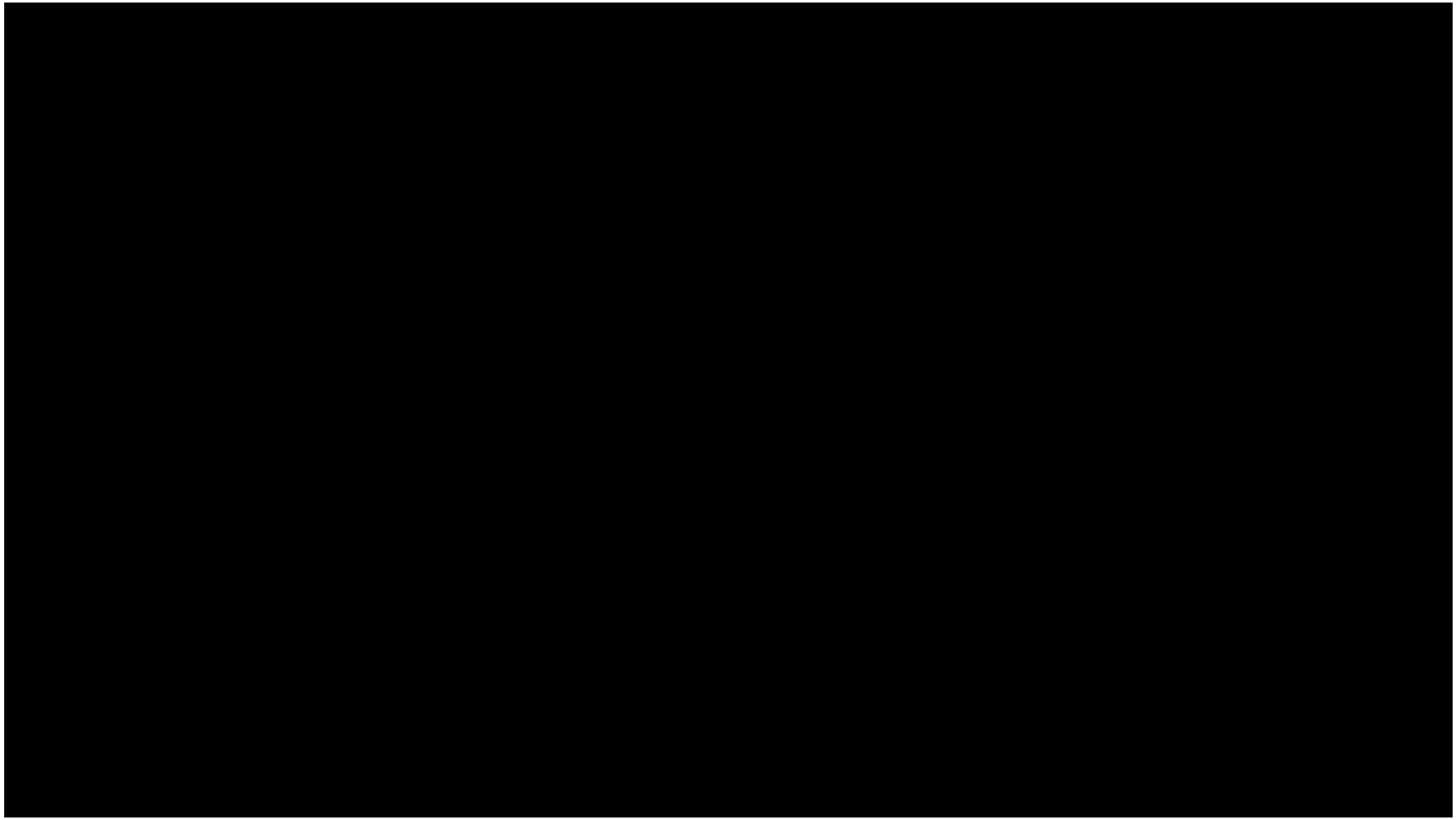
As data can be stored and processed in the “Exabyte” level and more connectivity and interaction is possible, information is ubiquitous. This triggers different threats

Internet	Big Data	Social Media	Internet of Things
• Use of cookies to store online behavior • Cloud Computing – Access to data and usage statistics by vendors – Ambiguities regarding legal issues (applicability of laws, demand for data access)	• Used to profile users, identify patterns and predict interests and behavior • Potential to result in future discrimination and inequalities	• Steering users' behavior of sharing • E.g., through ‘Like’ button • “Fake” news versus user-generated content • Privacy features only as built-in ‘add-ons’ rather than ‘by design’ • Exchange personal data for the benefits of using services	• Automatic adaptation of the environment to the user • Usage of explicit preferences and implicit observations • User autonomy is a central theme in considering the privacy implications of such devices.

What is GDPR?


Mirror
NEWS
POLITICS
SPORT
FOOTBALL
CELEBS
TV & FILM
WEIRD NEWS
TECH
MONEY
TRAVEL
FASHION
MORE
OFFERS
DISCOUNTS
BINGO
DATING
JOBS
BUYSELL
HOROSCOPES
CARTOONS
Our use of cookies
Here you can control cookies, including those for advertising, using the buttons below. Even if you turn off the advertising related cookies, you will still see adverts on our site, because they help us to fund it. However, those adverts will simply be less relevant to to you. You can learn more about cookies in our Cookie Notice on the site.
Purposes of data collection
Information storage and access
Personalisation
Ad selection, delivery, reporting
Content selection, delivery, reporting
Measurement
Our partners
1020, Inc. dba Placecast and Ericsson Emodo
1plusX AG
2KDirect, Inc. (dba iPromote)
33Across
7Hops.com Inc. (ZerqNet)
The technology to maintain this privacy management relies on cookie identifiers. Removing or resetting your browser cookies will reset these preferences. This process does not turn off all Internet advertising, only advertisements that are customised to your likely interests based upon previous web browsing activity.
I have finished – close this window
JustFashionNow
15% RABATT
ERSTE BESTELLUNG
IHG
Buchen Sie direkt und sichern Sie sich die niedrigsten Zimmerpreise
Jetzt buchen
Recruiter sollen Sie gut finden? Kein Problem!
Zu XING ProJobs
80% sparen
XING PROJOBS

What is GDPR?



