# Information and Communications Security SS 2020
# Assignment 4
# *Security Management*

23rd June 2020, Frankfurt

**Michael Schmid**
michael.schmid@m-chair.de
Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt
www.m-chair.de

# Agenda

I. Introduction Security Management
II. Use case Information Security Measurement
III. Use case Information Security Management
IV. Literature

# Speaker

- since 2012 deputy CISO @Hubert Burda Media Holding KG
- since 2017 PhD student @m-chair
- since 2017 founder and board member of AUDEG - Deutsche Auditoren eG
- > 10 years experience in the field of IT / Information Security
- areas of focus: ISMS, IT Compliance & Governance and Risk Management
- active participation in (inter)national committees: UPKRITIS, ISACA, GI & RMA

# 2 positions as Student Assistant @m-chair

2 new student assistants positions @m-chair

Details
https://www.m-chair.de/index.php/chair/career

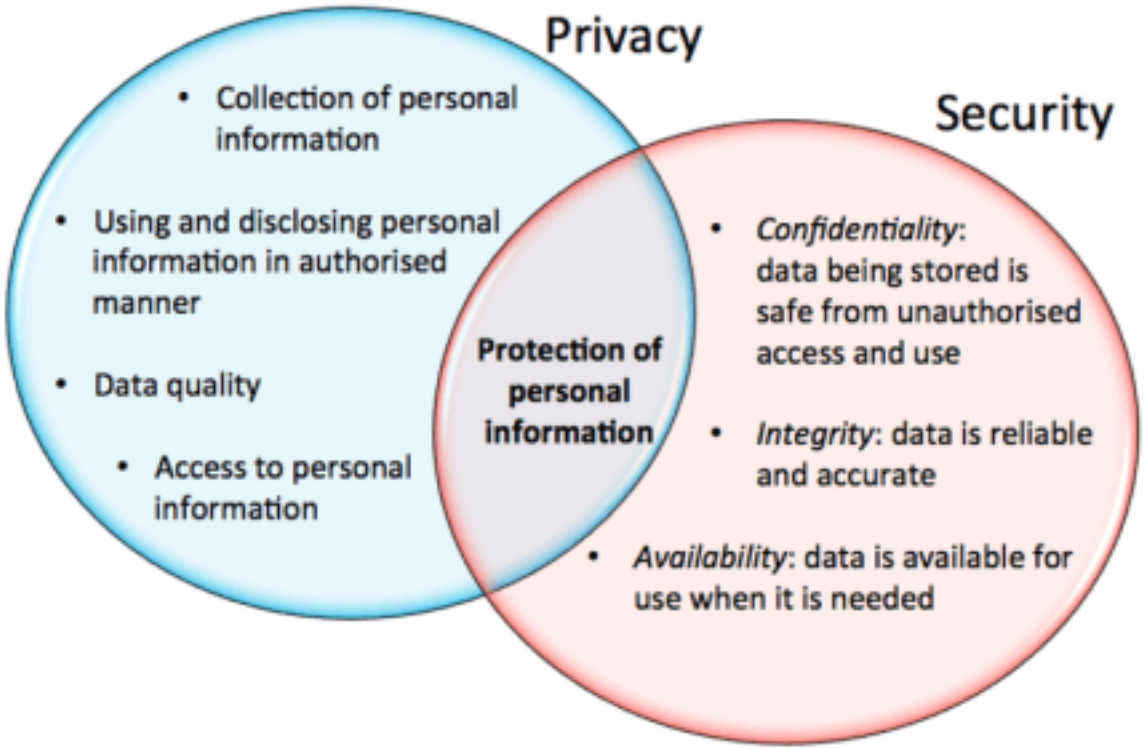
# I. Introduction Security Management

**G**overnance, **R**isk management and **C**ompliance (GRC)


Source: softexpert.com

# I. Introduction Security Management

Privacy vs. Security




Source: davidfroud.com

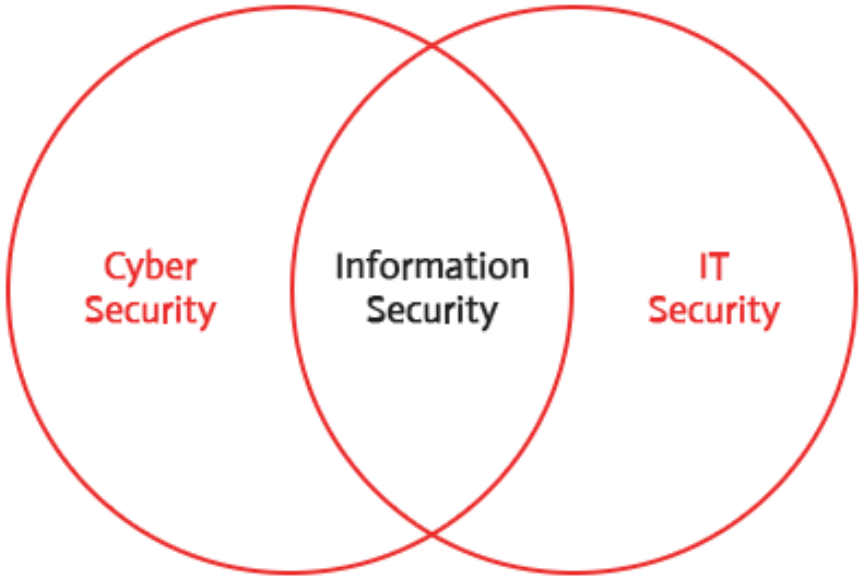
# I. Introduction Security Management

CIA vs. Information security?


