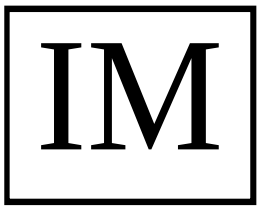



# Information Management and Knowledge Management (IMKM)

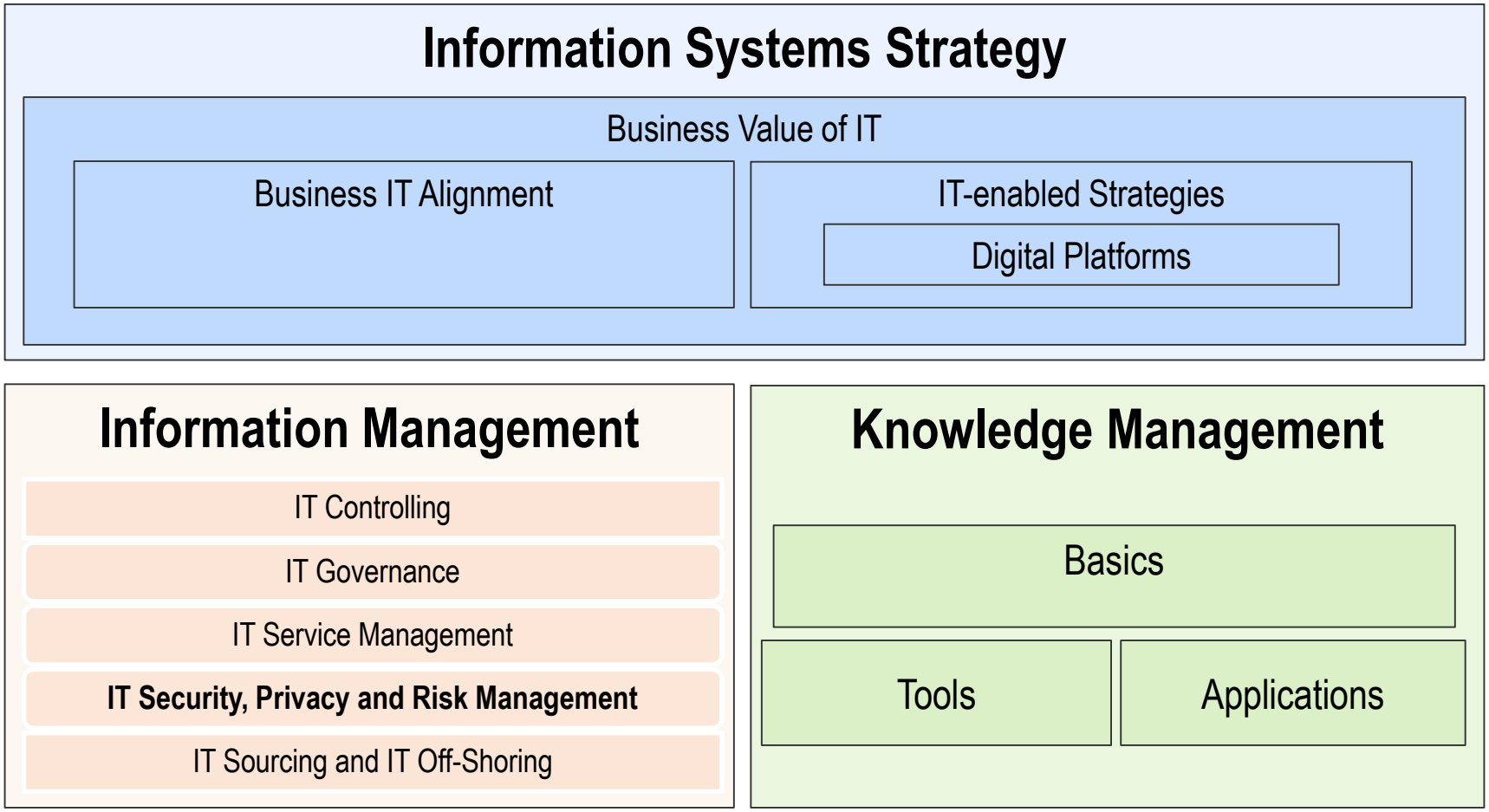
## Lecture 10

## *Information Security, Privacy and Risk Management*

TUM

Chair for Information Systems

# Lecture Schedule



# Lecture Schedule

| Date | No. | Topic/ Comment | |
|---|---|---|---|
| Friday, October 18, 2019 | 1 | Introduction and Fundamentals | |
| Friday, October 25, 2019 | 2 | Business Value of IS | Information Systems Strategy |
| Friday, November 1, 2019 | | *All Saints Day – No Lecture* | |
| Friday, November 8, 2019 | 3 | Business IT Alignment | |
| Friday, November 15, 2019 | 4 | IT-enabled Strategies | |
| Friday, November 22, 2019 | 5 | Digital Platforms (part 1) | |
| Friday, November 29, 2019 | 6 | Digital Platforms (part 2) | |
| Friday, December 6, 2019 | 7 | IT Controlling | Information Management |
| Friday, December 13, 2019 | 8 | IT Governance | |
| Friday, December 20, 2019 | 9 | IT Service Management | |
| **Friday, January 10, 2020** | **10** | **IT Security, Privacy and Risk Management** | |
| Friday, January 17, 2020 | 11 | IT Sourcing and IT Off-Shoring (Guest Lecture) | |
| Friday, January 24, 2020 | 12 | Basics and Tools of Knowledge Management | Knowledge Management |
| Friday, January 31, 2020 | 13 | Applications of Knowledge Management (Guest Lecture) | |
| Friday, February 7, 2020 | 14 | Q&A | |
| Thursday, February 13, 2020 | | **Exam** 10:30 am – 12:00 pm *(preliminary!)* | |
| Thursday, April 07, 2020 | | **Retake exam** 10:30 am – 12:00 pm *(preliminary!)* | |

