A Comprehensive and Comparative Metric for Information Security

Steffen Weiß[1], Oliver Weissmann[2], Falko Dressler[1*]
[1] Dept. of Computer Science 7, University of Erlangen, Germany
[2] atsec information security GmbH, Germany

Abstract

Measurement of information security is important for organizations to justify security decisions and investments. Unfortunately, there are no metrics available that allow for a comprehensive security assessment of an entire organization. It turned out that there are two main aspects which are important to develop such a metric. On the one hand, an appropriate security indicator is required and, on the other hand, a method for combining single security aspects to an overall security measure for an entire organization.

An approach fulfilling these two aspects is presented in this article. Besides a comparable indicator, based on the intuitive understanding of security, an approach is proposed for combining single security aspects to reflect the organization's security assessment.

The presented approach was evaluated on a small university department. It will influence on forthcoming ISO 27004 metric-standard, which aligns with the already existing and well known ISO 17799.

1. Motivation and Objectives

Number and severity of attacks against the IT-infrastructure of almost any organization is steadily growing [19]. Additionally, the number of uncovered security threats grows, for example in operating systems. Thus, the organization is under growing risk: intruders are able to attack organizations and might cause enormous damage. As a result, organizations are likely to loose assets and conclusively to loose money. In order to avoid such loss, organizations try to secure their systems and to save money by installing controls. However, the question arises where to invest and especially how much. Installing very many controls usually leads to an improved security, but to high costs due to installation and maintenance. In opposite, installation of none or not enough controls will lead to large and expensive security incidents, which, in turn, might be also very expensive for the organization. Therefore, there is a growing requirement for an appropriate measure for evaluating the security of an entire organization.

Moreover, there is an additional reason measuring the security risks of an organization: security risks usually influence the operational risk of an organization. Due to BASEL II [1], the operational risk of an organization has become an important aspect for loan granting.

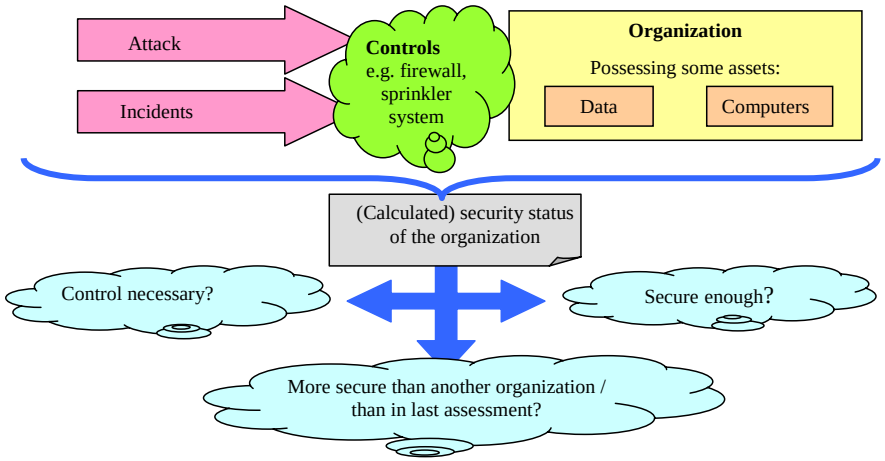

Fig 1. The security metric as the core module of a security program

Fig 1 summarizes the discussed problem in a graphical representation: attacks like viruses and theft but also security incidents can harm the organization's IT infrastructure. Nevertheless, there are controls like firewalls or sprinkler systems available, which protect the physical and logical assets of the organization. Taking all these aspects together, the security status of the organization can be determined. This status provides an appropriate measure for

* Corresponding author: Dr. Falko Dressler, Dept. of Computer Science 7, University of Erlangen, Martensstr. 3, 91058 Erlangen, Germany; Telephone: +49 9131 85-27914, Email: dressler@ieee.org

the potential risks. Additionally, it can be used for specifying and evaluating installed and required investments into security controls.