EU General Data Protection Regulation (GDPR)

- Applied EU-wide since 25 May 2018 in national data protection laws (e.g. the BDSG)
- Aims at giving control over personal data back to all EU citizens

Key Changes

1. Increased Territorial Scope (extra-territorial applicability)
2. Penalties
3. Consent
4. Breach Notification
5. Right to Access
6. Right to be Forgotten
7. Data Portability
8. Privacy by Design
9. Data Protection Officers

Examples

- Social media data
- Search engine usage data
- Health data
- Genome data
- Personal mobility data

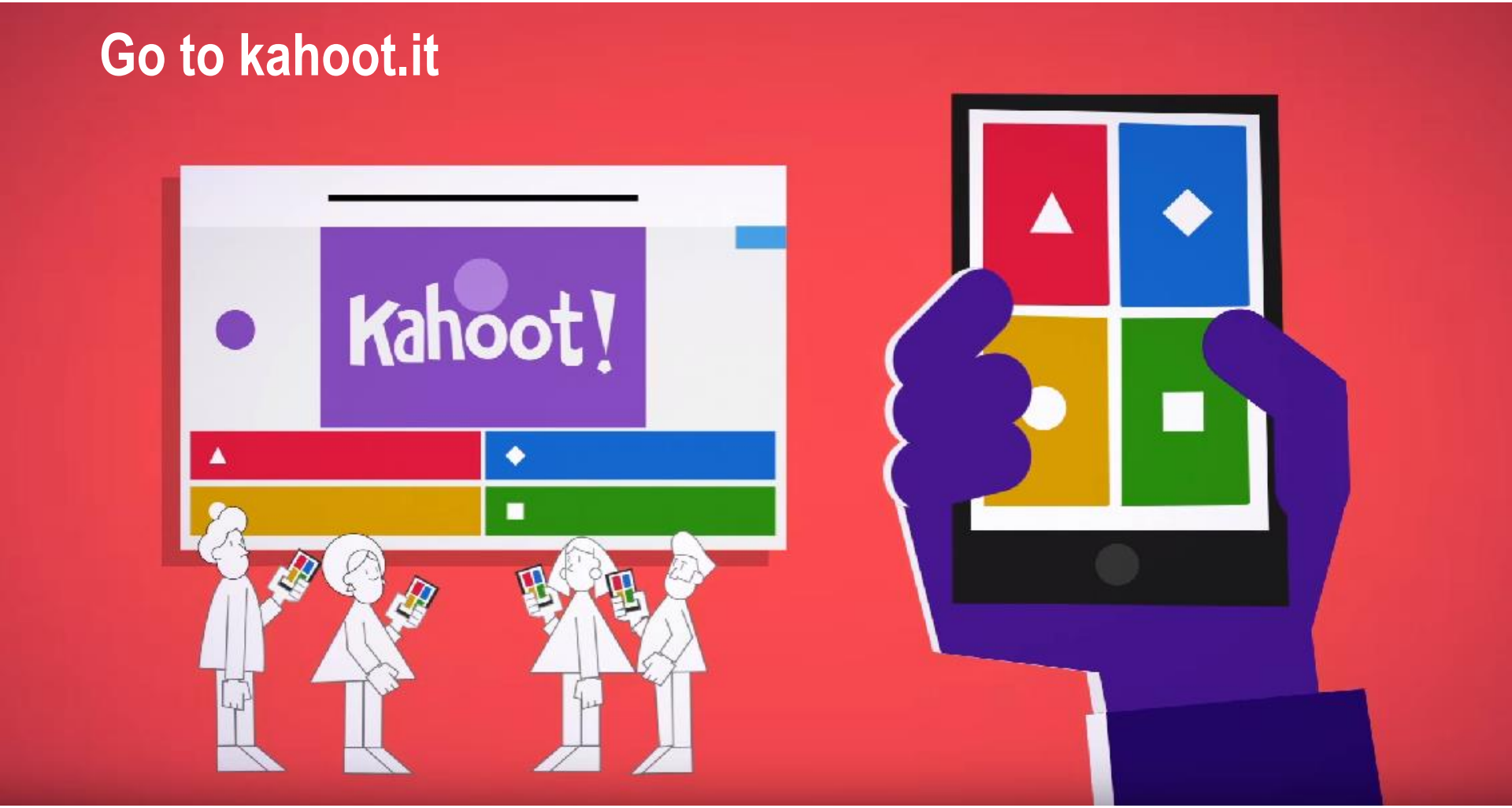
www.eugdpr.org

Data Protection Law in Germany

- EU General Data Protection Regulation (GDPR) implemented in the
- Federal Data Protection Law (Bundesdatenschutzgesetz, BDSG)
- State specific Data Protection Laws (e.g. BayDSG)
- Area specific regulations:
  - Code of Social Law
  - Telecommunications Act
  - Telemedia Act
  - …

Quiz Time!

Go to kahoot.it



IMKM Lecture 10: Information Security, Privacy and Risk Management

Outline

1. Information Security
2. Privacy
3. **Risk Management**
   1. Fundamentals
   2. Risk Management Process
   3. IT Projects

Learning Objectives

- *You understand information security.*
- *You understand the IT security objectives and can distinguish them.*
- *You understand privacy and can discuss the key changes of the GDPR.*
- *You understand and can discuss risk, its categories, and its two strategies.*
- *You can apply the risk management process and know examples for its steps.*
- *You understand and can apply the three characteristics of IT project risks.*

Risk Management

„When anyone asks me how I can best describe my experiences of nearly fourty years at sea, I merely say uneventful. I have never been in an accident of any sort worth speaking about ..... I never saw a wreck and have never been wrecked, nor was I ever in any predicament that threatend to end in disaster of any sort.“

Edward J. Smith, Captain of the Titanic about his experience as captain before Titanic‘s maiden voyage

The Issue of Risk

- **Risk is neither good or bad – it is just a fact**
- Some projects involve more risks than others
- Organizations should be prepared to invest in **high risk projects** only when the return is high BUT don't place all your assets in high risk projects

But:

What is an **IT risk**?