# IMKM Lecture 10: Information Security, Privacy and Risk Management

## Outline

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

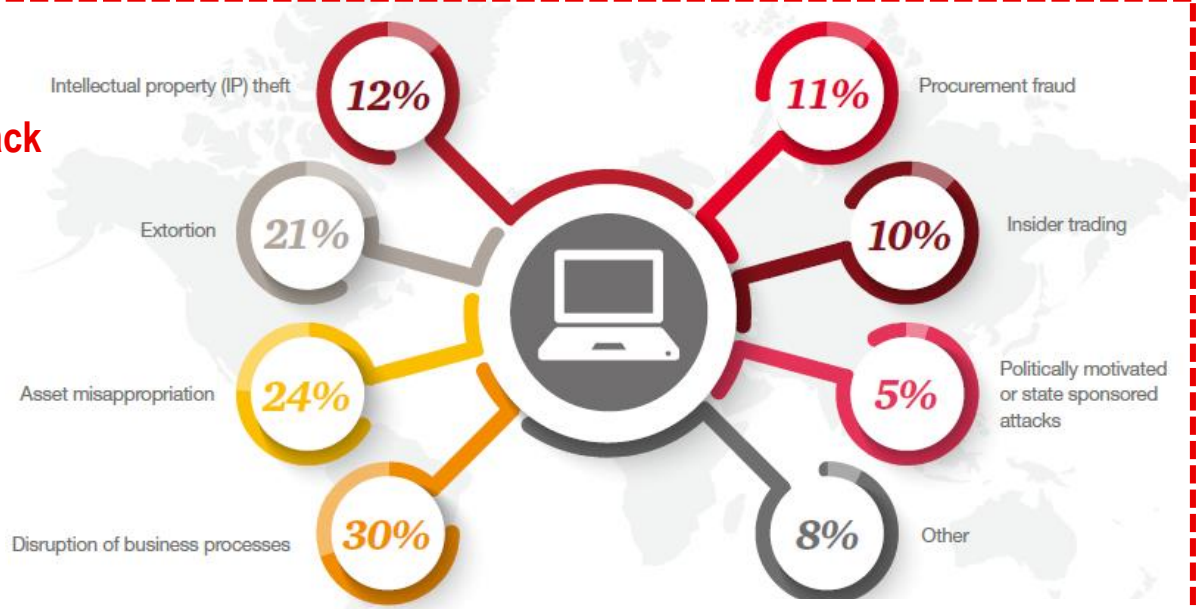
## Learning Objectives

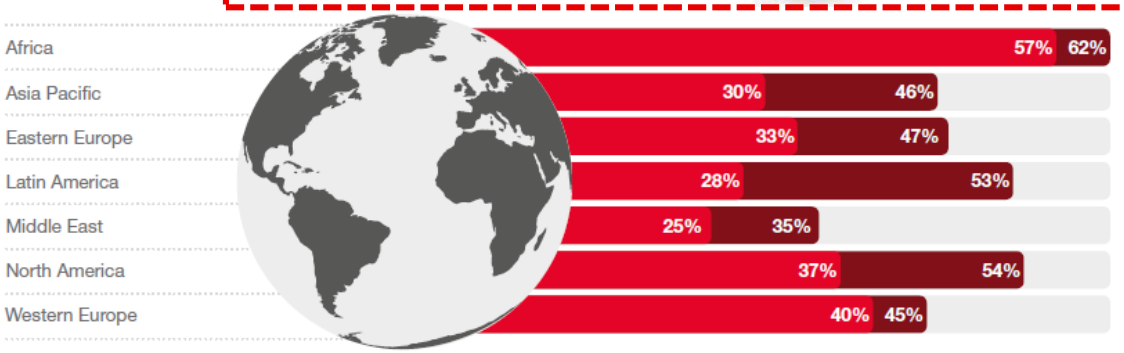
- *You know the basics and objectives of information security.*
- *You are able to discuss impacts of IT developments and the legal foundations of privacy.*
- *You are familiar with risks within information management and are able to outline and apply a risk management process.*
- *You are able to apply risk management methods.*

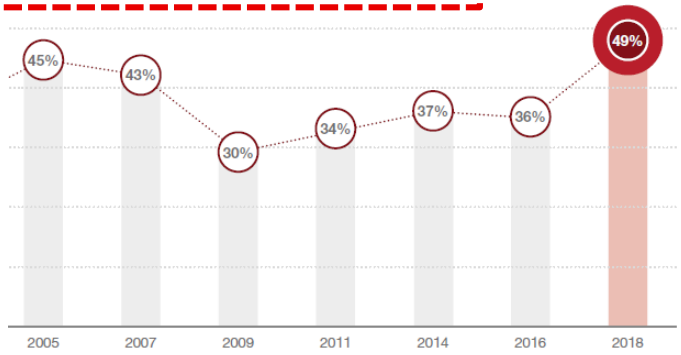
FAZ (2019)

# 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.

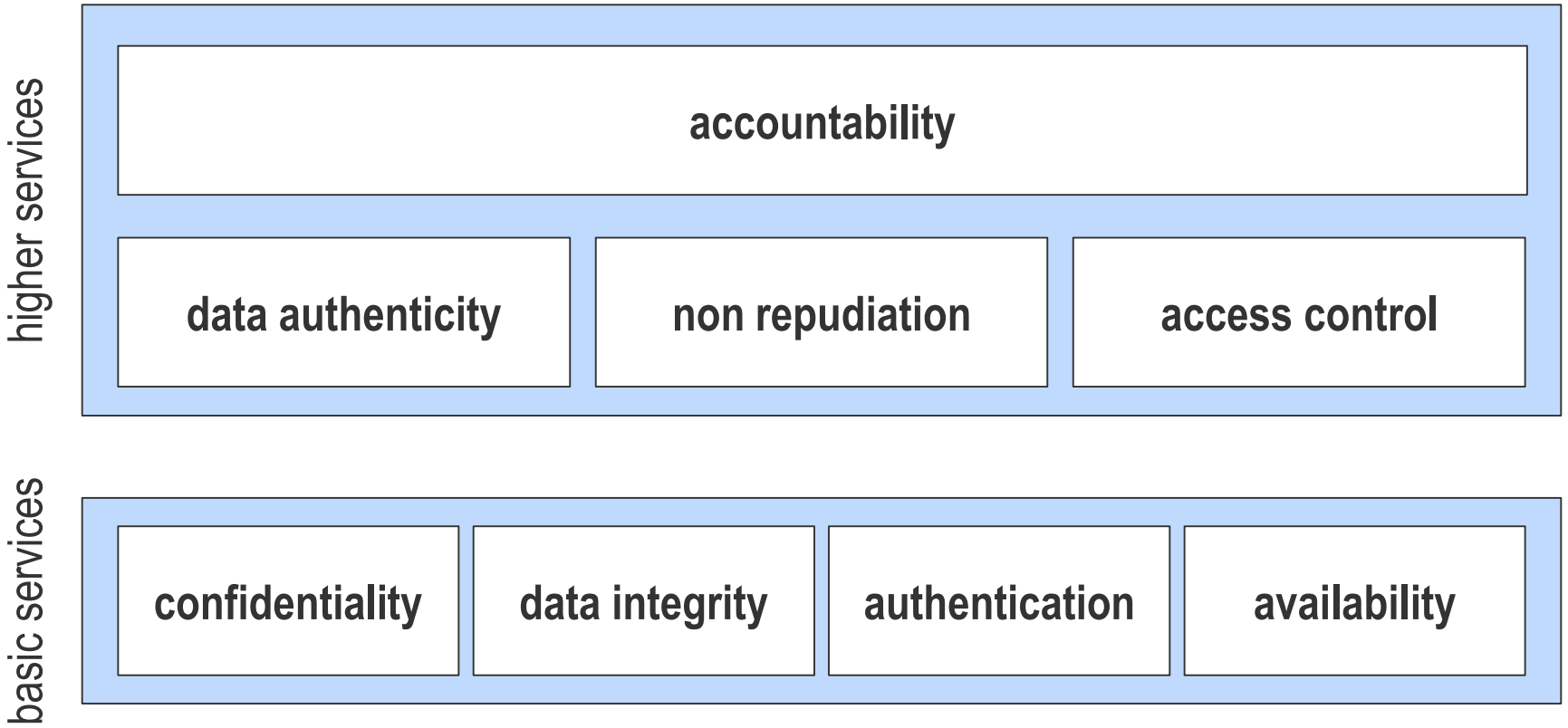
  ***Information security*** *is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical).* [1]

- 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)

# Methods to achieve Basic Security Service Objectives

- **Confidentiality**
  - Encryption (symmetric vs. asymmetric)
- **Integrity**
  - Hash-Functions
- **Authentication**
  - Knowledge of a secret (e.g.: password)
  - Possession of a certain object (e.g.: chip card)
  - Human characteristics (e.g.: finger print)
- **Availability**
  - Redundancy

# The Role of CISO

- Adopt a '**Service Provider**' approach
  - Facilitators who help achieve business goals in a more secure manner
- Lead and drive engagement with the board
  - Translate the complex world of information security and information risk into easily understandable issues and solutions
- Understand all the stakeholders, not just internal ones
  - Regulatory bodies, audit committees, etc.
- Be clear in expressing what outcomes that need to be achieved

Source: http://www.cio.com/article/2385369/it-organization/cisos-must-engage-the-board-about-information-security.html

# Creating a Culture of Security Awareness at Work

"A shift in corporate culture toward an **environment that values data privacy and security** is imperative..... Focus on changing people and **changing behaviors** toward the belief that **protecting company data is everyone's responsibility**."