2. Requirements on the Security Metric

In a first step, the main requirements are presented that are necessary for a security metric describing the overall organization's security. The most important aspects are:

- **Comprehensive assessment of the entire organization**: Assessment of single security aspects is useful for some extend. Nevertheless, the most important issue is the influence of these single aspects on the security of the entire organization. Thus, the measurement of the overall security status is of importance, not only the status of single aspects which are possibly not even relevant under special conditions. This overall security shall not only be limited to attacks like viruses or theft but shall also cover incidents like fire or flood. In our opinion, this is the most important requirement.
- **Objectivity**: Security assessment must not reflect one single person's opinion but must make results meaningful to a wider audience. Obviously, such a kind of objectivity cannot be well-defined or even expected. Thus, objectivity shall be claimed in terms of comparability, that is (possibly different) security experts achieve similar security results under similar conditions. In this context, objectivity also includes repeatability. The repeated application of the metric must produce similar outcomes.
- **Comparability**: It is important to measure and observe security improvements or declines over time. Additionally, results must be comparable to results of other organizations and the possibility is important to simulate different situations like additional controls. These three aspects are very important for organizations having established a security metric to analyze improvement or decline.

3. Related Work

Security metrics, at least such metrics trying to define a measure for the security of an entire organization, are a quite new area of research. Conclusively not many directly connected research results are available. In this section, some approaches focusing on the security assessment of organizations are presented. The most important solutions are:

- **Best-practice approaches** (e.g. ISO/IEC 17799 [12], BS 7799 [2, 3] and NIST SP 800-33 [14]): Contain suggestions for security controls to improve information security. For example, the control "Addressing security in third party agreements" of ISO 17799 contains terms, important to be included in agreements with suppliers. These approaches are useful as a starting point for security measures in organizations. Unfortunately, they mainly focus on providing sets of controls. The selection of controls is discussed, but the measurement of the quality and applicability of these controls is not handled in detail. Moreover, the evaluation of security as an overall measure is not dealt with at all. Thus, best-practice approaches are not suitable for an overall security metric.
- **Baseline protection** (especially the German baseline protection manual [5]): The baseline protection manual contains standard security safeguards, which are applicable to virtually every IT system providing basic security.

  An IT baseline protection analysis is carried out by accomplishing the following steps:

  - The structure of the existing IT assets is analyzed
  - Adequate protection requirements for information and IT assets used is identified
  - Assets are modeled with the help of existing modules of the IT baseline protection manual
  - A test plan is established using a target versus actual comparison

  A certificate aligning with this manual allows saying whether an organization has implemented the needed IT baseline protection standard security safeguards. The certificate can be awarded if an audit [4] is successfully performed. The audit mainly relies upon the documented results of the four steps mentioned above. Criteria are given to check the adequacy of the documentation, for example:

  - Comprehensiveness of the analysis of existing IT
  - Plausibility of defined protection requirements
  - Conceivability of the model of the IT system

Auditor's judgment is the basis for the decision whether the regarded object of investigation fulfils the discussed requirements and, thus, awarding an IT baseline protection certificate is acceptable.

The main problem about this measurement approach is that security of the entire organization is rather guessed. Only single aspects, which are usually much easier to evaluate, are assessed rather objectively.

- **Vulnerability analysis** (e.g. Microsoft Baseline Security Analyzer [13] and insecurity's Benchmarking Tool [7]): These tools search the system for vulnerabilities like

  - Missing security updates
  - Trivial passwords
  - Bad security settings

  In summary, vulnerability analyzers give a quick overview of the security status of networked systems. Nevertheless, the number of successful attacks does not depend on the number of vulnerabilities. There are other influences like number and type of installed controls, making vulnerabilities more or less likely to be exploited. Moreover, vulnerability analyzers can not be used to assess security of an entire organization because possible damages as the result of vulnerabilities are not regarded during the measurement. Thus, vulnerability analyzers are useful to get a first impression about the security of IT systems, but assessment of all security aspects an organization is faced to is not possible.
- **Penetration test** (e.g. [16], [9]): Experts attack the system to investigate – without causing real damage to the systems. Even if the results are more comprehensive as a vulnerability analysis, it is focused on single aspects and does not cover the overall security of an organization.
- **Risk management** (e.g. [8], [15]): Main part of risk assessment approaches is the assessment of the security in single scenarios. Even if there is some difference between the approaches, the general principle is always the same. In the following, we will explain the primary working principle on the example of NIST SP 800-30 [15]:

  For the calculation of severity of single scenarios, threat likelihood and threat impact are taken as input. Both are assessed on a scale with 3 units: 1.0 for high, 0.5 for medium, and 0.1 for low likelihood, 100 for high, 50 for medium, and 10 for low impact.

