The First Step in Improving Security Awareness: A Simple Self-assessment Framework

Suleyman Kondakci

***Abstract*—Enterprise management is often unable to estimate the crucial impact of unprotected or loosely protected information assets. The management must have an overall picture of the current status of their information security program and controls in order to make the appropriate judgments and investments, which will mitigate risks to an acceptable level. If security test and evaluation procedures and processes make it possible to illustrate the difference between the risks of protected and unprotected information assets, then the management will more easily be persuaded to support information security planning as a high priority long term task for the company. We present a simple yet efficient approach to help network/security administrators improve security awareness for their management and users. The approach relies on a process-based self-assessment method.**

***Index Terms*—Information assurance, quantitative risk assessment, security management.**

I. I Introduction

Security, in general, is a matter of human actions. In a sense, we are blindfolded because we observe and react to the technological matters without recognizing that the entire process is fundamentally dependent on humans. We should distance ourselves from unreliable intuitions about the essential aspects of the severity of security risks. For the majority of companies security evaluation is considered as the last step in the process of lifecycle security planning. A remarkably high proportion of management will merely trust a firewall and ignore the test and evaluation issues. Our observation of several leadership companies shows that security administrators have serious difficulties in convincing their managements about security risks and threats against them. Many network/security administrators lack the ability to explain/demonstrate the impact of security risks. There is a real need for a way of explaining the seriousness of the damage external and internal threats can cause.

Therefore, we have developed a simple and inexpensive method, which allows administrators to illustrate the difference between risk-impact figures in protected and unprotected networks. In short, this covers the following areas:

- System administrators who have difficulties in explaining the real impact.
- The cost of lack of awareness.
- The lack of necessary measures and methods needed to demonstrate to the management the level of impact.
- The tendency for most network owners to be easily manipulated by external and internal marketing behaviors and, as consequence, the purchase and deployment of tools and services that may not be necessary.
- These tools may provide more complicated services than the company needs, or may operate at a maximum complexity and thus cause diminished performance in the services the company is supposed to provide for its consumers.
- This attitude affects the balance of the security solutions to a great degree.

Why a balanced protection is required must be clear to the company management. An unnecessarily equipped network is not always the most secure network, although it may be the most expensive and inefficient one.

Security *objectives* and *policies* are the key factors that lead to security implementation of varying qualities. First of all, a *security policy* is a preventative means of protecting company assets. It communicates a coherent security standard to users, management, security staff, customers, collaborators, and evaluators.

The specification of the security objectives and policies are related to human actions, which are hard to control by means other than human intervention. For this reason, a careful evaluation of the objectives, can indeed, determine the overall procedural security for organizations. Because, the knowledge (objective) of organizations is a fundamental criterion for proper evaluations of overall technical abilities. We can run formalized assessment of the knowledge of an organization by evaluating the objectives of the organization. That is, security objectives cover the basic knowledge of the organization (what to protect, what is security and its importance); overall IT infrastructure, the entire environment, and the assets needed to match business requirements. Different knowledge levels may lead to different

Suleyman Kondakci, *Faculty of Computer Sciences, Izmir University of Economics*

policy definitions. Obviously, different policy definitions may also lead to different security solutions.

II. PROCESS-BASED ASSESSMENT FRAMEWORK

The proposed assessment technique is guided by a process-based risk assessment and problem identification framework. The framework utilizes one basic questionnaire containing specific control objectives and techniques to determine the current status of the security program for the assets that can be tested and measured. In the early stages, the guide does not establish new security requirements. However, if there is a lack of necessary protection mechanisms, the administrator should establish a set of new security requirements, and hence provide a security design as a part of the self-assessment process. The control objectives and techniques are abstracted directly from long-standing requirements found in statute, policy, and guidance on security.

What the problems are and how we identify them is not a trivial task. However, we can simply create various scenarios to demonstrate whether a system is protected or not and, the security administrator/staff should then be able to present any problem in a simple and non-confrontational manner in order to convince the management. These scenarios of a self-assessment must be presented by the security staff, or if available, by security test and evaluation facilities.

We present here a self-assessment process that provides a method for management to determine the current status of their information security programs and, where necessary, establish a target for improvement. The self-assessment method shown in Fig.1 contains the following elements and operations. The operations which need further explanations are as follows:

- Presentation of different scenarios with different security solutions and risk levels.
- Illustration of unprotected risk-impact figures.
- Illustration of protected risk-impact figures.
- Demonstration of the difference and severity with varying risk levels.
- Presentation of real-life survey results.