*-- Larry Ponemon, Chairman and Founder of the Ponemon Institute*

- Increasing awareness of security issues is the most cost-effective control that an organization can implement
- Developing a comprehensive ***Security Awareness*** program
  - Security Awareness should be an ongoing and engaging exercise
  - Seen not only as a part of a compliance or audit initiative, but rather a lasting behavioral change

Source: https://securityintelligence.com/top-five-tips-for-creating-a-culture-of-security-awareness-at-work/

# Creating a Culture of Security Awareness at Work

- **Find the motivation**
  - Finding ways of sparking the emotional interest of employees
  - Raising awareness of security issues and concerns in a wider context
- **Gamification**
  - Using gamification techniques for personnel in security operations centers
  - Creating an air of healthy competition
- **Form Security Awareness Allies**
  - Getting other departments (beyond the Security team) involved
- **Public Recognition**
  - Making employees feel valued can be done via the intranet, newsletters, internal marketing materials and general recognition from management
- **Keep It Simple and Aligned to the Business**
  - Focus on specific incremental goals rather than trying to be all-encompassing
  - Identify the behaviors the organization wants to promote and align this to business results

Source: https://securityintelligence.com/top-five-tips-for-creating-a-culture-of-security-awareness-at-work/

# IMKM Lecture 10: Information Security, Privacy and Risk Management

## Outline

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

## Learning Objectives

- *You know the basics and objectives of information security.*
- *You are able to discuss impacts of IT developments and the legal foundations of privacy.*
- *You are familiar with risks within information management and are able to outline and apply a risk management process.*
- *You are able to apply risk management methods.*

# Privacy


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

**Distinction can be made between (1) *constitutional (*or decisional*) privacy* and (2) *tort (*or informational*) privacy* [2]**

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

# Impacts and issues by certain threads

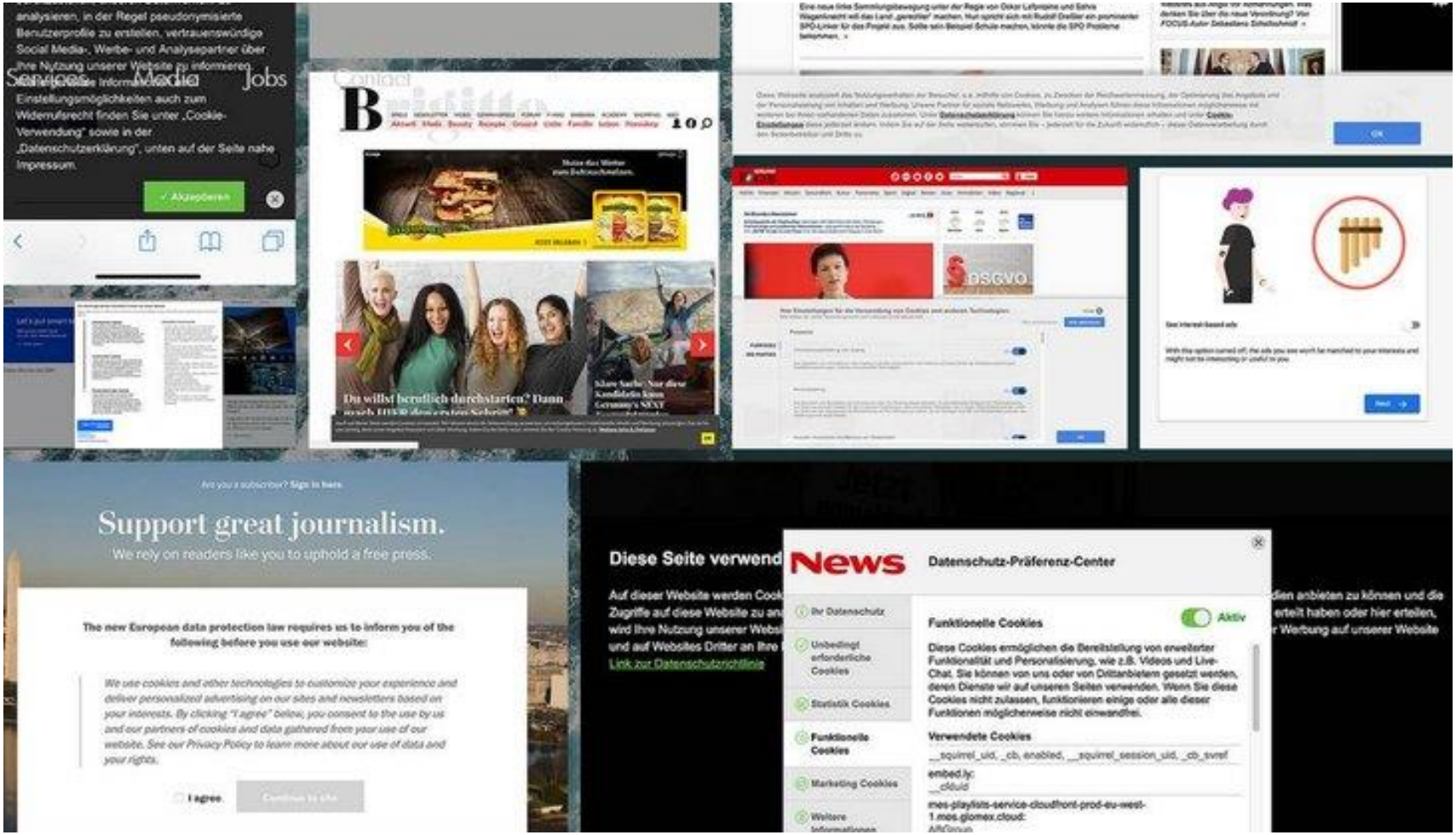
As data can be stored and processed in the “Exabyte” level and more connectivity and interaction is possible, information is ubiquitous. This triggers different threats