  The product of these two factors along with the predefined thresholds for the product determines the resulting risk level. Evaluation of risk levels is also possible with a risk level matrix provided in NIST SP 800-30.

  In conclusion, risk assessment approaches provide a good overview about the threats of an organization and, even if the approach is not very detailed, it is a good starting point.

An additional approach to be mentioned is NIST's metric for IT-security – the NIST SP 800-55 standard [18]. Results of the Williamsburg conference [11] have influenced it to some extend. NIST SP 800-55 is probably the first standard in this field.

The primary working principle is the adaptation of appropriate indicators to stakeholders needs. The document

- describes the roles and responsibilities of the agency staff that have a direct interest in the success of the IT security program,
- provides guidance on the background and definition of security metrics, the benefits of the implementation etc.,
- presents an approach and a process for the development of useful IT security metrics, and
- discusses those factors that can affect the technical implementation of a security metrics program.

The main problem is its lack of a concrete definition of the measurement execution (even if it is called a metric) and a try to make results more objective. Thus, the NIST SP 800-55 standard is not useful for the metric.

In addition to all standards and models presented above, there are approaches like [10] which present models for some aspects of security. However, these models are rather directed to an analytically exact description of aspects of security and not to a comprehensive assessment and, therefore, they are not of interest for our novel approach.

4. Fundamentals and Integration of the Metric

4.1. Integration into the management cycle

As the metric shall be directly applicable in any organization, it is necessary to deal with integration of the metric into the management cycle of the organization. Generally, there are two directions of exchange: On the one hand, data already available in the Information Security Management System (ISMS) can be used for the metric. On the other hand, the metric can support the decision process and, therefore, one can make use of it within the ISMS.

Moreover, administrative work is necessary to carry out the metric, for example:

- **Operability of and integration with the ISMS**: It must be checked that efficiency of controls is assured and that controls are capable of enabling prompt detection of and response to security incidents.
- **Responsibilities**: Responsibilities for the metric program have to be assigned, e.g. who is responsible for the assessment, who decides which business units to measure.
- **Documentation**: Policies have to be defined where and how to document assessment meetings, decisions, results of the assessment etc.
- **Resource management**: Policies have to be defined who assigns the resources, how one can complain about insufficient resources etc.
- **Policies for reviews, audits, and checks**: Policies shall be defined to advise who shall take part in review, audit, and check meetings and when to conduct these meetings.

Even if the following description of the metric seems like a one-time proceeding, the evaluation of the security metric is a continuous process. The Plan-Do-Check-Act (PDCA) cycle, as suggested in BS 7799-2 and the according ISO standard currently being under development, is the reference model used in this approach. Fig 2 illustrates this cycle that works as follows:

- **Plan phase**, the integration with the ISMS is established and the objects to measure are identified
- **Do phase**, the actual implementation of the security metric is carried out
- **Check phase**, results are monitored and reviewed
- **Act phase**, discovered improvements are implemented

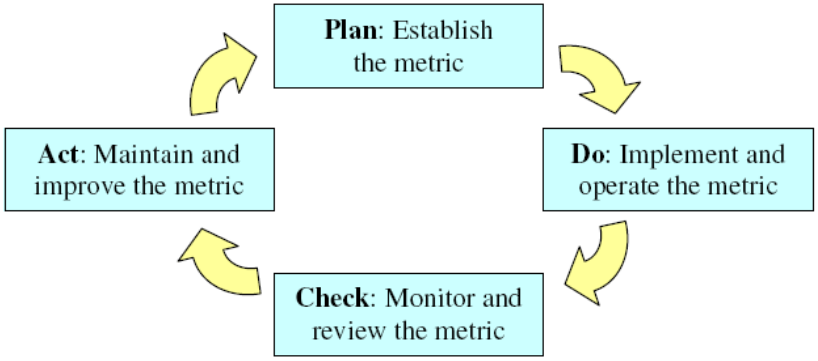

Fig 2. Management cycle

4.2. Basic indicator for security

As described, none of the approaches above allows assessing the overall organization's information security. The most important problem seems to be the lack of an appropriate basic indicator allowing security expression of an entire organization.