How can we become the **trusted advisor** on choosing the **IT risks worth taking**?

Image: www.mypharmacare.ca

What is an IT risk?

- **Risk** is the probability of an adverse future event multiplied by its magnitude.
- Risk Exposure
  RE = $p_{\text{adverse future event}}$ * magnitude of adverse future event
- **Security** is the absence of unbearable risks (DIN 2002)
- Risk Reduction Leverage
  RRL = $(RE_{\text{before}} - RE_{\text{after}})$ / cost of intervention

Risk Categorization

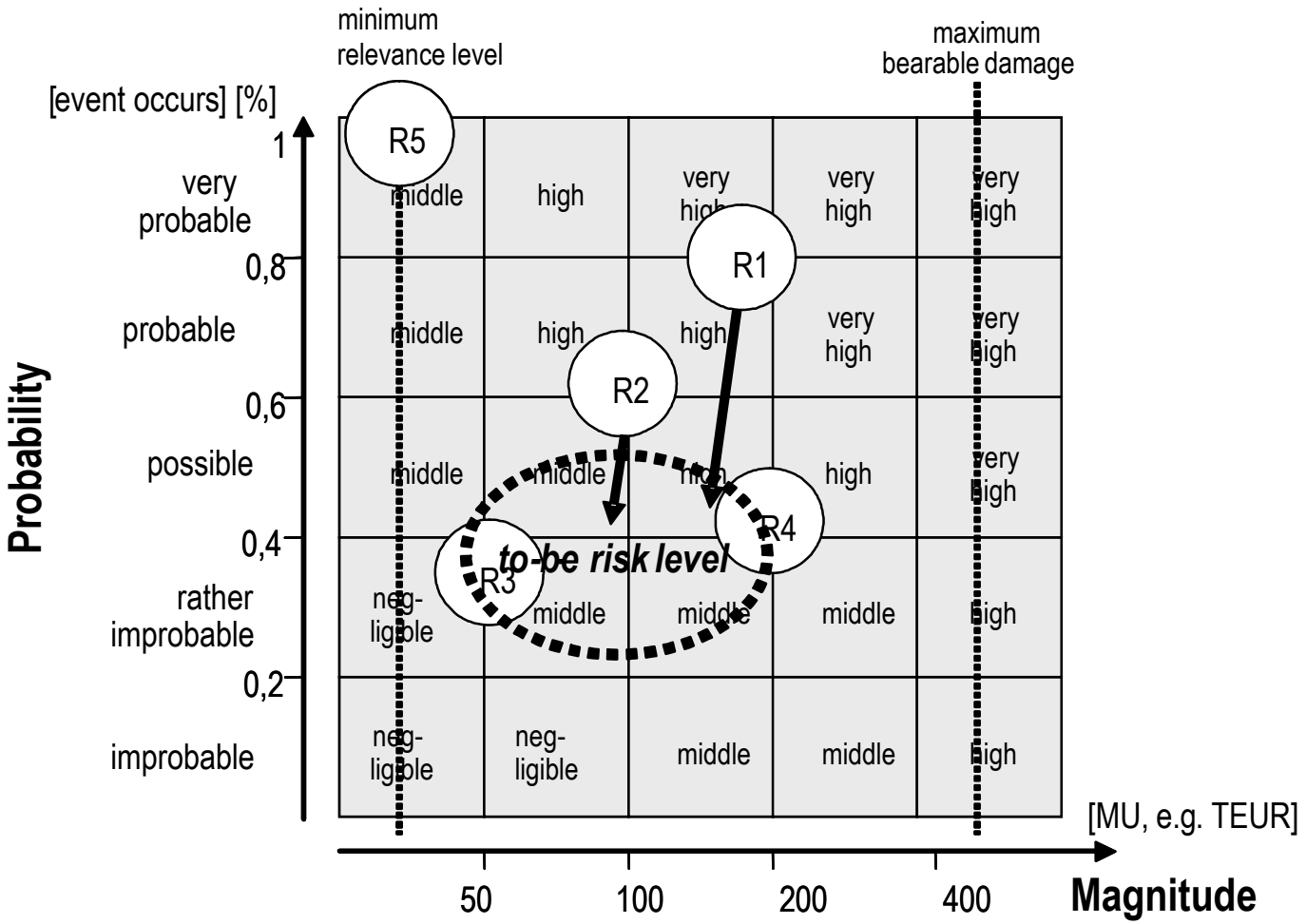
- **Known risks**
  - Those risks that can be uncovered after careful evaluation of the project plan, the business and technical environment in which the project is being developed, and other reliable information sources (e.g., unrealistic delivery date)
- **Predictable risks**
  - Those risks that are extrapolated from past project experience (e.g., past turnover)
- **Unpredictable risks**
  - Those risks that can and do occur, but are extremely difficult to identify in advance (e.g., zero-day attack)

Reactive vs. Proactive Risk Strategies

- **Reactive** risk strategies
  - "Don't worry, I'll think of something"
  - The majority of software teams and managers rely on this approach
  - Nothing is done about risks until something goes wrong
    - The team then flies into action in an attempt to correct the problem rapidly (**fire fighting**)
  - **Crisis management** is the choice of management techniques