Source: comtact.co.uk

# I. Introduction Security Management

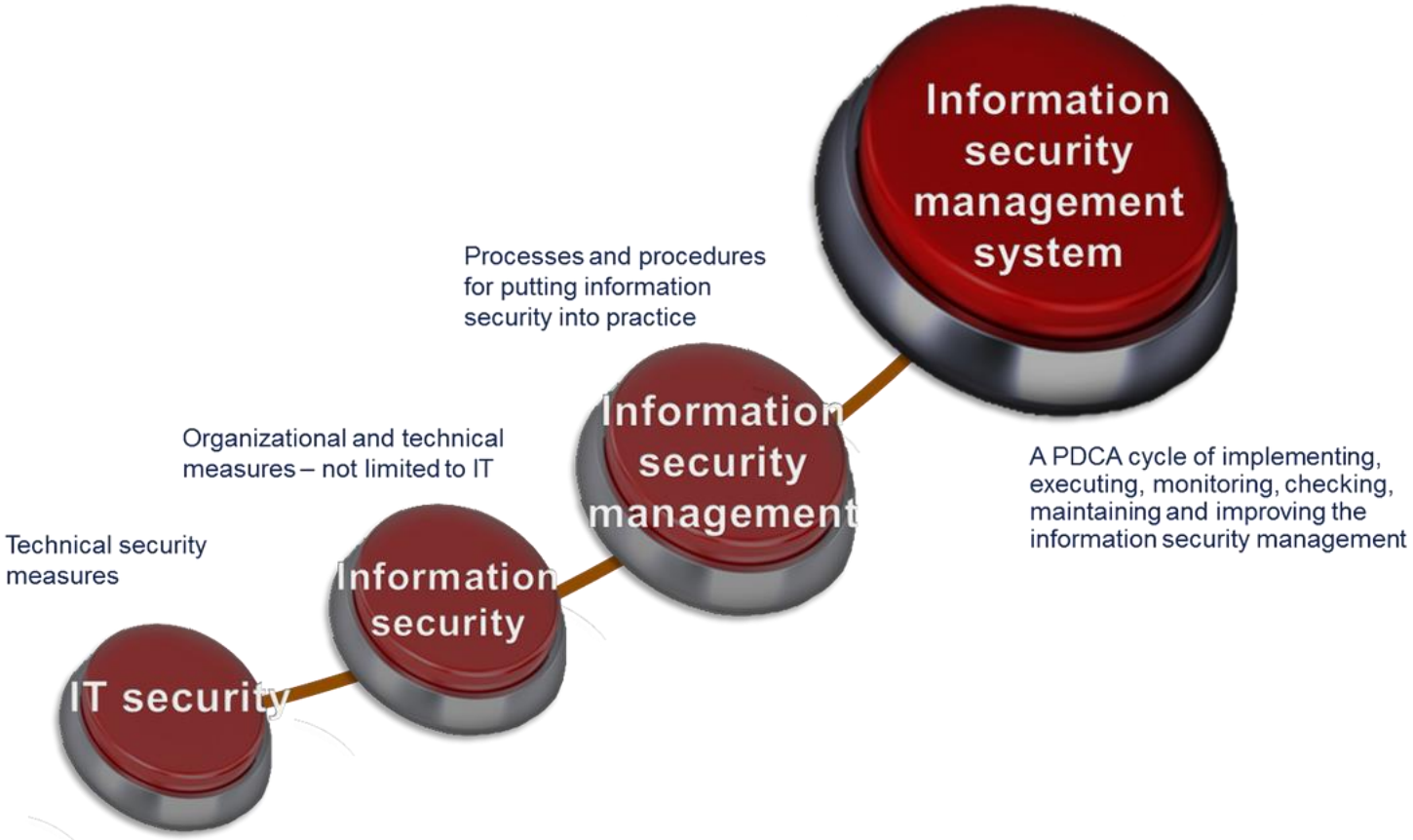
Cyber vs. Information vs. IT Security




Source: businessbeam.com

# I. Introduction Security Management

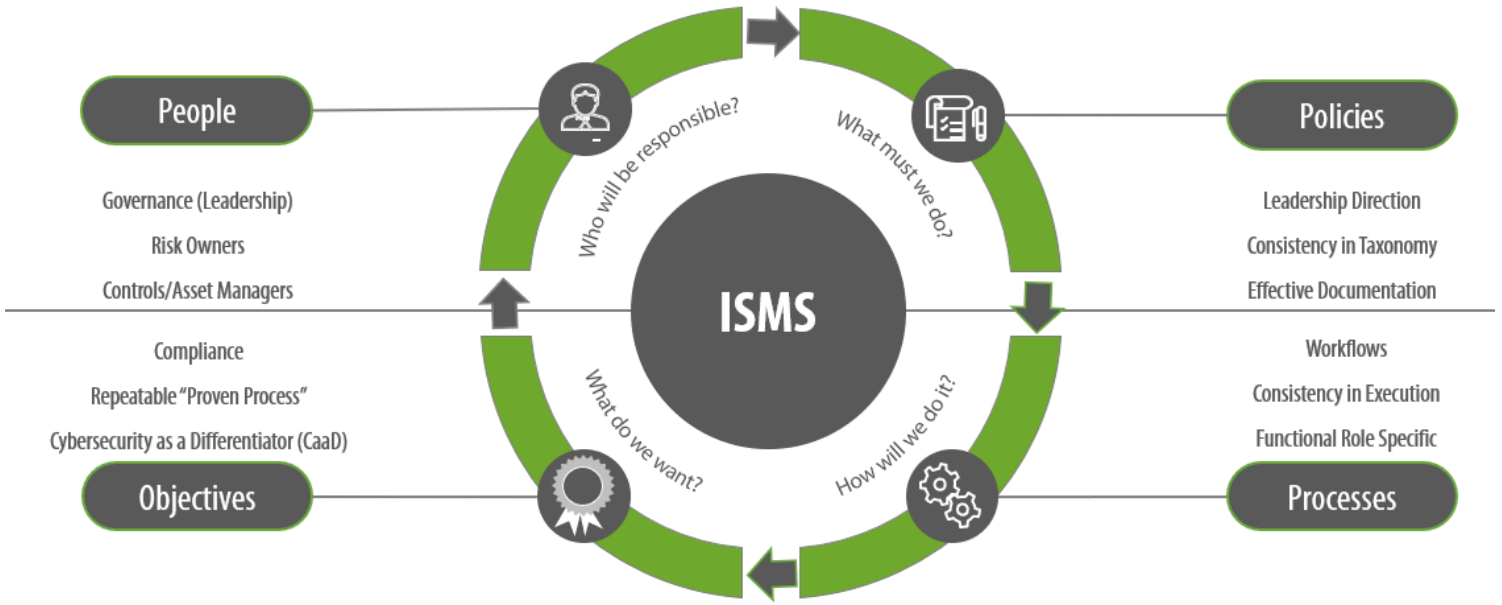
From IT security to an Information security management system