A good starting point for this basic indicator seems to be the intuitive understanding of security. According to this, total security is reached if nothing is lost (over a long period of time). Moreover, an organization is regarded more secure than another if it possesses the same set of assets but lost less than a competitor. It is also regarded to be more secure if it possesses more assets but has lost the same.

Incorporating these aspects into one single formula, the indicator S for security of an organization can be calculated by

S = 100% - [percentage of lost assets]

This basic indicator is time-dependent. This means that it will be different if different time periods are analyzed. One year seems to be an appropriate period of time for security evaluations, but generally every other value may be taken from the concept level.

As the term “percentage of lost assets” and the example given above suggest, the basic indicator is based on incidents. Thus, the losses of incidents are counted and summarized.

Finally it shall be mentioned that S might possibly be negative. However, this indicates that more than assets available are expected to be lost during the given period of time. This is theoretically possible as assets can be repaired. However, it is probably unbearable for an organization, thus in reality it is rather unrealistic to occur.

4.3. Structure of security measurement

Some important basics for the metric were described before. In the next step, the general structure of the security metric is described. As previously shown, the only reasonable procedure to measure the security of an entire organization is risk management. While the assessment schema is imprecise, its incorporated approach of modeling threats to an organization using scenarios is a common and very useful approach.

Using the scenario technique, all incidents and attacks an organization is faced to are modeled in different scenarios. For each scenario, single adverse conditions along with their reasons, their “way of propagation” (for example the vulnerabilities that are exploited), and their consequences are listed. Therefore, a scenario contains a complete description of an incident or an attack. Examples are incidents like fire and flood but also attacks like spams or network attacks.

For the metric approach, this scenario technique is used as a basis. It is extended by the integration of security incident data and a combining assessment.

As a result, the following steps to evaluate the metric can be distinguished:

1. Identification of scenarios to model the risks of an organization.
2. Assessment of the single scenarios.
3. Combination of the scenarios to indicators for the entire organization.

Single aspects will be described in more detail in the next section.

5. A Metric for Information Security

5.1. Identification of single scenarios and assigning of values

In the first step of security assessment, all relevant scenarios are identified. For that, all threats, vulnerabilities, and possible damages of an organization are regarded. The resulting scenarios which are possibly occurring (like viruses, fire, theft etc.) are listed. Making identification easier, a generic list of scenarios is provided. It can be taken as a starting point for modeling scenarios of an organization.

Before assessment of scenarios can start, it is necessary to assign assets a monetary value to be able to add different types of assets. But one monetary value is not sufficient as there are different aspects (dimensions) of security. For example, confidential data is stored on a special computer which is needed in the production line of an organization. If the computer is physically damaged, availability of the computer is lost but confidentiality is not addressed. Depending on the integration into the business process and on data stored on the computer, this damage might cost more or less than a loss of confidentiality of data.

Thus, different dimensions of security are necessary. According to related work, e.g. [20], [8], [6], and [17], security dimensions are availability, confidentiality, and integrity. However, these three dimensions are enriched by a fourth dimension, financial resources. It became necessary to model also losses which do neither refer to availability, confidently, and integrity. Examples are basic physical devices which just have to be replaced if damaged. Even if it is highly recommended to take these four dimensions of security, the metric is principally open to additional (or less) dimensions.

5.2. Assessment of single scenarios

Assessment of single scenarios is the second step of the metric. During this step, the rate of occurrence of each scenario on its own is assessed. Additionally, the average number of damages in the four dimensions availability, confidentiality, integrity, and financial resources are assessed. All together, 5 values have to be assessed: the rate of occurrence and the damage in each of the four dimensions. These five values are the basis for the assessment of the security of an entire organization.

Rules for the assessment of scenarios are rather abstract. Assessment staff may use data measured on the system itself, e.g. number and damage of spam mails.