A. *Roadmap for Evaluators: The Self-Assessment approach*

This approach (shown in Fig. 1) builds on the presentation of different scenarios and sample security solutions to show the severity of the risk-impact figures.

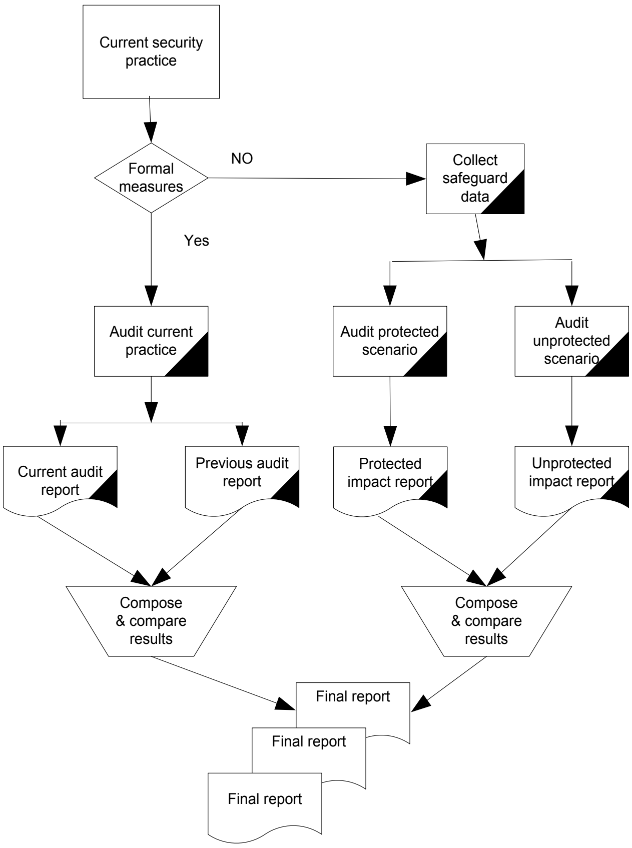

Fig. 1. A flow diagram of the test and evaluation process for evaluators.

The scenarios contain samples of networks with realistic assets of various importance. For the sample network, the following tasks need to be performed:

- The calculation of unprotected overall risk.
- The calculation of protected overall risk.
- The illustration of results of the calculation, preferably in the form of a graph.

Further, we must define a set of measures that form the security plan for the company. The plan should contain at least the following:

- Security policy and implementation.
- Security administration procedure.
- Periodic auditing and risk assessment.
- Staff and user training.
- Incident response procedure.
- Lifecycle security plan.

The most distinctive feature of this approach is that it can run two separate tests if needed. Prior to the tests, the company policy is analyzed in order to collect data on the current security implementation. If a security implementation is found then it will be evaluated. If the company has no security implementation and relies on ad hoc safeguards, the safeguard information will be collected and evaluated. In the first case, previous evaluation results and the current results are used to calculate and illustrate risk-impact figures. In the latter case, the evaluator will probably face the challenge of illustrating the difference between protected and unprotected scenarios. The evaluation of protected and unprotected scenarios should be performed, if necessary, by running a simulation program, using the most precise real-life values possible. The accuracy of the calculated risk levels is important since it will be used to convince the management of the importance of the encountered impact.

B. *Quantitative Risk Estimation*

A variety of valuable sources presenting assessment and quantification methods are given in [1]. We apply here a simple weighted averaging (shortly scoring) scheme consisting of a list of scored security items.

We use four subranges and a master scale of scores varying between 0 and 5. This scoring system is simple and practical although different subranging (e.g., 10 subranges) and scaling (e.g., 0 to 100) could probably provide a finer dynamic range. Thus, when measuring risks, we can use any of the scales shown below:

0 <= score <= 1.25	(or 0 <= score <= 25)	→ weak,
1.25 < score <= 2.5	(or 25 < score <= 50)	→ moderate,
2.5 < score <= 3.75	(or 50 < score <= 75)	→ severe,
3.75 < score <= 5.0	(or 75 < score <= 100)	→ very severe.

For strength evaluation we can use the above scheme. Interchanging the use of the two schemes is possible. For example, to evaluate the strength of a virus, it is more appropriate to use the term *strong* instead of *severe* and keep using the terms *weak* and *moderate* as well. To evaluate weaknesses *weak, moderate, severe*, and *very severe* terms are used to indicate four different evaluation levels.