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

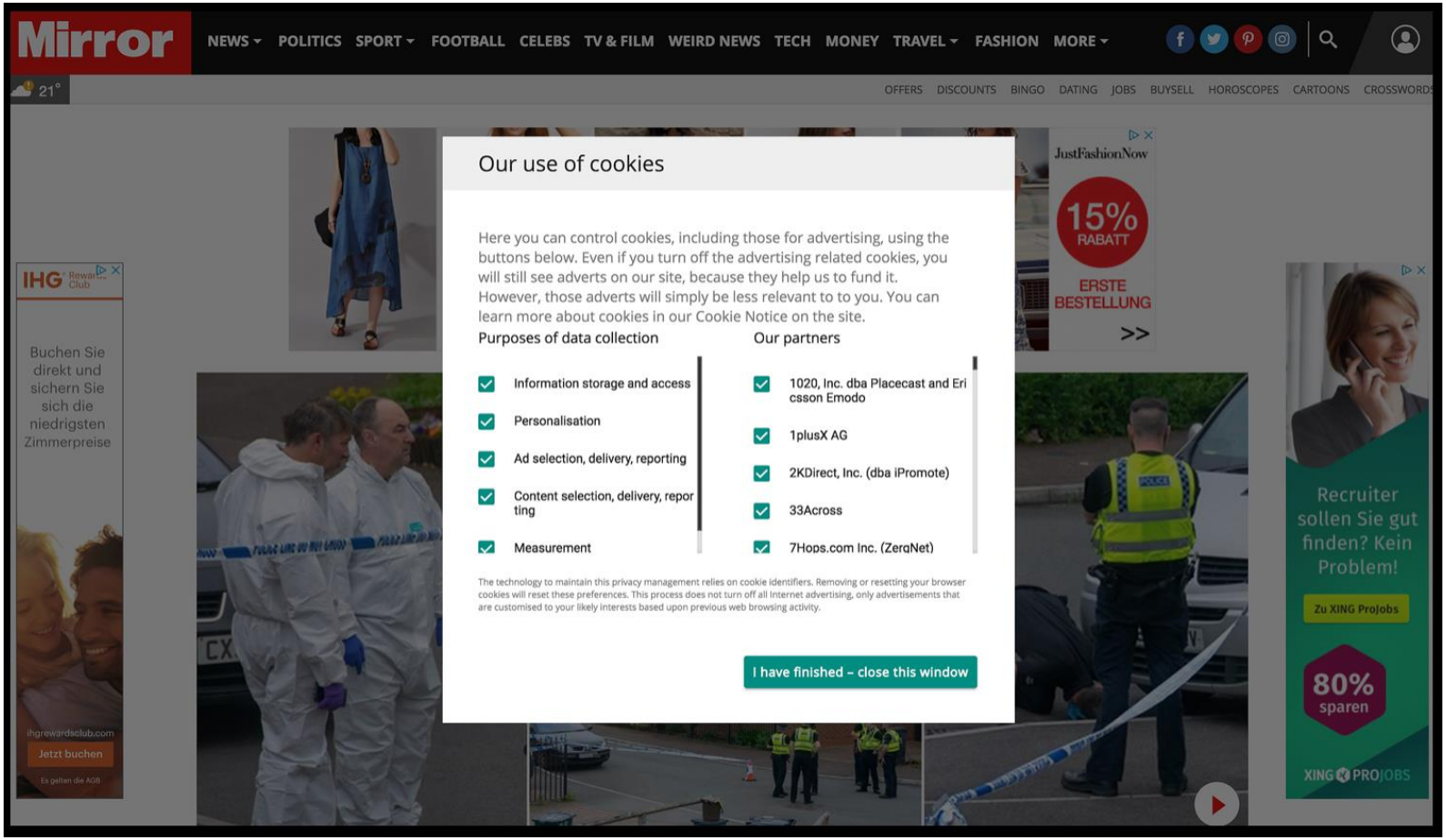
# Data Protection Law in Germany

- 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
  - …

# What is GDPR?


Services
Media
Jobs
Einstellungsmöglichkeiten auch zum Widerrufsrecht finden Sie unter „Cookie-Verwendung" sowie in der „Datenschutzerklärung", unten auf der Seite nahe Impressum.
✓ Akzeptieren
Du willst beruflich durchstarten? Dann
DSGVO
Are you a subscriber? Sign in here.
Support great journalism.
We rely on readers like you to uphold a free press.
The new European data protection law requires us to inform you of the following before you use our website:
We use cookies and other technologies to customize your experience and deliver personalized advertising on our sites and newsletters based on your interests. By clicking "I agree" below, you consent to the use by us and our partners of cookies and data gathered from your use of our website. See our Privacy Policy to learn more about our use of data and your rights.
I agree
Diese Seite verwend
News
Datenschutz-Präferenz-Center
Ihr Datenschutz
Unbedingt erforderliche Cookies
Statistik Cookies
Funktionelle Cookies
Marketing Cookies
Weitere
Funktionelle Cookies
Aktiv
Diese Cookies ermöglichen die Bereitstellung von erweiterter Funktionalität und Personalisierung, wie z.B. Videos und Live-Chat. Sie können von uns oder von Drittanbietern gesetzt werden, deren Dienste wir auf unseren Seiten verwenden. Wenn Sie diese Cookies nicht zulassen, funktionieren einige oder alle dieser Funktionen möglicherweise nicht einwandfrei.
Verwendete Cookies
__squirrel_uid, _cb, enabled, __squirrel_session_uid, _cb_svref
embed.ly:
__cfduid
mes-playlists-service-cloudfront-prod-eu-west-1.mes.glomex.cloud:

# What is GDPR?

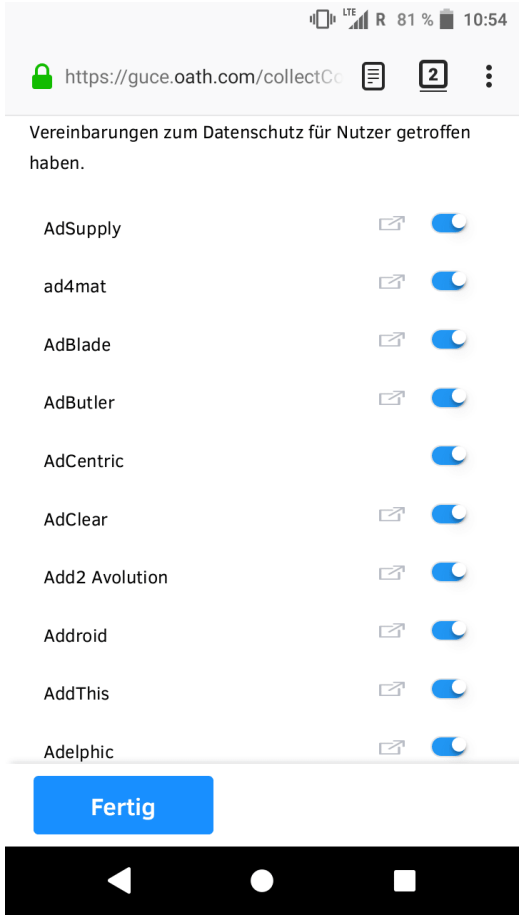

Mirror
NEWS
POLITICS
SPORT
FOOTBALL
CELEBS
TV & FILM
WEIRD NEWS
TECH
MONEY
TRAVEL
FASHION
MORE
21°
OFFERS
DISCOUNTS
BINGO
DATING
JOBS
BUYSELL
HOROSCOPES
CARTOONS
CROSSWORDS
Our use of cookies
Here you can control cookies, including those for advertising, using the buttons below. Even if you turn off 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 Rewards Club
Buchen Sie direkt und sichern Sie sich die niedrigsten Zimmerpreise
ihgrewardsclub.com
Jetzt buchen
Es gelten die AGB
Recruiter sollen Sie gut finden? Kein Problem!
Zu XING ProJobs
80% sparen
XING PROJOBS