In this case, it must be guaranteed, that all incidents are reported. If no adequate values can be measured on the system itself, data from insurers or other data sources may be taken and positive or negative influences are modeled accordingly. In this case, all influences are written down in an informal way in the first step. These influences cover for example

- The strength of the attacker
- Installed controls
- Specific context making incidents and attacks more or less likely
- Training of personnel

Afterwards, the losses, expressed in monetary values, are calculated. At least, if values of insurers are taken and additional influences are modeled, objectivity can probably not reach 100%. Nevertheless, the scenarios cover rather small pieces of the context of the organization. Therefore, it can be assumed that professionals are able to assess influence of controls and context in quite a good manner. Yet, it must be admitted that measuring number of occurred incidents is a much better way to assess values.

5.3. Combination of results

Probably the most important aspect of the metric is the combination of the scenario assessment to an assessment of the overall security of an entire organization.

The basic “indicator of security” presented above can be seen as an expectation of the security, being 100% minus the expected percent of lost assets. Calculating this value is rather easy: the sum of available assets can be calculated by summing up all assets belonging to the business unit under measurement. The expected loss is the sum of the expected losses of the singles scenarios. As the occurrence of single scenarios can be modeled with Poisson processes, the expected damage of one scenario is the product of the average damage times the rate of occurrence.

This single value gives a first impression on information security, but it is not sufficient to tell something about the distribution of the damage over the years. In other words, it does not say whether security varies between “very good” and “very bad” or whether there are only minor differences. Additionally, it does not tell something about scenarios that are leading to very big damages on their own. Therefore, two additional indicators are necessary: on the one hand, the distribution of the security over the time and, on the other hand, an indicator telling something about the occurrence of very big damages. These two distributions are the “likely security” and the “minimum security”:

- **Likely security** is the probability that at least a given security is reached (being equal to the probability that a given percentage of loss is not exceeded). This value is good for getting an impression about the expected distribution of the information security over the time.

  For its analytically correct calculation, all combinations of scenario occurrences are listed that do not exceed a given percentage of loss. The probability that at least a given security is reached is the probability that any of these combinations occurs.

  However, the complexity of calculating likely security is very high. Thus, an approximation is highly recommended instead.
- **Minimum security** is the probability, that no scenario occurs, which (on its own) leads to a security less than a given threshold. This value is equal to the probability that no scenario occurs which leads to a loss bigger than a given percentage of assets. This indicator helps to recognize probability of occurrence of very big incidents.

  For calculation, all scenarios which would exceed the allowed loss are listed in a first step. Afterwards, the probability that none of these scenarios occurs, is calculated.

It should be mentioned that these three indicators are calculated for each dimension of security (availability, confidentiality, integrity, and financial resources) on its own. Thus, for calculation of the security in dimension availability, the sum of all the values of all assets in dimension availability is taken. For the damages, the damage of the scenarios in the dimension availability is taken.

5.4. Reusability of values

In some cases, it is useful to reuse results of security assessment of organizations. For example, some big organizations may want to assess security of the entire organization based on the results of single units. Other organizations may want to incorporate results of their outsourcer’s assessment into their own security assessment. For these cases, we suggest procedures to incorporate results in other assessments.

If independence of business units can be assumed, knowledge about the used scenarios is not necessary. The results of the assessment are sufficient. These results are taken over into one scenario. This scenario stands as a replacement for the unit that is modeled by the scenario.

If business units are not independent (e.g. two units of the same organization, cited in the same building and connected to the same computer center) this procedure can not be applied. Instead, scenarios of both units have to be combined.

In both cases, it is important to ensure a fitting scope. In detail, this means that only functionality which has similar protection may be taken into consideration. A negative example would be sourcing out highly confidential data to a company that usually deals with web servers which do not contain confidential data.

6. Evaluation and Discussion

The feasibility of the proposed metric was evaluated by its application to in a small unit of our university. Some results of this evaluation are presented in this section, starting with some information about the unit under measurement Afterwards, evaluation results and a discussion of the meaning are presented.

6.1. Background of the unit under measurement

About 30 people are employed by the organization under measurement. It is responsible for research and teaching in a specific field of computer science.

A few aspects of the security of the organization shall be mentioned to get a rough understanding:

Physical theft of assets is supposed to be higher than the average value as students have the possibility to enter the building also during non-opening hours.

Due to experiences of the responsible administrator, intentional network attacks on availability, confidentiality, and integrity are supposed to be somehow less and of lower severity than in other organizations.

Availability of telephone, Internet, clients, and the server needs not be high as work to perform is not time critical and not Internet- or computer-centric.