By applying a simple weighted assessment and decision-making algorithm on alternative sets of security objective attributes, the evaluator can readily obtain results showing different potential losses (impacts) or advantages of various alternative solutions. The decision results, in turn, lead to different security policies, and hence different countermeasures are obtained. The use of the scoring scheme in decision-making needs further justification. As explained above, the entire scale of a measurement is divided into four subranges, weak, moderate, severe, and very severe. The results of the evaluation are matched to a subrange in order to quantify the evaluator's judgment and obtain a final decision. That is, the evaluation process produces quantitative values varying between 0 and 5, or optionally, between 0 and 100.

In a security planning process, we need to assess the risks in each phase in order to minimize the propagation of weaknesses in subsequent phases. In due course, a simple metric is needed to quantify and classify the assessment results to determine the degree (weak, moderate, severe, and very severe) of the weaknesses. For strength assessment we use weak, moderate, strong, and very strong evaluation levels. If a strength assessment results in the subrange of weak we can terminate the process and iterate with a new solution in order to produce a result within moderate, strong, or very strong, as required.

Each asset has an attribute ID describing an asset, an asset value describing the weight of the asset, and a list of items representing evaluation scores of the corresponding asset. Theoretically, an asset can also represent a single security attribute or an entire system containing several attributes. It can, thus, represent a security objectives attribute, a security policy attribute, or attributes of an operational system (e.g., a firewall, database server, and a web-service) under evaluation.

During the risk assessment, we build tables that contain the necessary threat information and asset values (weights) to calculate a scalar risk value for each asset (see, for example, Table I).

An asset value can be thought of as the importance of the asset that describes the level of security classification for the asset. That is, an asset with a higher value when compromised by an attacker will denote a higher risk level. A target of Evaluation (TOE) [2] describes an asset that is under evaluation. To calculate risk values for a given TOE, the table must contain values related to the given vulnerability-success degree of a related attack on the TOE. This vulnerability-success degree is determined by use of prior probability distribution models, [3] and [4].

TABLE I

THREAT-SUCCESS TABLE FOR AN ASSET FACING DIFFERENT THREATS

Vulnerability/Threat /Attack	Unprotected A(w).P(s)	Protected A(w).P(s)
Tribe Flood	5x0.7	5x0.5
MAC Spoof	5.05	5x0.2
Firewalking	5x0.1	5x0.1
Viral infection	5x0.6	5x0.3
Overall	9.5	5.5

The actual values shown in Table I depend on the degree of success of an attack and the effective vulnerability of the system being attacked.

These values are computed for an unsecured asset that is neither equipped with countermeasures (CM) nor has a defined security policy. Therefore, we need to define the necessary policy, and set up appropriate countermeasures in order to minimize the risk factors. In the cases of both protected and unprotected assets, we need to cerate test scenarios and run them in turn. This process will result in risk values that are stored in tables for further risk-impact calculations. Using the following scalar computations by use of Equation (1), we obtain scalar risk values for both unprotected and protected TOEs respectively. The scalar risk value of asset ***j***, $R\{U \vee P\}_j$, is given as

$$R\{U \vee P\}_j = \sum_{i=1}^{i=N} A(w)_j \cdot P(s)_i^j . \qquad (1)$$

where $A(w)_j$ represents the asset value and $P(s)_i^j$ represents the likelihood of the success of an attack for a given threat type directed to that asset. During the test, attack successes follow binomial characteristics, which can be expressed as *Bernoulli trials*. In short, the probability of the number of successful attacks, ξ, equal to *r* is

$$P\{\xi = r\} = C_r^n p^r q^{n-r}\ , \quad r = 0,1,\ldots,n. \qquad (2)$$

where *r* is the number of successful attacks, *n - r* is the number of failures . Here, *p* is the probability of attack and *q = (1 – p)* is the probability of failure. Thus, we can state that the initial probabilities of a state for a given node can be obtained either via experiments or analytical means by use of the equations given above.

For example, according to our observations, W32/Nimda worm, [5], has an empirically determined probability model

$$P(n) = 1 - \left(1 + \frac{n}{78.6}\right)^{-0.862} \qquad (3)$$

where,
P = the probability of infection,
n = number of contacts with infected nodes.