# What is GDPR?

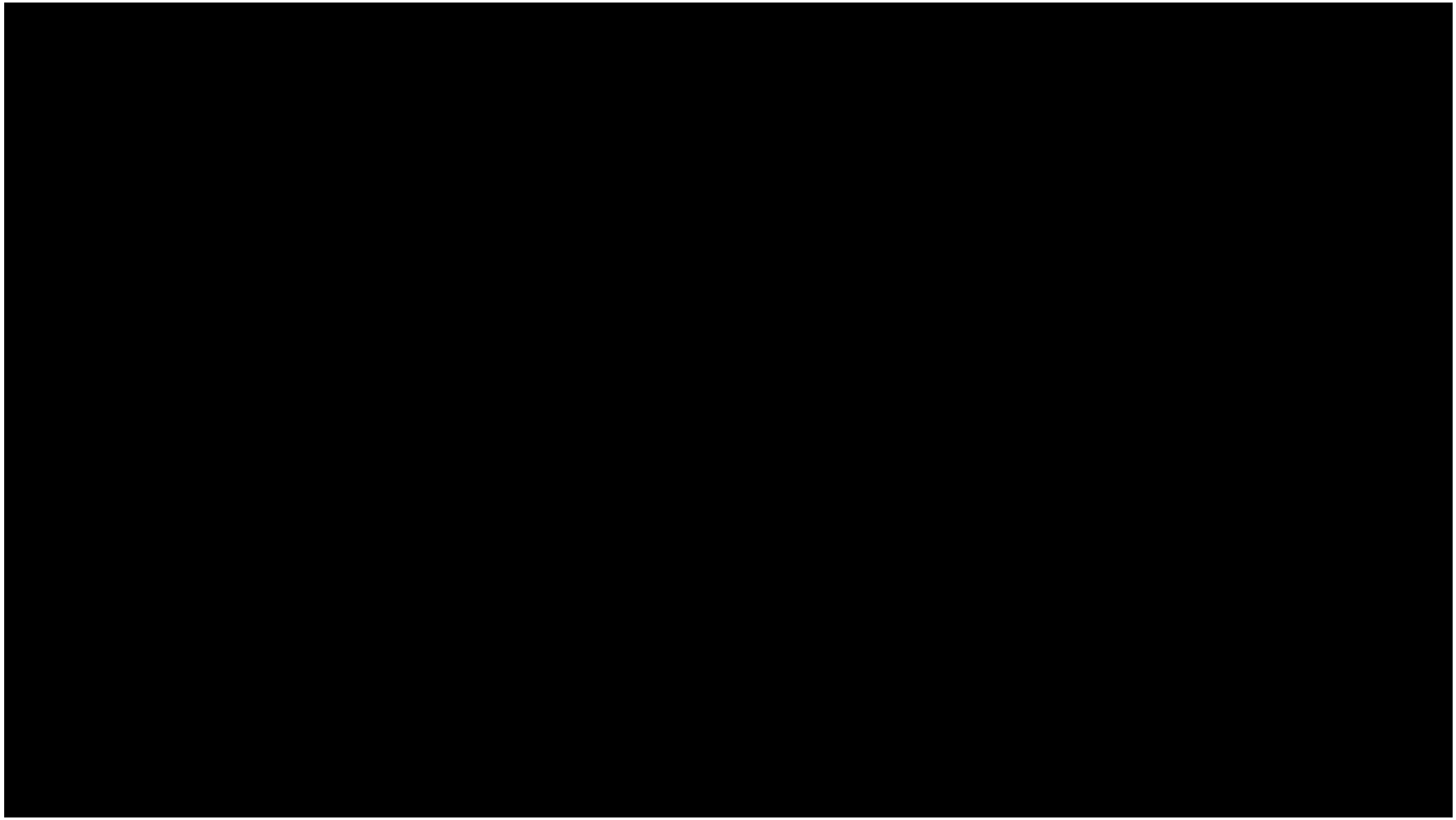

**More at:**
**https://m.heise.de/security/meldung/l-f-Das-DSGVO-Absurditaetenkabinett-4057866.html**

# What is GDPR?

**Oath users (AOL, Yahoo, …) had to give their consent that the service shares their data with several hundred advertisement partners… all of them were preselected.**



# 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

# IMKM Lecture 10: Information Security, Privacy and Risk Management

## Outline

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

## Learning Objectives

- *You know the basics and objectives of information security.*
- *You are able to discuss impacts of IT developments and the legal foundations of privacy.*
- *You are familiar with risks within information management and are able to outline and apply a risk management process.*
- *You are able to apply risk management methods.*

# 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

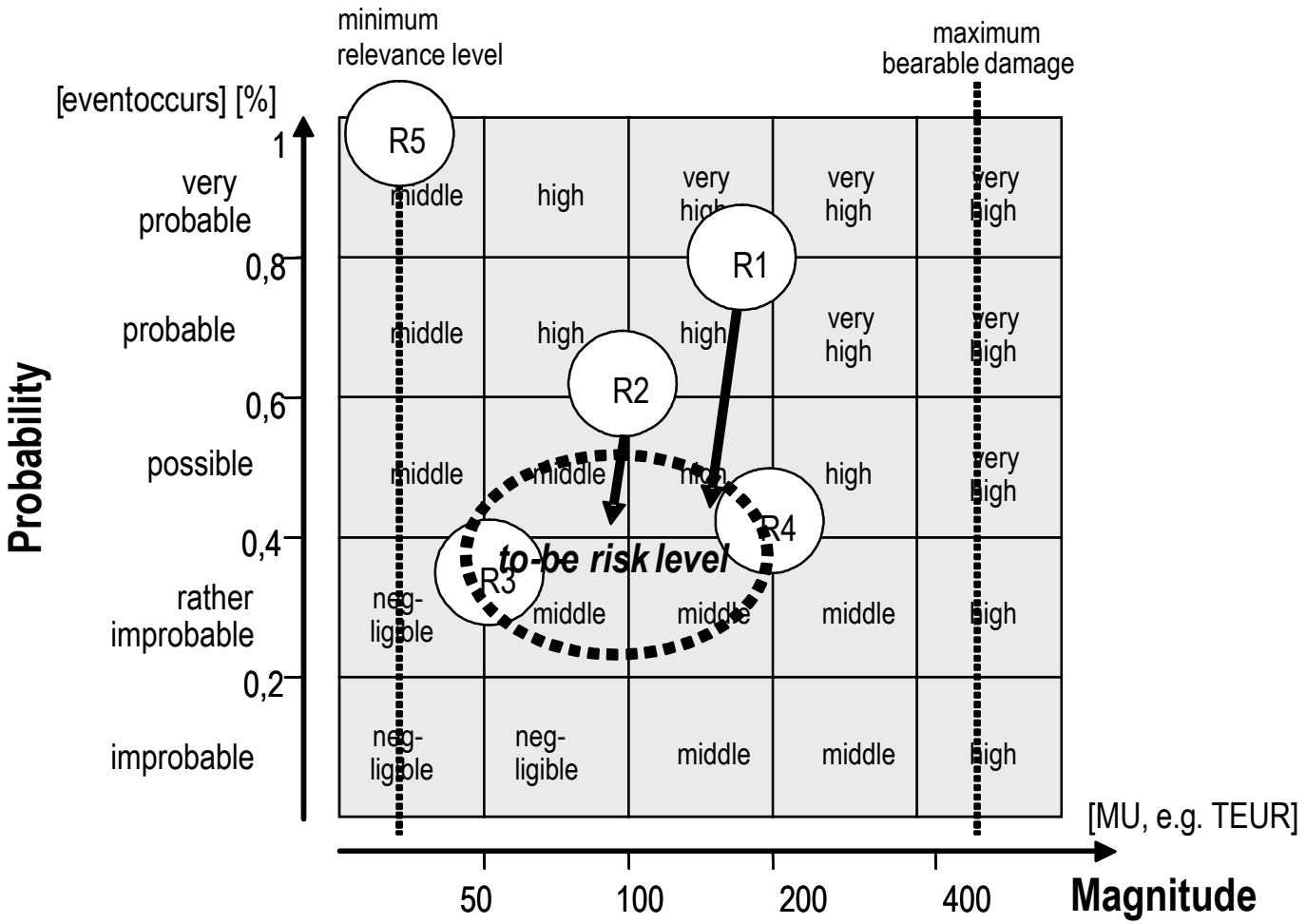
- **Known risks**
  - Those risks that can be uncovered after careful evaluation of the project plan, the business and technical environment in which the project is being developed, and other reliable information sources (e.g., unrealistic delivery date)
- **Predictable risks**
  - Those risks that are 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