Much source-code and self-written programs are available, being an important part of the organization. It is not a serious problem if programs or code are not available for a few hours. If data is damaged, very much effort is necessary to rebuild software.

Operating system's version is very old on some computers, because programs do not run on newer versions. Unfortunately, patches are not available any more for these old systems. Being included into daily work, these computers are assigned the same authorization on the network as patched systems.

All computers have complete reading access to the whole network. Thus, intruders have the possibility to easily access data using single compromised systems.

In summary it can be said, that this sample organization appears as a very common company facing the same threats and having the same security problems.

6.2. Results of the "expectation" indicator

During evaluation, altogether 19 scenarios were selected and afterwards assessed using the procedure described above. Scenarios assessed were for example *unauthorized access*, *internal attacks over the network* etc. The total process of selecting scenarios and assessment lasted about four hours.

The results of the security assessment are presented in the following, starting with the expectation of the information security as shown in Table 1.

Availability	Confidentiality	Integrity	Financial resources
93.59%	28.81%	86.34%	96.84%

Table 1: Calculated expectation of security

To give an example, the value of 93.59% for availability means that 93.59% of assets will not be damaged during one year and all other assets will be completely damaged. This value is an average value over the years, thus actual damage can differ. Nevertheless, it provides a first impression about security.

Comparing assessment results with the background of the organization under measurement (see section 6.1), the achieved results meet our expectations. Due to reading access on the whole network and unpatched systems, it is very easy for an attacker to access confidential data. Thus, an expectation of about 29% in dimension confidentiality is an adequate value.

Integrity is better as confidentiality but also rather low. Only in about 86% of security is reached. This value corresponds to the number of unpatched systems, but due to no permission to alter data on network its influence is not that dramatic.

6.3. Results of the "likely security" indicator

Likely security, the probability that at least a given security threshold is reached, contains a little bit more information than the expectation. We will not present all results individually but rather summarizing the results in a graphical representation as shown in Fig 3.

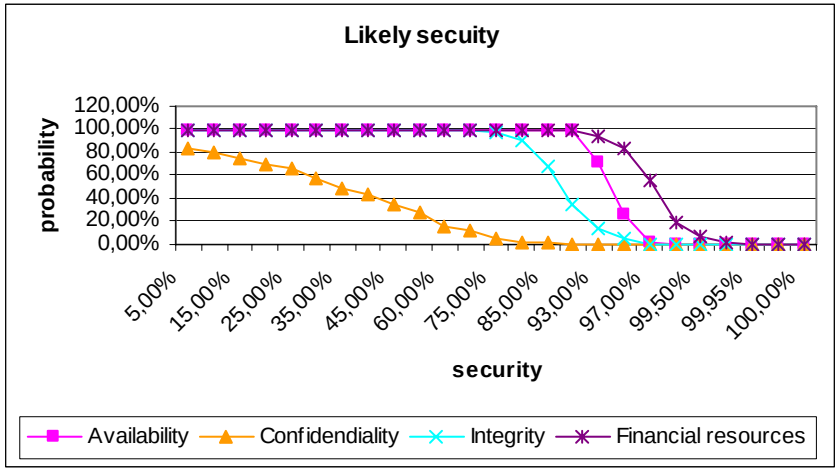

Fig 3. Graphical representation of likely security

Again, we want to give an example on the meaning of these results: as one can read out of the diagram, the probability that security in dimension availability is at least 93% is in about 0.72. This means that a loss of 100%-93% = 7% of assets or even less will occur most years (72 out of 100).

Likely security underlines the bad performance of confidentiality already mentioned in section 6.2. For example, it tells that at least 50% security is reached only every third time (approx. 30%).

For dimensions availability and financial resources, the likely security diagram also provides important information. It tells that the security results in these dimensions are unlikely to fall below 90%. Again these results are a refinement of the "expectation" results presented in section 6.2.

6.4. Results of the "minimum security" indicator

Moreover we want to present the results of minimum security, the probability that no scenario occurs, which – on its own – leads to a security less than a given threshold.

For better understanding of the diagram as depicted in Fig 4, we want to discuss an example here as well. The 93% security threshold in dimension integrity shall be taken for this. The calculated probability is in about 90% as one can see in the diagram. This means, that the probability that no scenario occurs, which leads to a damage of at least 100%-93% = 7%, is 90%.