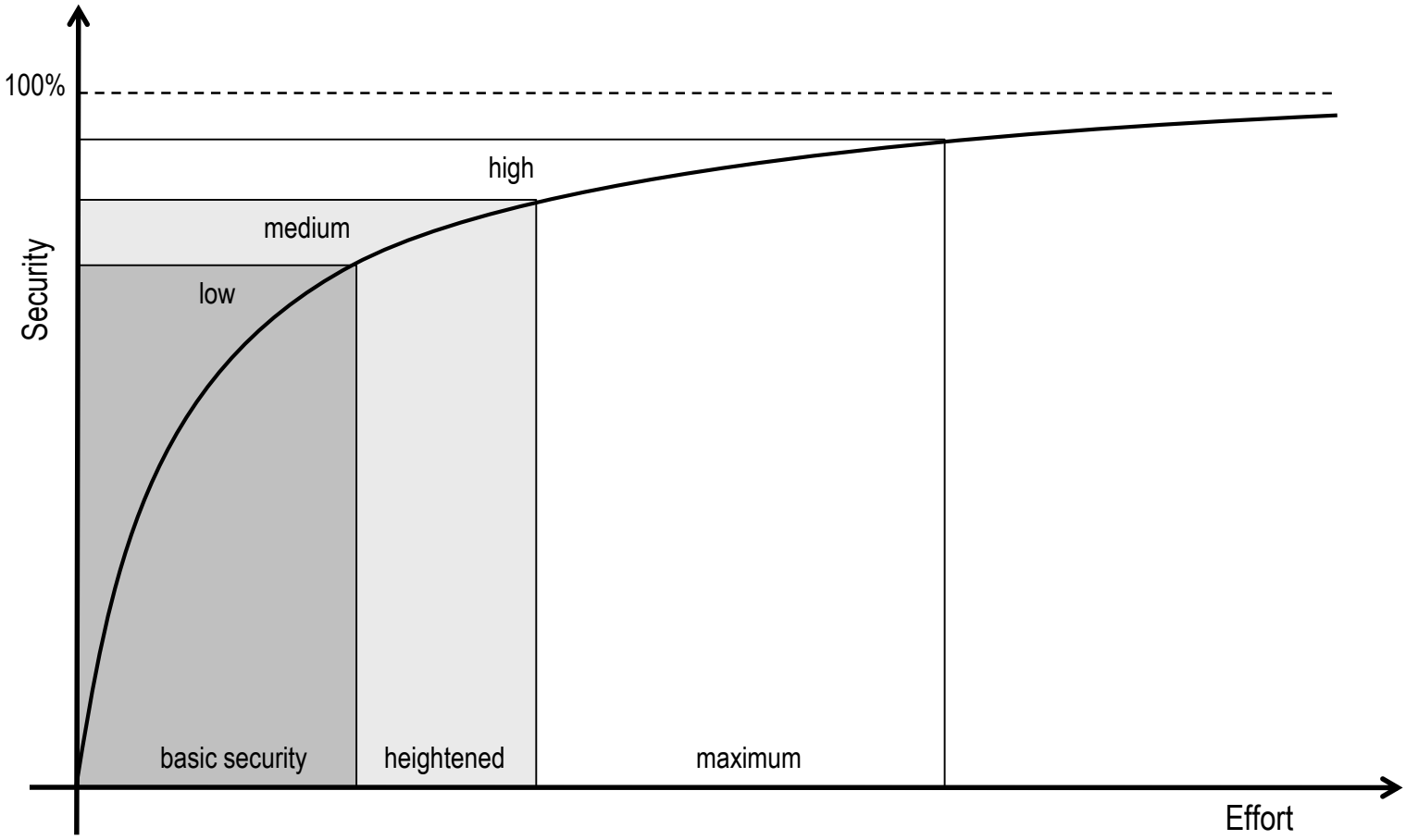
- **Proactive** risk strategies
  - Steps for risk management are followed
  - Primary objective:
    - **avoid risk** and
    - have a **contingency plan** in place to handle unavoidable risks in a controlled and effective manner

What is the right balance?



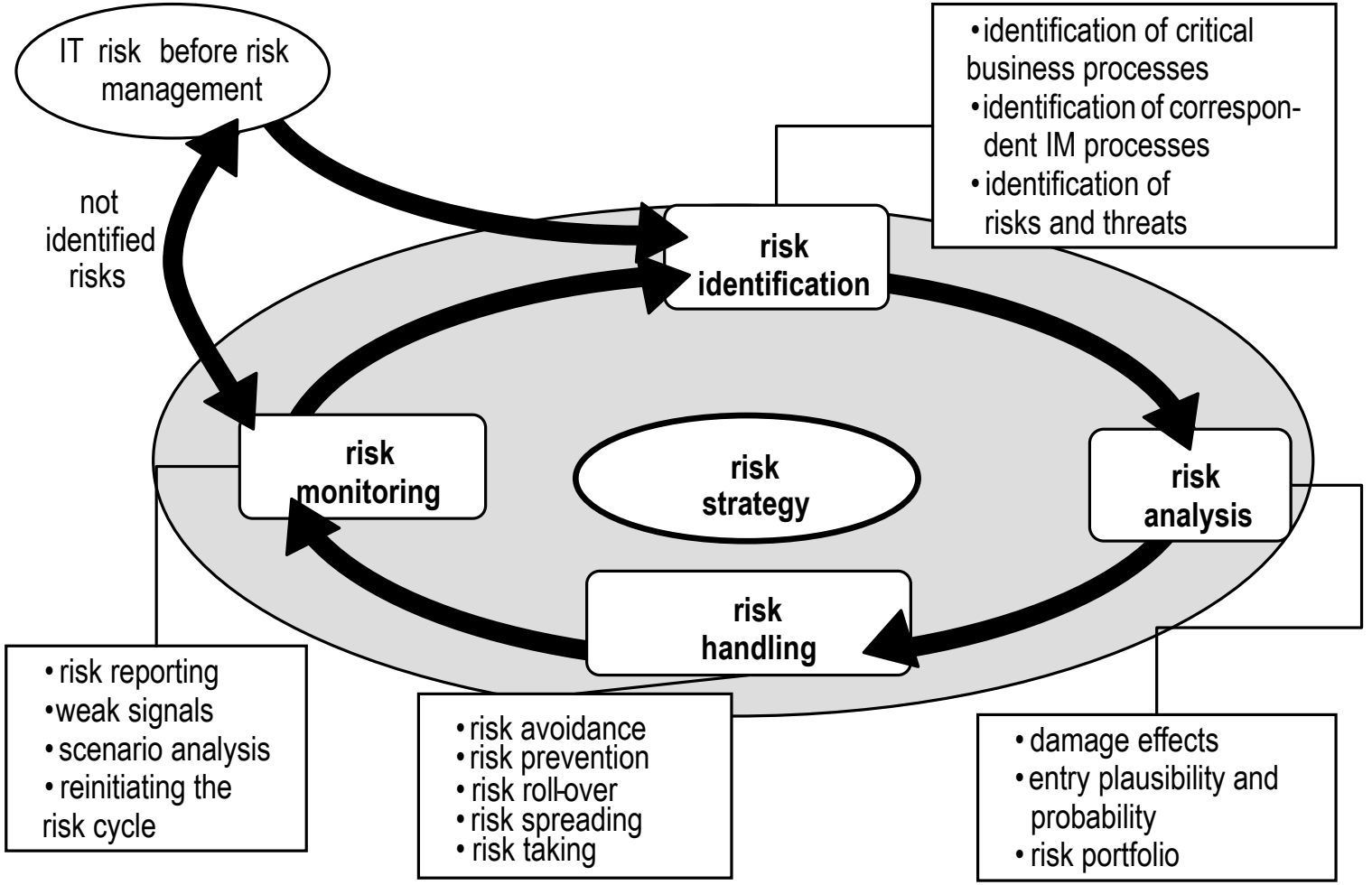
Source: Adapted from Junginger (2004, p. 281)