Source: it-pillars.com

# I. Introduction Security Management

## Information Security Management System (ISMS)




Source: cyberintsolns.com

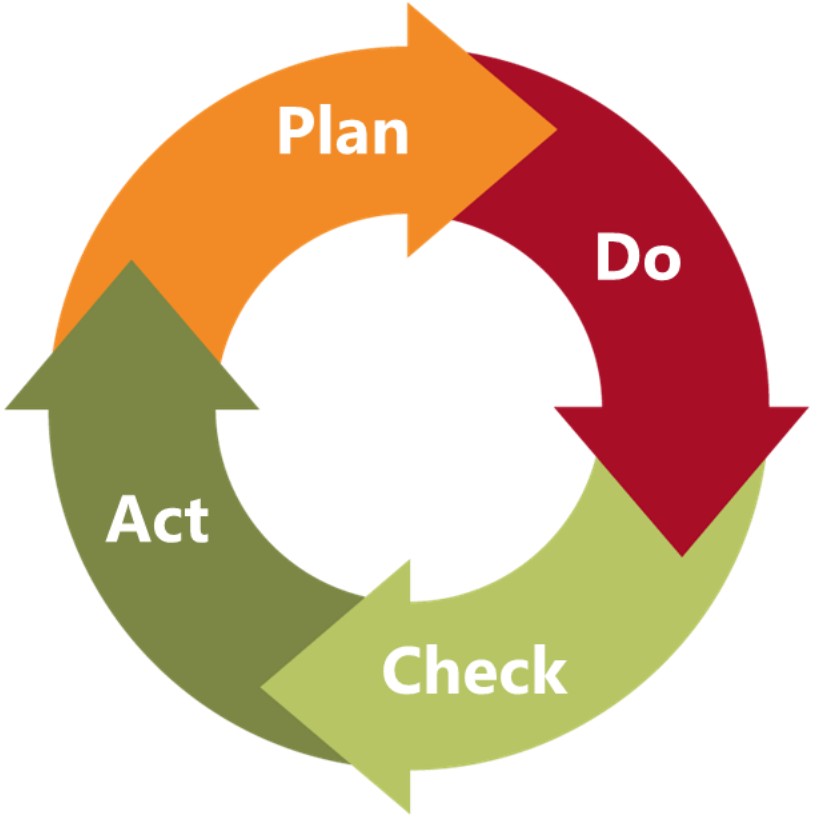
# I. Introduction Security Management

ISO/IEC 27001:2013 is the internationally recognised management system standard for information security.