Even if minimum security seems much better than likely security on first sight, it is not. Recapping the meaning of this indicator, confidentiality is not good because a loss of 10% or 15% of assets (security: 90% or 85%) in only one incident is still a big problem.

Results for availability and financial resources are quite good in this case. This is due to the low and not severe number of losses in both dimensions.

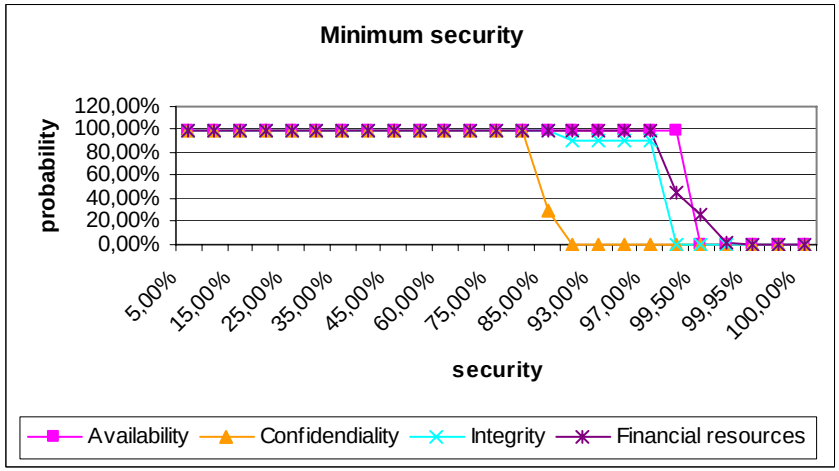

Fig 4. Graphical representation of minimum security

6.5. Discussion of the results and in comparison to the requirements

In the preceding sections, security results were discussed. In this section, we want to show that requirements stated above can be fulfilled within the presented security metric. Therefore, we compare results with the requirements stated in section 2:

- **Comprehensive assessment of the whole organization** is possible within this metric. The only requirement is that all possible incidents targeting the organization are modeled, but that has not evolved as a problem during evaluation. The combination process summarizes the results of the single aspects to a security assessment of the entire organization and, thus, a comprehensive assessment of the whole organization is possible.
- **Objectivity** in terms of (possibly different) security experts achieving similar security results under similar conditions can be reached, at least better than existing approaches can afford. For example the baseline protection manual [4] – which is the only real comprehensive and objective measurement of information security at the moment – requires a rather subjective assessment of the organization's security as a whole. Only smaller units are assessed with rather objective methods. Moreover the NIST SP 800-55 [18] approach does not even try to achieve objective results. Within the approach presented in this paper, assessment experts have on a maximum to assess strictly separated, small areas. Assessing small areas is easier and more objective because influences can be assessed easier and there is usually supporting material to make decisions more objective. Thus, objectivity can at least be reached better as with current approaches.
- **Comparability** was not possible to be investigated in depth. Comparing security under different conditions was possible. For example it was possible to show that additional controls lead to additional security. Moreover the general structure of the indicator allows comparison. Therefore, we can conclude that comparability was achieved.

7. Conclusion and Further Work

The aim of research was the establishment of a metric allowing the comprehensive assessment of an entire organization. Moreover it was requested that objectivity and comparability of metric results can be reached. As a result, a top down approach for the measurement was chosen. First, a suitable basic indicator to fulfill these requirements was designed. Afterwards, a procedure was developed, allowing to combine single aspects of security to indicators for the entire organization – based on the basic indicator. Besides an expectation indicator, giving a rough overview on the security, two distributions are calculated – one concerning the distribution of damages and one concerning the severity of incidents.

Combination is mainly based on scenario technique, which is already known from risk assessment and risk management and extends these approaches. Therefore, not only attacks but also incidents can be taken into consideration for security assessment.

The metric developed fulfills the primary goals stated in section 2. Most important, the metric comprehensively measures the overall security of an organization, not limiting to single aspects like attacks but measuring all influences – including incidents – on the entire organization. Additionally, the approach provides the most objective security assessment of organizations compared to the literature. Finally, the individual security indicators, based on the basic indicator, provide a comparability of the security at different times and between different organizations.