Risk Management for Security: Pareto at work…



Source: Krcmar (2015), p.525

Risk Management Process within Information Mgt



Krcmar (2015), p. 532

Risk Identification: Objectives and Tools

Risk Identification…

- …transfers uncertainties in a set of clearly defined risks

- …makes use of tools such as
  - expert interviews
  - brainstorming
  - analogies
  - risk registers

Example for Risk Identification: Risk Registers

Table 2. Full list of risk factors

1. Organization
   - 1.1 Lack of top management commitment to the project
   - 1.2 Change in ownership or senior management during the process of development
   - 1.3 Mismatch between organization culture and required business process changes needed for new system
   - 1.4 Resources shifted away from the project because of changes in organizational priorities
   - 1.5 Projects started for political reasons that carry no clear business value
   - 1.6 Failure to get project plan approval from all parties
   - 1.7 Project implementation has major effect on organizational structure
   - 1.8 Project implementation has major effect on business process
2. Requirement
   - 2.1 Incorrect system requirements
   - 2.2 Continually changing scope or syste
   - 2.3 Unclear/misunderstood requirement
   - 2.4 New and/or unfamiliar subject matte requirements definition
   - 2.5 Users and developers ignore busine
   - 2.6 Conflicting in defining system requir
   - 2.7 Users lack understanding of system
   - 2.8 Undefined project success criteria
   - 2.9 Difficulty in defining the inputs and
   - 2.10 System requirements not adequate
3. User
   - 3.1 Lack of cooperation and responsibil
   - 3.2 Users unrealistic expectations
   - 3.3 Excessive use of outside consultant
   - 3.4 Users resistant to change
   - 3.5 Users with negative attitudes towar
   - 3.6 Lack of adequate user participation
   - 3.7 Conflicts between users and develo
   - 3.8 Conflict between user departments
   - 3.9 Underfunding of maintenance by th
4. Technology
   - 4.1 Project involves new technology an
   - 4.2 Lack of effective development meth
   - 4.3 Large number of links to other syst
   - 4.4 High level of technical complexity
   - 4.5 Immature technology
5. Team
   - 5.1 Lack of commitment to the project among development team members
   - 5.2 Conflicts between team members in terms of characters, attitudes and conceptions
   - 5.3 Frequent turnover within the project team and shortfalls
   - 5.4 Team members not familiar with the task being automated
   - 5.5 Team members lack skills required by the project
   - 5.6 Inadequately trained development team members
6. Planning and control
   - 6.1 Project milestones not clearly defined
   - 6.2 Lack of effective project management methodology
   - 6.3 Poor project planning
   - 6.4 Inexperienced project manager
   - 6.5 Ineffective communications among different stakeholders
   - 6.6 Inadequate estimation of required resources and budget
   - 6.7 Inadequate estimation of project schedule
   - 6.8 Poor control in tracking project
   - 6.9 Not managing change properly
   - 6.10 Improper definition of roles and responsibilities
   - 6.11 Poor risk management
   - 6.12 Choosing the wrong development strategy
   - 6.13 Lack of control over consultants, vendors and subcontractors
7. Market and competition
   - 7.1 Change of market needs that the expected benefits vanish
   - 7.2 Competitors take unanticipated preemptive actions or simply respond by developing a better application
   - 7.3 Unanticipated favorable or unfavorable reaction from regulatory bodies, customers, vendors and business partners that can affect the application
   - 7.4 The application could become obsolete with the introduction of a new superior technology, service or product
   - 7.5 External dependencies not met
   - 7.6 Multi-vendor projects complicate dependencies: Integration of packages from multiple vendors hampered by incompatibilities and lack of cooperation between vendors

Liu et al. (2010)

Risk Analysis: Objectives and Tools

Risk Analysis…

- …assesses the identified risks regarding their
  - **probability** of occurrence and
  - (negative) **impact** on the organization/project