Source: caveonix.com

# I. Introduction Security Management

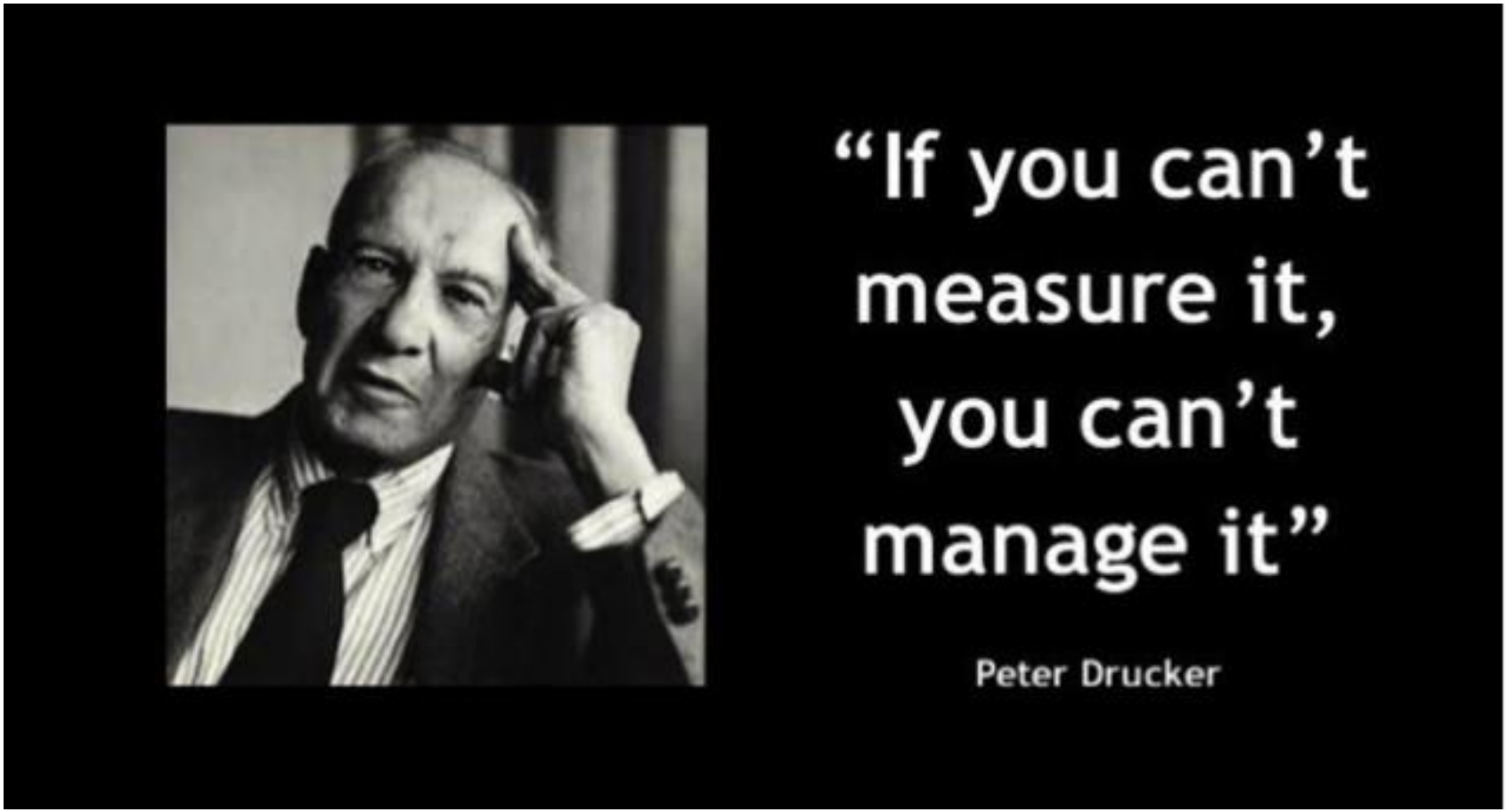
PDCA or Demin circle




Source: glauxsoft.com

# I. Introduction Security Management

## Information Security Measurement




Source: busyqueenbee.com

# I. Introduction Security Management

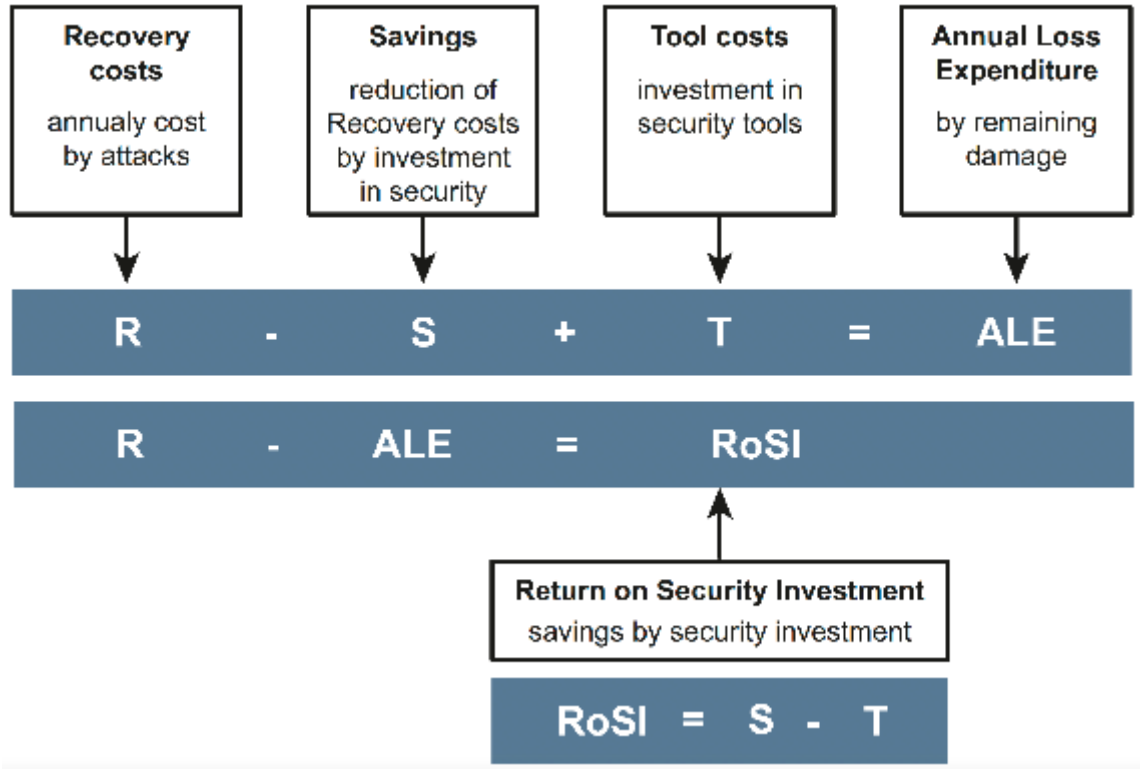
Key Performance Indicator (KPI)


Source: adbox24.de

# II. Use case Information Security Measurement

Return on Security Investment (RoSI)

RoSI means that by looking at all costs (including those caused by damage from an attack) it can be shown whether and when an investment in information security measures leads to a return on investment or not.



# II. Use case Information Security Measurement

Return on Security Investment (RoSI)

Description of the abbreviations:

**Recovery Costs - R (cost of probable damage)**
These costs describe all expenses that are necessary to restore the original condition after damage has occurred. They are included in the total costs of business activities. The recovery costs depend on the actual occurrence of damage, but must be estimated for the future on the basis of experience.

**Savings - S (reduction of the cost of probable losses)**
These are the costs saved by the introduction of cyber security mechanisms (tools) because they are very likely to successfully prevent an attack. These costs must also be estimated.

**Tool Costs - T (costs for cyber security measures)**
This is the total cost of ownership (TCO) of cyber security measures designed to prevent potential attacks with a high probability.

# II. Use case Information Security Measurement

Return on Security Investment (RoSI)

Description of the abbreviations (cont.):

**Annual Loss Expenditure - ALE (remaining costs)**
These are the remaining costs (damage) after an investment in cyber security measures.

**Return on Security Investment - RoSI (saved costs, achieved profit)**
Savings in the recovery cost (damage) achieved by investing in cyber security measures

Hint:
As long as T (Tools), the TCO of cyber security measures, are smaller than S (Savings), the reduction of costs, RoSI is positive:

formula: R-(R - S + T)= RoSI = S - T