The evaluation of a small university department underlined these results. Moreover, it illustrated that modeling of scenarios and assessment was easily and intuitively to understand and to accomplish for the assessment staff.

In conclusion it can be said that the metric is the first approach to comprehensively and comparably measure security of organizations. It is a first step for measuring an organizations' information security. Its importance is underlined by the fact that the approach will be incorporated into the ISO standard ISO/IEC 27004, a metric for information security.

Nevertheless, the approach is only a starting point for security metrics. Especially measurement of single aspects has not been dealt with in detail but is very important for an objective measurement. Thus, further research work will be directed to these aspects. For example, the questions shall be answered how specific controls influence scenarios and aspects like logical theft of data can be measured.

References

[1] Basel Committee on Banking Supervision. *Working Paper on the Regulatory Treatment of Operational Risk*. Bank for international settlements, 2001.

[2] British Standard Institute (publisher). *Information Security Management. Specification for Information Security Management Systems (BS 7799-2)*. British Standard Institute, London, 1999.

[3] British Standard Institute (publisher). *Information Security Management. Code of Practice for Information Security Management. (BS 7799-1)*. British Standard Institute, London, 1999.

[4] Bundesamt für Sicherheit in der Informationstechnik (publisher). *Qualifizierung/Zertifizierung nach IT-Grundschutz – Prüfschema für Auditoren.* Bundesamt für Sicherheit in der Informationstechnik, Bonn, 2003.

[5] Bundesamt für Sicherheit in der Informationstechnik (publisher). *IT Baseline protection manual*. Bundesamt für Sicherheit in der Informationstechnik, Bonn, 2004.

[6] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation.* Common Criteria Project Sponsoring Organizations, 1999.

[7] The center for internet security (cisecurity). *Homepage at http://www.cisecurity.com/* . The center for internet security (cisecurity), 2005.

[8] Club de la securite des systemes d´information francais (publisher): *Mehari*. Club de la securite des systemes d´information francais, Paris, 2000.

[9] Corsaire Limited. *Penetration Testing Guide: http://www.penetration-testing.com/* . Corsaire Limited, 2004.

[10] Felix C. Gärtner. *Byzantine Failures and Security: Arbitrary is not (always) Random.* Swiss Federal Institute of Technology (EPFL), Lausanne, 2003.

[11] Ronda Henning (workshop chair). *Workshop on Information Security System Scoring and Ranking.* Applied Computer Security Associates, 2002.

[12] ISO/IEC. *Information technology – Security techniques – Code of practice for information security m*anagement (final draft). ISO, 2005.

[13] Microsoft Corporation. *Microsoft Baseline Security Analyzer V1.2.1*. Microsoft Corporation, 2005

[14] Ron Ross, Stu Katzke, Arnold Johnson, Marianne Swanson, Gary Stoneburner, George Rogers, and Annabelle Lee. *Recommended Security Controls for Federal Information Systems (Final public draft; NIST SP 800-53)*. National Institute of Standards and Technology Gaithersburg, 2005.

[15] Gary Stoneburner, Alice Goguen, and Alexis Feringa. *Risk Management Guide for Information Technology Systems (NIST SP 800-30).* National Institute of Standards and Technology, Gaithersburg, 2002.

[16] David A. Shinberg: A Management Guide to Penetration Testing, 2003.

[17] Stuart. E. Schechter. *Computer Security Strength & Risk: A Quantitative Approach (thesis)*. Harvard University, Cambridge, 2004.

[18] Marianne Swanson, Nadya Bartol, John Sabato, Joan Hash, and Laurie Graffo. *Security Metrics Guide for Information Technology Systems (NIST SP 800-55)*. National Institute of Standards and Technology, Gaithersburg, 2003.

[19] Dean Turner, Stephen Entwisle, Oliver Friedrichs, David Ahmad, Daniel Hanson, Marc Fossi, Sarah Gordon, Peter Szor, Eric Chien, David Cowings, Dylan Morss, and Brad Bradley. *Symantec Internet Security Threat Report Trends for July 04–December 04*. Symantec Corporation, 2005.

[20] Susan Zevin (Acting Director). *Standards for Security Categorization of Federal Information and Information Systems (FIPS PUB 199).* National Institute of Standards and Technology, Gaithersburg, 2003.