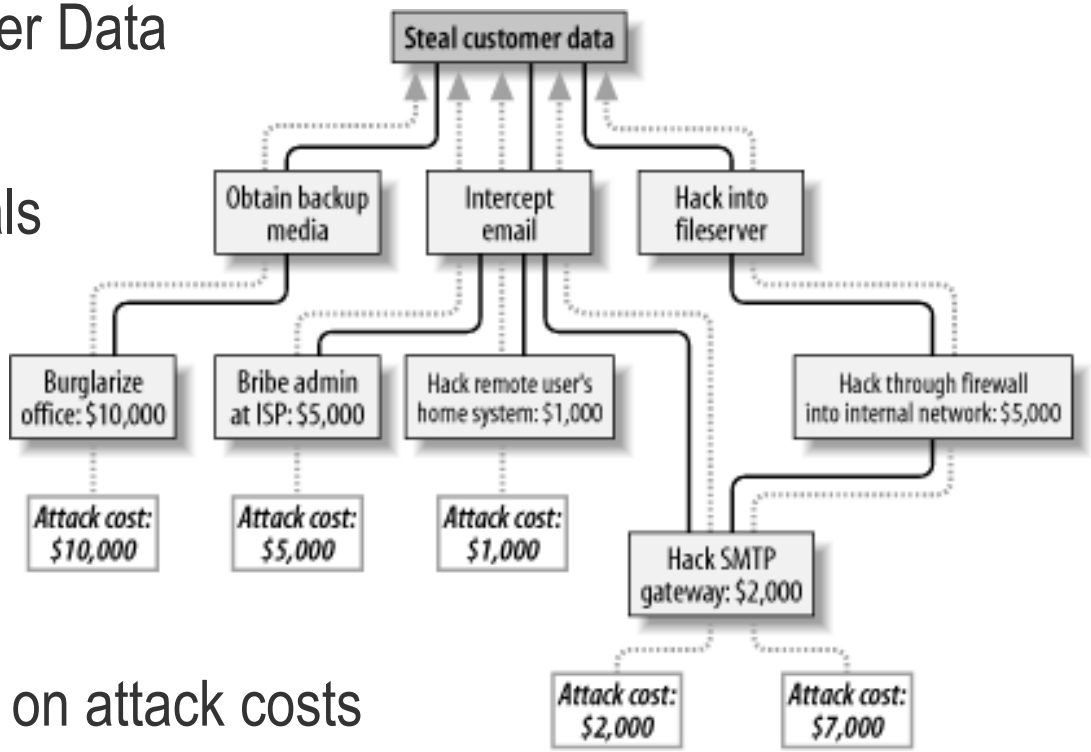
- …makes use of tools such as
  - expert interviews
  - cause-and-effect analysis
  - decision trees
  - risk prioritization
  - Threat tree

Example for Risk Analysis: Threat Trees

Threat trees summarize potential threats in a top-down view.

- Example: Stealing Customer Data

- Leaves are threatened goals
- Division in sub-trees
  - AND or OR relations



Goal: find weakest link based on attack costs

Schneier (1999); Eckert (2009)

Risk Handling: Objectives and Tools

Risk Handling…

- …evaluates, plans, and executes **strategies** for the analyzed risks

- …makes use of tools such as
  - risk strategy lists
  - decision tables
  - decision trees
  - cause-and-effect analysis

Example for Risk Handling: Risk Strategy Lists with Best Practices

1. Avoiding Poor Estimating and/or Scheduling
2. Avoiding Ineffective Stakeholder Management
3. Avoiding Insufficient Risk Management
4. Avoiding Insufficient Planning
5. Avoiding Shortchanging Quality Assurance
6. Avoiding Weak Personnel and/or Team Issues
7. Avoiding Insufficient Project Sponsorship

Nelson (2007)

Risk Monitoring: Objectives and Tools

Risk Monitoring…

- …**tracks** the evolution of risks over time

- …makes use of tools such as
  - status reports
  - to-be analyses
  - risk visualizations

Example for Risk Monitoring: Visualizations to track the Volatility of Risks

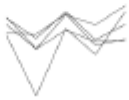
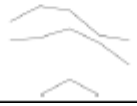
C	Risks	Visualization	Temporal Characteristics
1	Complex System Architecture Customer Financial Obligations Solution Uncertainties		Remain constant initially Gain importance towards project end
2	Low Project Priority Implementation Partner Unknown Ongoing Escalation Events Unclear Critical Success Factors Unrealistic Budget		
3	Inexperienced Project Lead No Quality Assurance/Risk Management Post Go Live Approach Not Defined Risk Tolerance		
4	Inadequate Technical Infrastructure Internal and External Decision Makers Hardware Partner Not Involved Weak Business Commitment		
5	Development Methodology High Customer Visibility Undocumented Third Party Services		
6	Core Development Dependencies Customer Inability to Undertake Project Functionality Gaps		Lose importance before project end Re-gain importance towards project end
7	Implementation and Dev. Interdependencies Incomplete Contract Requirements No Comparable Installations No Ramp-Up No Risk Sharing Agreements Production Downtime Impact Unclear Customer Objectives Unclear Governance Model		Peak just after project start Lose importance thereafter
8	Customer Expectations Expected Performance Issues High Number of Interfaces Industry Specific Solutions No Change Management Approach Requirements Not Understood		Lose importance initially Re-gain importance towards project end
9	Complex Data Conversion High Impact on Processes Non-Conducive Political Environment Non-T&M Payment Terms Unclear Roles		Steadily lose importance

Table 3. Derived Risk Clusters

Hoerrmann et al. (2011)

Risk analysis in IT projects: Three characteristics that influence project risks

1. **Size of project — in terms of workers/years of effort**
   - This is a simple but important risk dimension measurable in worker/years.
   - The interpersonal communications task alone increases exponentially with the size of the team.
2. **Degree of company-relative technology experience**
   - There is an education/familiarization cost associated with new or untried:
     - tools
     - concepts
     - hardware features
     - suppliers of hardware or software
     - communications standards
   - Expect unexpected (unplanned) interface problems.