# II. Use case Information Security Measurement



**Sample calculation RoSI: Notebook losses**

In this example, a calculation of the Return on Security Investment (RoSI) is to be carried out based on the losses of notebooks and the investment in a suitable cyber security measure that protects the data on the notebooks.

The first thing to discuss is how likely it is that a notebook will be lost or stolen, and what resulting damage would occur:

1. What is the probability of losing a notebook?
   - The various available studies on lost or stolen notebooks show that on average 6% of notebooks are stolen or lost annually (probability of occurrence).

# II. Use case Information Security Measurement

Return on Security Investment (RoSI)

**Sample calculation RoSI: Notebook losses (cont.)**

2. How high is the damage if the data stored on a notebook is misused by third parties?
   - If the various studies (Computer Security Institute - Crime&Security Survey, Security Issues and Trends, ...) on the damage caused by lost notebooks are analysed, the result is that the average damage per stolen notebook is over EUR 10,000.
   - This is only the damage caused by misuse of the data, the loss of hardware, software and the recovery of a replacement device must be added to this should be considered (EUR 2,000 to 3,000).
3. Cyber security measure to protect the information stored on a notebook are stored
   - To estimate the cost necessary to adequately protect a notebook, it is assumed that a hard disk encryption product is used.
   - The purchase of such a cyber security measure costs about EUR 110, which is on average about 4% of the purchase price of a notebook.

# II. Use case Information Security Measurement

Return on Security Investment (RoSI)

**Calculation of the Return on Security Investment (RoSI)**

As an example, a company is assumed where 500 employees own a notebook on which valuable data worthy of protection is stored for work.

Assumptions:

- Damage caused by the loss of stored data per stolen notebook = EUR 10,000
- The number of notebooks stolen each year is assumed to be 6% = 30 notebooks (probability of occurrence).
- One-time license costs: 500 * EUR 110 = EUR 55,000
- For the further costs of installation, rollout and administration, EUR 10,000 is assumed in the first year and EUR 5,000 in the following years.
- 30 notebooks * EUR 10,000 = EUR 300,000
- Here only the damage caused by the misuse of the stored data.