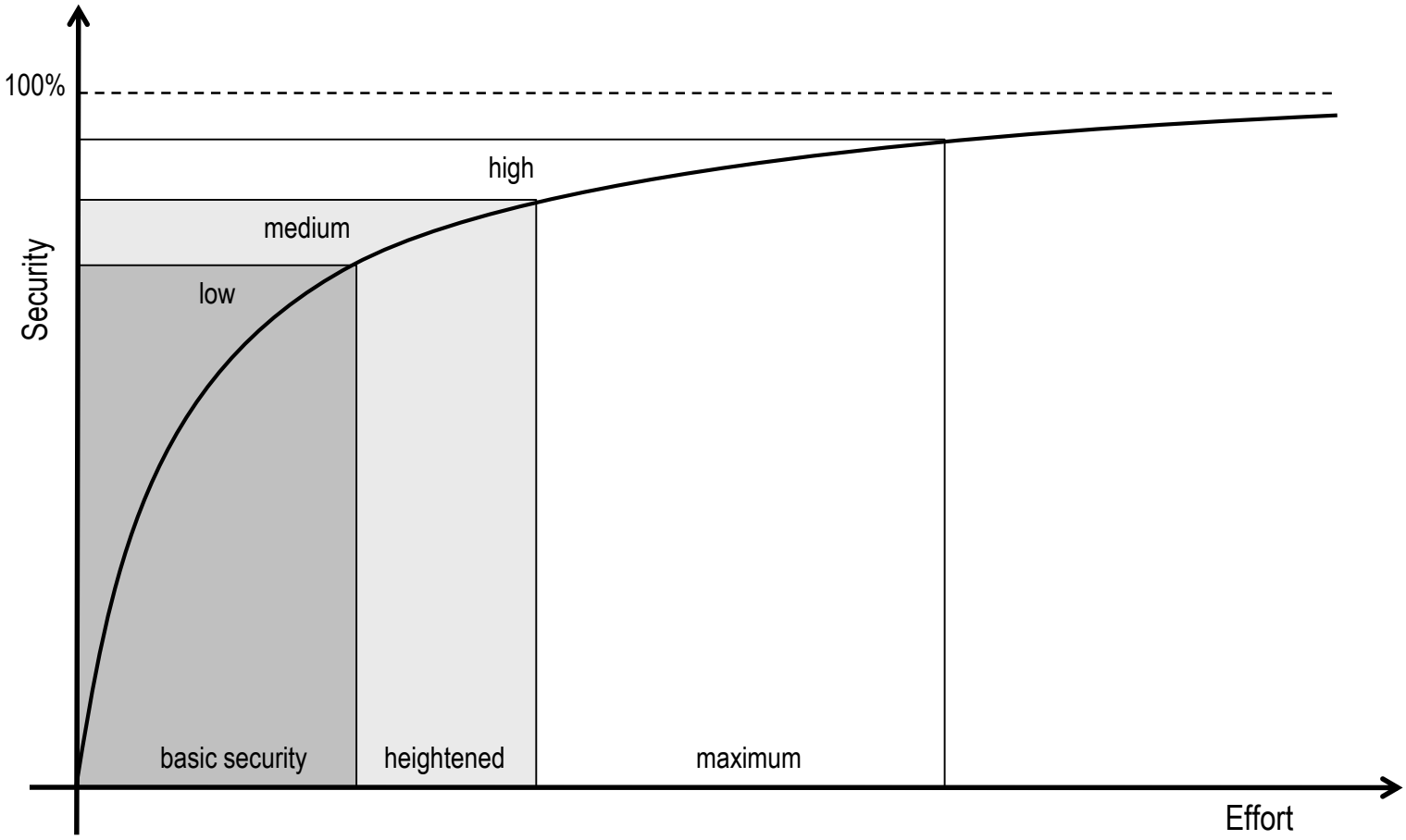
- Proactive risk strategies
  - Steps for risk management are followed
  - Primary objective is to avoid risk and to have a contingency plan in place to handle unavoidable risks in a controlled and effective manner