Applegate et al. (1999)

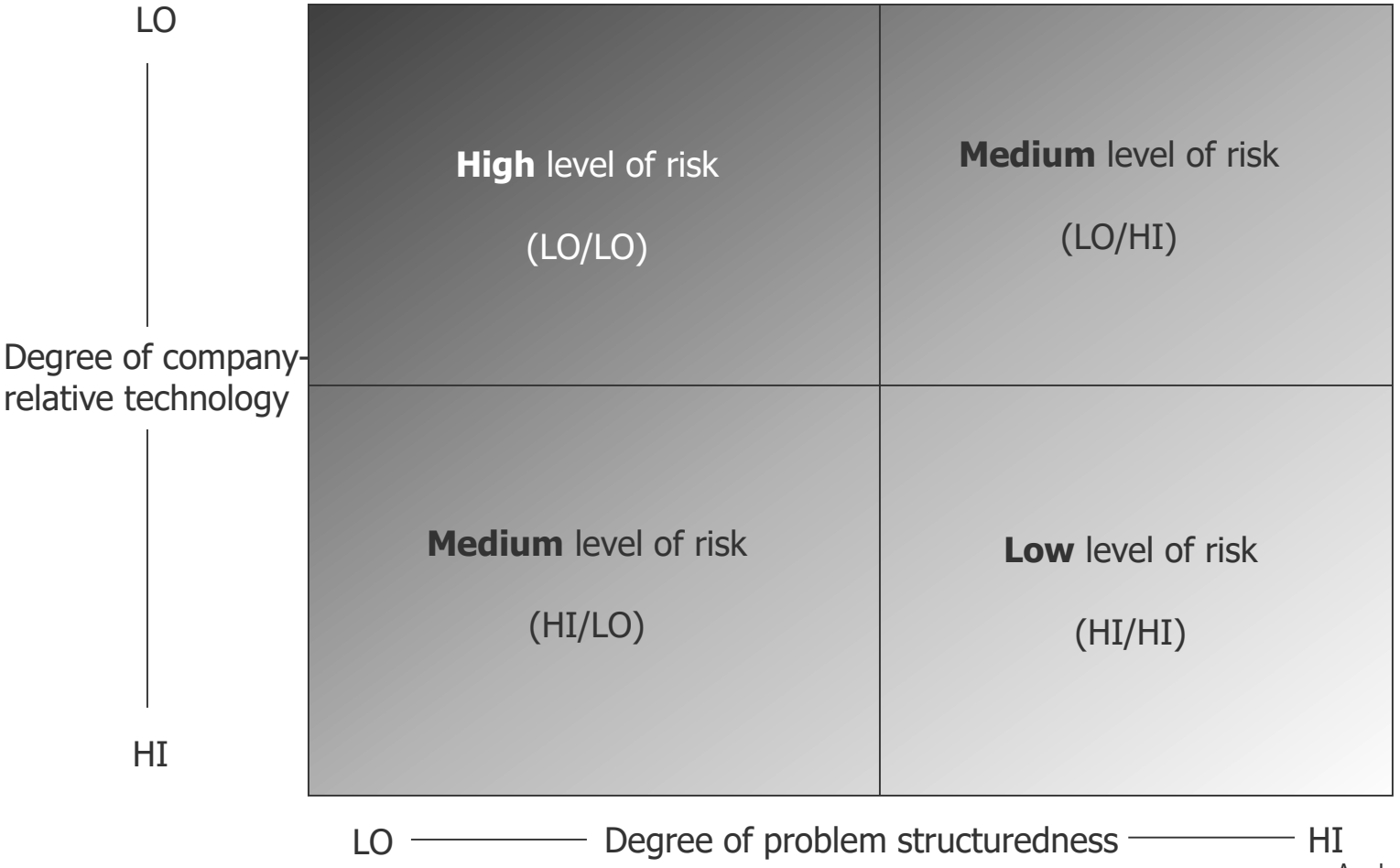
Risk analysis in IT projects: Three characteristics that influence project risks

3. Degree of inherent structure

- How well-defined are the project's outputs?
- How well does the implementation team understand what has been requested?
- Have they built a system like this before (plan to throw one away…)

Applegate et al. (1999)