# II. Use case Information Security Measurement

Return on Security Investment (RoSI)

## Return on Security Investment RoSI – Example calculation

| Calculation | | | | | In total |
|---|---|---|---|---|---|
| Time span | 1st year | 2nd year | 3rd year | 4th year | 4 years |
| Initial costs | | | | | |
| Implementation/ Rollout, Admin | | | | | |
| Value of no losses from sec breaches | | | | | |
| RoSI 1st year | | | | | |
| RoSI 2nd year | | | | | |
| RoSI 3rd year | | | | | |
| RoSI 4th year | | | | | |

# II. Use case Information Security Measurement

Return on Security Investment (RoSI)

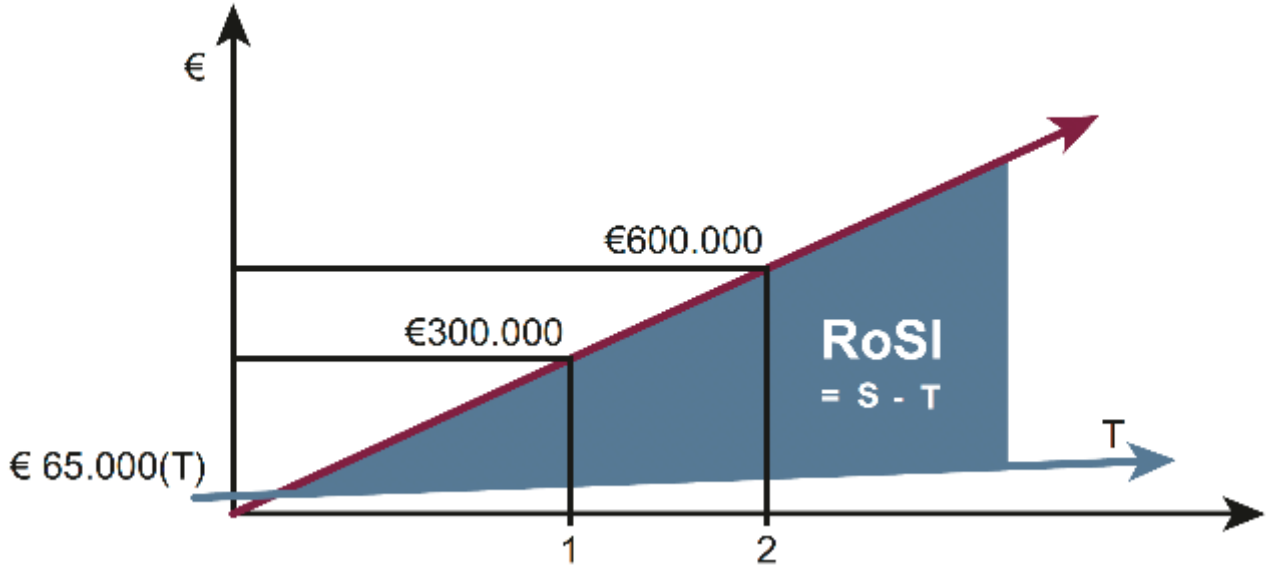
## Return on Security Investment RoSI – Example calculation

| Calculation | | | | | In total |
|---|---|---|---|---|---|
| Time span | 1st year | 2nd year | 3rd year | 4th year | 4 years |
| Initial costs | EUR 55,000 | - | - | - | EUR 55,000 |
| Implementation/ Rollout, Admin | EUR 10,000 | EUR 5,000 | EUR 5,000 | EUR 5,000 | EUR 25,000 |
| Value of no losses from sec breaches | EUR 300,000 | EUR 300,000 | EUR 300,000 | EUR 300,000 | EUR 1,200,000 |
| RoSI 1st year | EUR 235,000 | | | | |
| RoSI 2nd year | | EUR 530,000 | | | |
| RoSI 3rd year | | | EUR 825,000 | | |
| RoSI 4th year | | | | EUR 1,120,000 | EUR 1,120,000 |

# II. Use case Information Security Measurement

Return on Security Investment (RoSI)

Cyber security costs and the potential loss over four years




This shows that a ROI of EUR 235,000 can be achieved in the first year alone. After four years the ROI is EUR 1,120,000.
The figure clearly shows that the investment T in hard disk encryption is smaller than the prevented damage S that would occur through the misuse of the stored data.

Source: Norbert Pohlmann – Cyber Sicherheit

# II. Use case Information Security Measurement

## Return on Security Investment (RoSI)

Other examples where a RoSI calculation can usually be easily performed are

Anti-malware solutions:

- In this area, most companies themselves have available figures on the costs incurred by malware damage in recent years.

ID management, SingleSignOn (SSO) or authentication with biometric procedures:

- Here the savings effect of helpdesk costs can be very well proven (EUR 100 to 200 per year per user).

# III. Use case Information Security Management

GAP analysis

**Example**

Actual situation

Conducting a GAP analysis for an SME. This SME develops and operates classic websites, mobile offers and apps.