# What is the right balance?



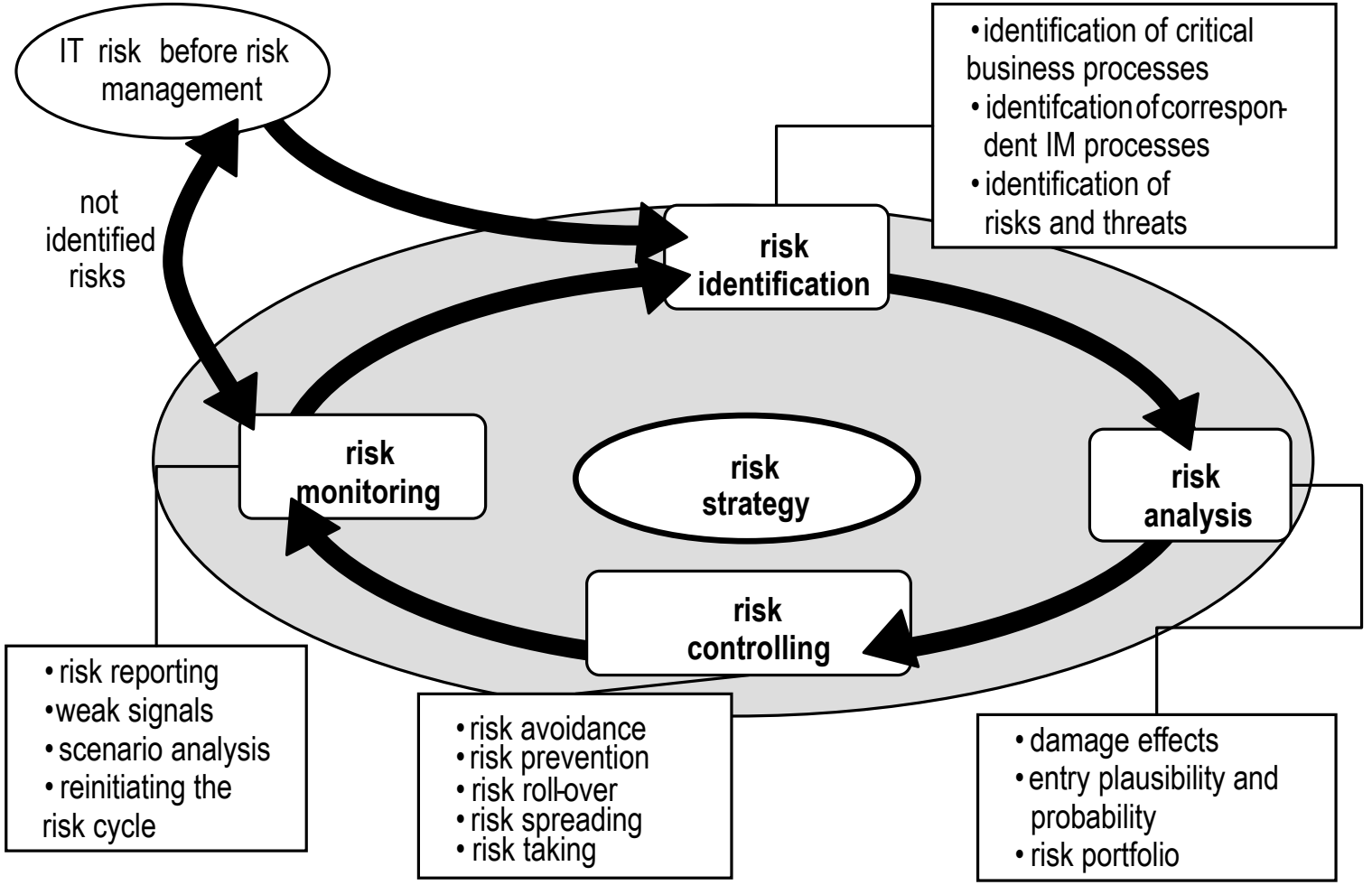

Source: Adapted from Junginger (2004, p. 281)

# Pareto at work…




Source: Krcmar (2015), p.525

# Risk Management Process within IM




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

# Risk Registers: Example

**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

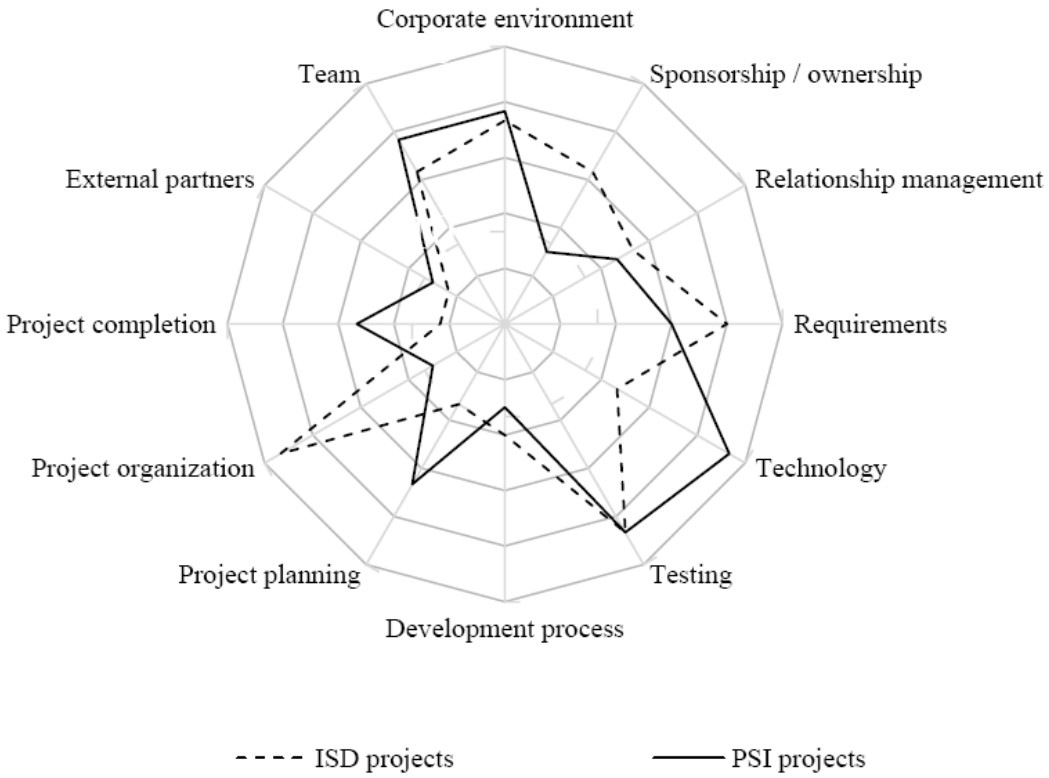
***Risk Analysis…***

- …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
  - Threat tree
  - risk prioritization

# Risk Prioritization: Differences Across Project Types

*Figure 3: Relative importance of risk sub-categories in ISD and PSI projects.*

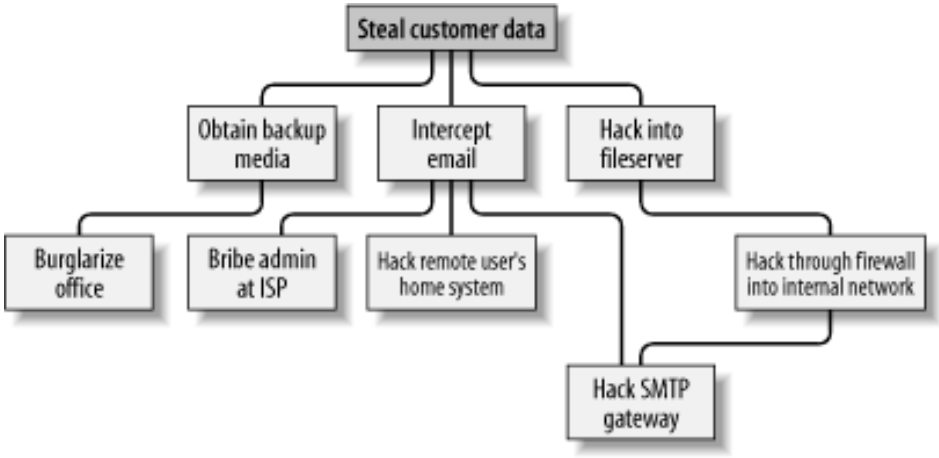



Hoerrmann et al. (2014)