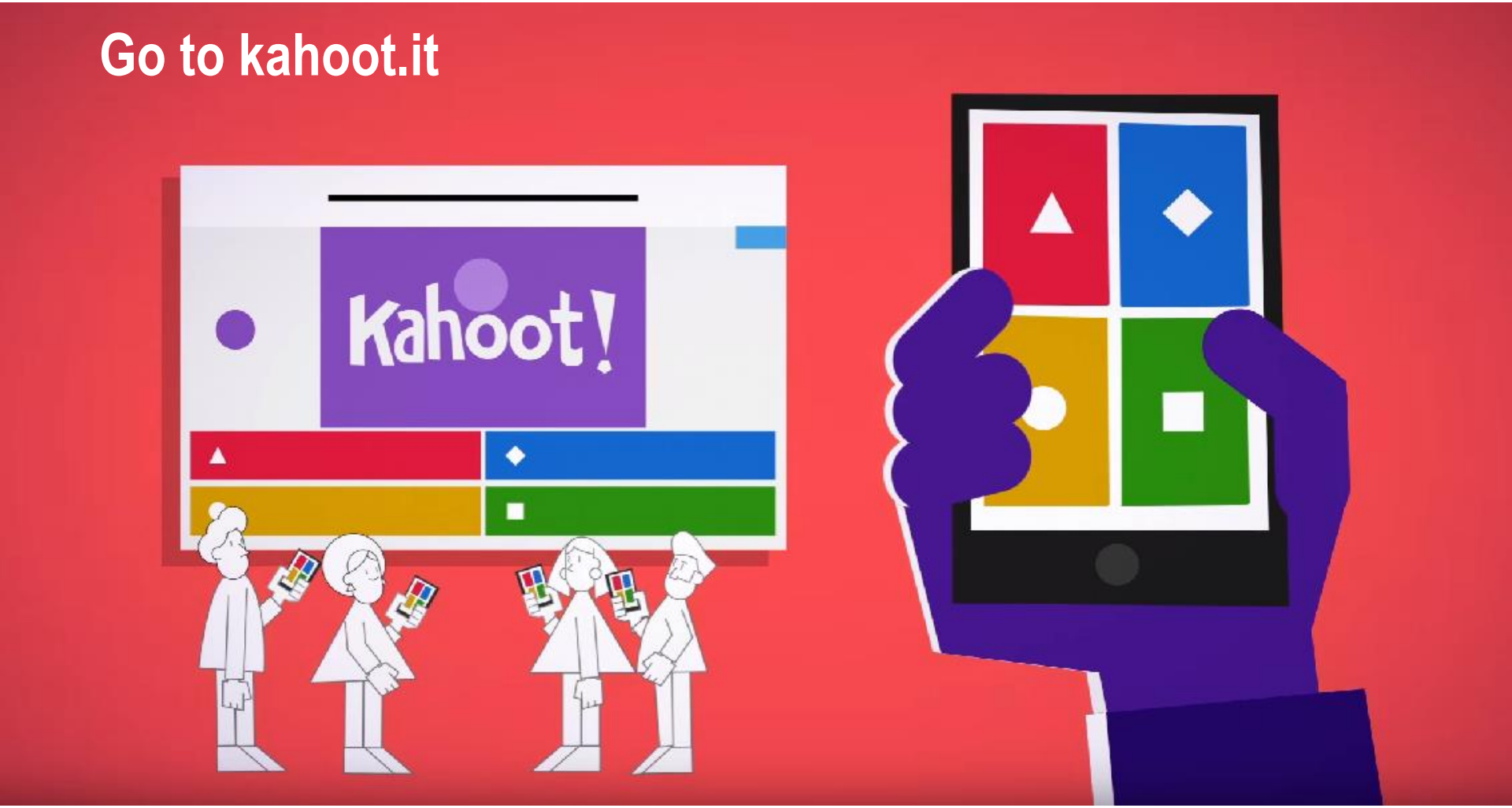
Risk analysis in IT projects: Understanding the Degree of IT Project Risk



Applegate et al. (1999)

Quiz Time!

Go to kahoot.it



Core Literature: Krcmar, Informationsmanagement (2015)

1. Einleitung (pp.1-8)
2. Begriffe und Definitionen (pp.11-26)
3. Modellierung (pp. 31-78)
4. Aufgabe des Informationsmanagements: Informationsmanagement (pp. 85-109)
5. Aufgabe des Informationsmanagements: Management der Informationswirtschaft (pp. 113-165)
6. Aufgabe des Informationsmanagements: Management der Informationssysteme (pp. 173-302)
7. Aufgabe des Informationsmanagements: Management der Informations- und Kommunikationstechnik (pp. 315-385)
8. Führungsaufgaben des Informationsmanagements
   8.4 IT-Risikomanagement und Informationssicherheit (pp. 522-543)
9. Referenzmodelle des Informationsmanagements (pp. 601-630)
10. Einsatzfelder und Herausforderungen des Informationsmanagements (pp. 633-753)
11. Fallstudie „Rockhaus AG“ (pp. 767-783)

References

- Applegate, L. M., McFarlan, F. W., & Mckenney, J. L. (1999). Corporate Information Systems Management: The Challenge of Managing in an Information Age. Homewood, IL: Irwin McGraw-Hill.
- BSI. (2017). Guide to Basic Protection Based on IT-Grundschutz - 3 Steps to Information Security. Bonn.
- BSI. (2018). BSI-Standards. Retrieved from https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html
- DeCew, J. W. (1997). Pursuit of Privacy: Law, Ethics, and the Rise of Technology. Ithaca, NY: Cornell University Press.
- Eckert, C. (2009). IT-Sicherheit: Konzepte - Verfahren - Protokolle. Munich: Oldenbourg.
- Hoermann, S., Schermann, M., Aust, M., & Krcmar, H. (2014). Risk Profiles in Individual Software Development and Packaged Software Implementation Projects: A Delphi Study at a German-Based Financial Services Company. International Journal of Information Technology Project Management (IJITPM), 5(4), 1-23.
- Hoermann, S., Schermann, M., & Krcmar, H. (2011). When to Manage Risks in IS Projects: An Exploratory Analysis of Longitudinal Risk Reports. Wirtschaftsinformatik Proceedings 2011; 28.
- ISO/IEC (eds.) (2018): ISO/IEC 27000, version of February 2018, in https://www.iso.org/standard/73906.html
- Krcmar, H. (2015). Informationsmanagement. Berlin Heidelberg: Springer Gabler.
- Liu, S., Zhang, J., Keil, M., & Chen, T. (2010). Comparing Senior Executive and Project Manager Perceptions of IT Project Risk: A Chinese Delphi Study. Information Systems Journal, 20(4), 319-355.
- Nelson, R. R. (2007). IT Project Management: Infamous Failures, Classic Mistakes, and Best Practices. MIS Quarterly Executive, 6(2).
- Nissenbaum, H. (2004). Privacy as Contextual Integrity. Washington Law Review, 79, 101-139.
- PwC. (2018). Pulling Fraud out of the Shadows - Global Economic Crime and Fraud Survey 2018.
- Rao, U.; Nayak, U. (2014): The InfoSec Handbook, Berkeley 2014.
- Royal Society (1983). Risk Assessment / Report of a Royal Society Study Group. In. London: Royal Society.
- Schneier, B. (1999). Attack Trees - Modeling Security Threats. Dr. Dobb's Journal of Software Tools, 21(12), 21-29.