The constants are empirically determined varying with the type of the virus. Note that this model is specific to our experiments conducted on a LAN with 500 loosely protected e-mail boxes. As an example, consider a mailbox that has contacted 12 infected mailboxes on the same local area network. The probability of being infected will be 0.115. Increasing the number of infected contacts to 500 may cause the probability to go up to 0.82. In turn, the test results will produce two vectors; one for protected risk values another for unprotected risk values.

$$U = \left[RU_{A_1} \cdots RU_{A_N} \right],$$

$$P = \left[RP_{A_1} \cdots RP_{A_N} \right], \qquad (4)$$

where, ***U*** is the risk vector of unprotected assets, and ***P*** is the risk vector of protected assets. Both risk figures and differences are illustrated by graphical charts to visualize the overall risk figure. This is an efficient way to depict the overall impact, which is often difficult to estimate utilizing qualitative approaches. It is highly probable that most managements are financially motivated, and therefore may be successfully convinced by risk-impact figures supplied by the security administrator. The simple chart in Fig. 2 depicts the results gathered from the evaluation process.

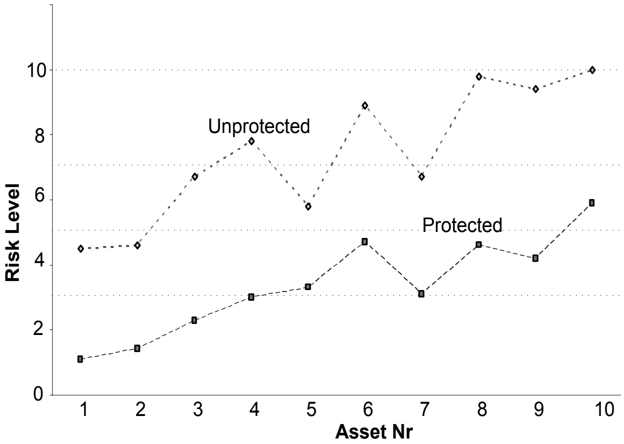

Fig. 2: The difference of protected and unprotected network with 10 assets.

It is important to note that the average value of the risk level for the same protected network is as low as ***4.0*** compared to the unprotected value of ***8.0***. The difference also indicates the fact that risk-impact figures are doubled when the necessary security measures are not implemented.

C. A Special Case

Here we present the scenario of a virus-infected mailbox that causes a serious virus infection throughout the Internet. The simulated scenario shown in Fig. 3 can be evaluated by utilizing realistic worm attacks. The steps of the operation in the simulation will consider the following events:

1) A User Agent (UA), if infected, may spread the virus to every UA in the company network, and perhaps to the entire Internet,

2) A simulation of actual attacks in order to obtain the cost (impact) of the unprotected scenario for the company network.
3) A simulation of a new scenario for a protected set of UAs in order to estimate the impact in a protected environment. Results and impact values can then be processed further to demonstrate the overall risk-impact figure.

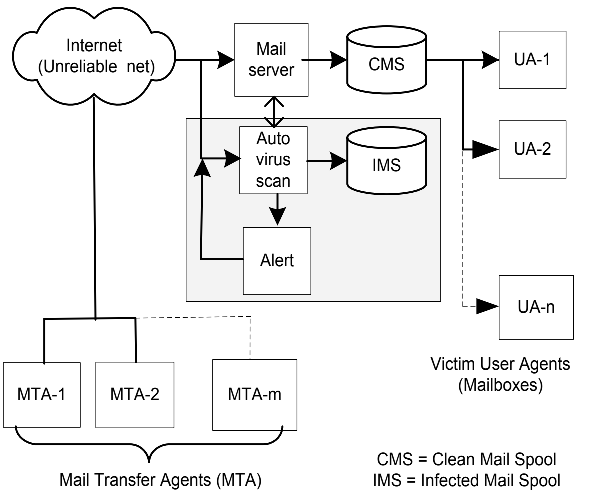

Fig. 3. A Typical architecture of auto-virus scan and quarantine system.

For evaluation purposes, Fig. 3 depicts an environment where the company network is connected to the Internet. It is likely that there are several unreliable Message Transfer Agents (MTAs), which, if infected, will spread the virus to other MTAs and User Agents (UAs) through the Internet. An MTA can be thought of as a mail server, and the UA as the end user mailbox. It should be noted that a virus-infected node can spread the virus to other MTAs and UAs throughout the Internet. However, mailboxes (UAs) are more probing and hence susceptible to viruses and worms. In particular, they have the ability to automatically transfer viruses to all e-mail addresses found in their address books, both locally and globally, so can be more destructive than the MTAs. Such an unprotected UA is a haven for aggressive worm scans that aim to penetrate the entire communication infrastructure and Internet. Hence, the impact is not isolated within the company network but represents a serious threat to all susceptible systems.