# Threat Trees

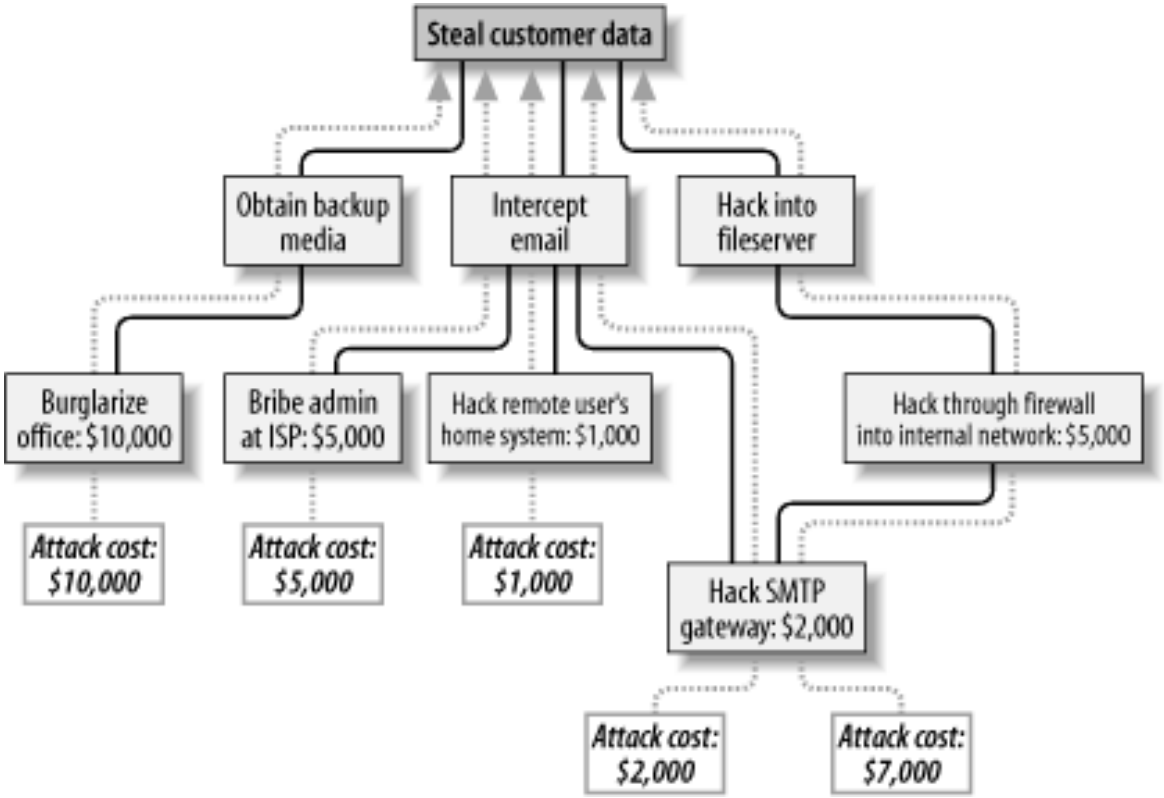
Threat trees summarize potential threats in a top-down view.

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




Schneier (1999); Eckert (2009)

# Example Threat Tree: Stealing Customer Data of ABC Corp.




Schneier (1999)

# Risk Controlling: Objectives and Tools

***Risk Controlling…***

- …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

# Risk Strategy Lists: 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

# Risk Visualizations: The Volatility of Project Risks

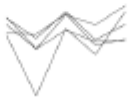
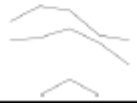
| C | Risks | Visualization | Temporal Characteristics |
|---|---|---|---|
| 1 | Complex System Architecture<br>Customer Financial Obligations<br>Solution Uncertainties |  | Remain constant initially<br>Gain importance towards project end |
| 2 | Low Project Priority<br>Implementation Partner Unknown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

*Table 3. Derived Risk Clusters*

Hoerrmann et al. (2011)

# The Issue of Project Risks

- Project characteristics
- Applegate, McFarlan and McKenney (1999) refer to three project dimensions which have the primary influence on implementation risk
  - project size,
  - the degree of new technology involved, and
  - the level of problem structure in the project.

Applegate et al. (1999)

# Project Characteristics

- **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.
- **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.

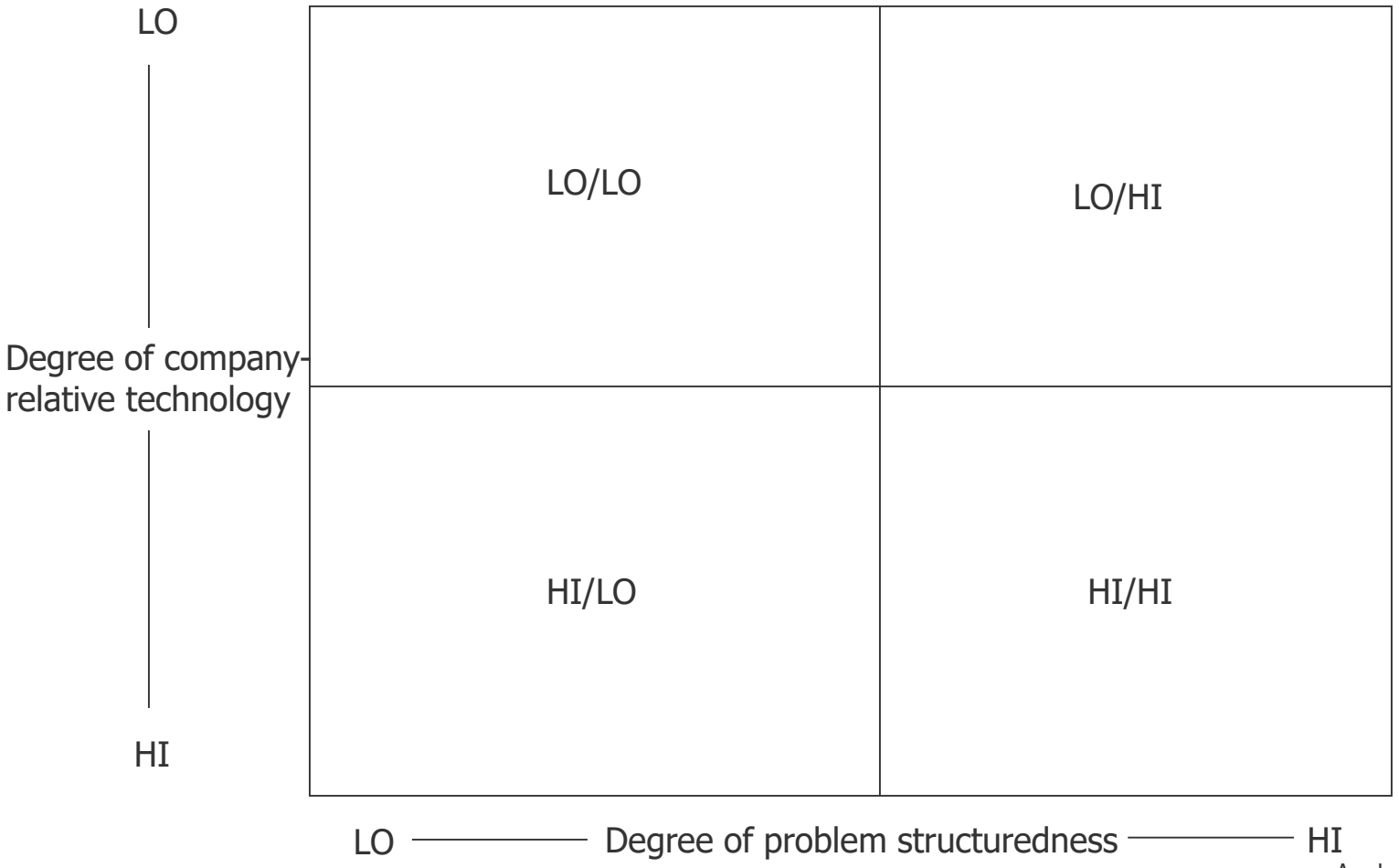
Applegate et al. (1999)

# Project Characteristics …

- **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)

# Understanding the Degree of IT Project Risk




Applegate et al. (1999)

# 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.
- 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.
- 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.