1. Determination of the need for protection of the information assets
2. Assignment of information values to IT systems
3. Risks derived therefrom
4. Risk mitigation measures

# III. Use case Information Security Management

GAP analysis

Determination of the need for protection (regular, advanced and high) of the information assets

| Cat. | Data | Confident -iality | Integrity | Availability | Total |
|---|---|---|---|---|---|
| I | Customer/subscriber data | high | high | regular | **high** |
| II | | | | | |
| III | | | | | |
| IV | | | | | |
| V | | | | | |
| VI | | | | | |
| VII | | | | | |
| VIII | | | | | |
| IX | | | | | |

# III. Use case Information Security Management

GAP analysis

Determination of the need for protection (regular, advanced and high) of the information assets

| Cat. | Data | Confident -iality | Integrity | Availability | Total |
|---|---|---|---|---|---|
| I | Customer/subscriber data | high | high | regular | **high** |
| II | Extended customer data records (newsletter, B2B, income …) | high | high | regular | **high** |
| III | Financial data for online business | high | high | regular | **high** |
| IV | Source code | regular | regular | regular | **regular** |
| V | Access data (to portals, web analysis systems, newsletter systems etc.) | high | advanced | advanced | **high** |
| VI | Business data (*business results, customer presentations, concepts …) | advanced/ *high | advanced/ *high | regular/ *regular | **advanced/ *high** |
| VII | Technical concepts | high | advanced | regular | **regular**** |
| VIII | Employee data (e.g. target agreements) | high | advanced | regular | **high** |
| IX | Web analysis data | regular | regular | regular | **regular** |

**Overruled by management

# III. Use case Information Security Management

GAP analysis

| | | Category | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| No. | IT system | I | II | III | IV | V | VI | VII | VIII | IX |
| 1 | Newsletter tool | x | x | | | | | | | |
| 2 | Deployment tool | | | | | | | | | |
| 3 | PM tool | | | | | | | | | |
| 4 | CMDB | | | | | | | | | |
| 5 | SAP | | | | | | | | | |
| 6 | File server | | | | | | | | | |
| 7 | Desktops | | | | | | | | | |
| 8 | Notebooks | | | | | | | | | |
| 9 | Mail server | | | | | | | | | |
| 10 | FTP server | | | | | | | | | |
| 11 | Cloud | | | | | | | | | |

Mapping between information assets and IT system

# III. Use case Information Security Management

GAP analysis

| | | Category | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| No. | IT system | I | II | III | IV | V | VI | VII | VIII | IX |
| 1 | Newsletter tool | x | x | | | | | | | |
| 2 | Deployment tool | | | | x | | | | | |
| 3 | PM tool | | | | | x | | | | |
| 4 | CMDB | | | | | x | | | | |
| 5 | SAP | | | x | | | x | | | |
| 6 | File server | x | x | x | x | x | x | x | x | x |
| 7 | Desktops | x | x | x | | x | x | x | x | x |
| 8 | Notebooks | x | x | x | x | x | x | x | x | x |
| 9 | Mail server | x | x | x | x | x | x | x | x | x |
| 10 | FTP server | x | x | | | | | | | |
| 11 | Cloud | x | x | x | x | x | x | x | x | x |

Mapping between information assets and IT system

# III. Use case Information Security Management

GAP analysis

Risk assessment

| Risk No. | Risk description | Risk category | Information asset | IT system | Impact | Probability |
|---|---|---|---|---|---|---|
| R1 | Unauthorized use of data (e.g. shipping of advertising without opt-in) | Legal risk, reputational risk | I, II | 1, 6, 7, 8, 9, 10, 11 | high | Entry as good as certain |
| R2 | | | | | | |
| R3 | | | | | | |

# III. Use case Information Security Management

GAP analysis

## Risk assessment

| Risk No. | Risk description | Risk category | Information asset | IT system | Impact | Probability |
|---|---|---|---|---|---|---|
| R1 | Unauthorized use of data (e.g. shipping of advertising without opt-in) | Legal risk, reputational risk | I, II | 1, 6, 7, 8, 9, 10, 11 | high | Entry as good as certain |
| R2 | Theft of customer data, company or business data, employee data | Legal risk, reputational risk, business process risk | I, II, III, IV | 1, 6, 7, 8, 9, 10, 11 | high | Entry as good as certain |
| R3 | Manipulation of customer data, company or business data, employee data | business process risk | I, II, III | 1, 6, 7, 8, 9, 10, 11 | high | Entry as good as certain |

# III. Use case Information Security Management

GAP analysis

## Risk mitigation measures

| Measure No. | Measure | Against risk | IT system/application | Priority | Implement-ation |
|---|---|---|---|---|---|
| M1 | Set up a central process for employee approval and access | R1 | all | medium | Q3 2020 |
| M2 | | | | | |
| M3 | | | | | |
| M4 | | | | | |
| M5 | | | | | |
| M6 | | | | | |

# III. Use case Information Security Management

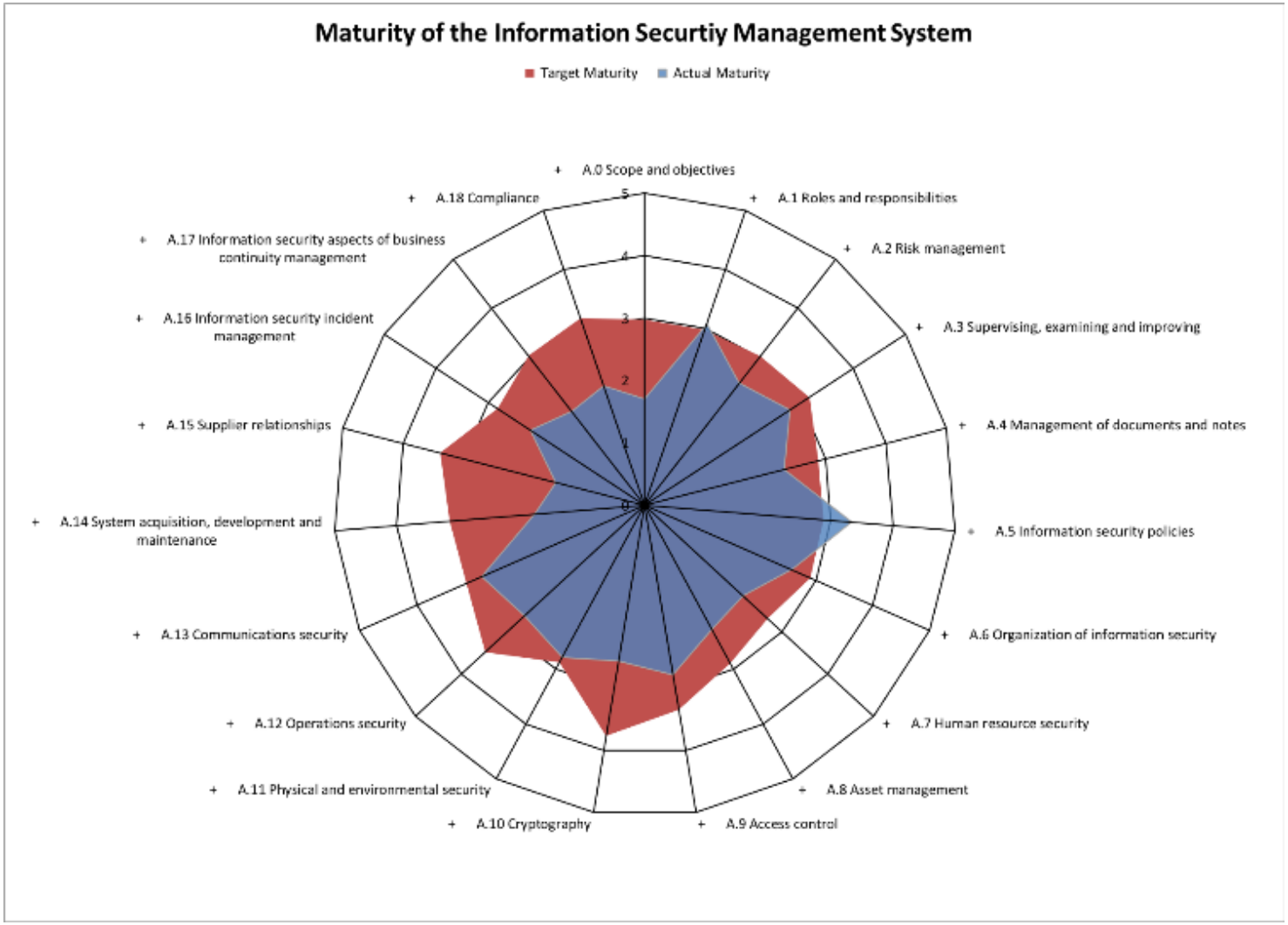
GAP analysis

## Risk mitigation measures

| Measure No. | Measure | Against risk | IT system/application | Priority | Implemen-tation |
|---|---|---|---|---|---|
| M1 | Set up a central process for employee approval and access | R1 | all | medium | Q3 2020 |
| M2 | Systematic withdrawal of access rights after leaving the company | R1, R2, R3 | all | high | Q3 2020 |
| M3 | Defined role and user concept of the applications | R1 | Newsletter tool, Deployment tool, PM tool, CMDB | medium | Q4 2020 |
| M4 | Awareness training according to target group | R1, R2, R3 | all | high | Begin Q3 2020 |
| M5 | Revise rights structure of the file server | R1, R2, R3 | File server | high | Q3 2020 |
| M6 | Develop specifications for data exchange (customer data) | R1, R2 | Mail server, FTP server, Cloud | medium | Q4 2020 |

# III. Use case Information Security Management

GAP analysis




Source: Hubert Burda Media

# IV. Literature


- Management of Information Security, M. E. Whitman, H. J. Mattord
- Guide to Disaster Recovery, M. Erbschilde
- Guide to Network Defense and Countermeasures, G. Holden
- Real Digital Forensics: Computer Security and Incident Response, 1/e; Keith J. Jones, Richard Bejtlich, Curtis W. Rose
- Computer Security: Art and Science, Matt Bishop (ISBN: 0-201-44099-7), Addison-Wesley 2003
- Security in Computing, 2nd Edition, Charles P. Pfleeger, Prentice Hall

## Chair of Mobile Business & Multilateral Security

**Michael Schmid**
Goethe University Frankfurt
E-Mail: michael.schmid@m-chair.de
WWW: www.m-chair.de