Note that the network shown in Fig. 3 can be transformed into a protected one by adding the auto worm-scanning functionality represented by the dashed area in the figure. The self-assessment method will simulate, with higher precision, both of the scenarios (protected and unprotected) to illustrate the serious risk-impact figure. A comparison of protected impact levels and unprotected impact levels clearly demonstrate the realistic security level, helping to improve the viability of the classified assets within the company and the entire Internet.

III. Correlation Between Objectives and Implementations

It is obvious that the success of an effective security implementation is strongly associated with adequately defined security objectives. Here, we will illustrate this by examining the relations between the objective and policy data and between the policy and the final implementation data. Consider a sample evaluation of *n* solutions. We will determine the correlation between the security objectives and policies, and correlation between the security policies and the corresponding implementations. The efficiency of a security implementation depends on the proper definition of the security policy, which is set up humans and prone to human errors. There exist different views of human reliability in engineering and several papers have been published discussing ways to analyze and improve cognitive reliability of human, [6].

For the evaluation of security items we apply a Bernoulli process to determine the entry-level (prior) distributions. Each evaluation produces a set of final evaluation scores. To estimate a distribution from this set we choose a sample set of size *n*, which should be proportionally large enough compared to the overall population size. To reiterate, we have divided the entire measurement scale into four equal intervals (subranges), i.e., *weak = {0,…,25}, moderate = {26,…,50 }, severe (strong) = {51,…,75},* and *very severe (strong)= {76,…,100}*. The Bernoulli trial is also a useful tool for determining the subrange of a given set of security attributes. For example, we can determine whether a security objectives or a policy item is characterized as weak, moderate, or strong. This method is specifically time-efficient when a large network of assets is being evaluated. The idea is similar to quality evaluation of a production line. For this, we do not need to evaluate hundreds of assets but can choose a subset to determine the overall security classification of the large network. As shown in Table II, each security planning process consists of the definition of the objectives, the policies, and the implementation of the final solution.

The assessment uses three sets of evaluation data: one set of objective data, one set of policy data, and one set of implementation data. Each set contains 20 scores; that is, 20 scores from the security objectives (SO), 20 scores from the security policies (SP), and 20 scores from the security measures (SM).

TABLE II

PARTS OF THE EVALUATION SCORES OF 20 SOLUTIONS. THE SOLUTIONS ARE EVALUATED BY THEIR SECURITY OBJECTIVES (SO), SECURITY POLICIES (SP), AND SECURITY MEASURES (SM).

SO	60	16	100	80	60	. . .	76
SP	56	0	100	60	76	. . .	50
SM	950	20	100	44	40	. . .	76

The data values have been obtained by evaluating the strength of each security solution. We choose, first, only objectives from the table (first row) singly and evaluate their objective scores. We will here find the number of evaluations having scores less than or equal to *x* where *x* is defined as $x \le 51$. This range of values represents the scores for the category of *weak* and *moderate*. Then, we select the policy scores of the corresponding entries (second row) and evaluate them to determine whether the objective and policy data correlate. Then, we chose the implementation scores of the corresponding entries (third row) and evaluate them to determine whether the policy and implementation data correlate. Note that, statistically, we repeat the experiment *n* times independently, that is, we evaluate the score of the i*th* solution in i*th* trial, i.e.,

$$\zeta_i = \begin{cases} 1, & X_i \le x \quad i = 1,2,\ldots,n \\ 0, & X_i > x, \quad x \le 51 \end{cases} \tag{5}$$

where X_i denotes the score of the i*th* solution. Obviously, $S_n = \zeta_1 + \cdots + \zeta_n$ is the number of solutions for which the evaluated scores do not exceed the value of *x*. This indicates that we have a Bernoulli trial with the success probability of

$$P \equiv P\{X \le x\} = F(x), \quad 0 \le x \le 1, \tag{6}$$

$$P\{S_n = k\} = C_n^k (F(x))^k (1 - F(x))^{n-k}, \quad for \quad k = 0,1,2,\ldots,n. \tag{7}$$

Thus, the probability that the number of security objectives, *y,* for which the evaluated scores do not exceed the value of *x* is

$$P\{S_n \le y\} = \sum_{k=0}^{y} C_n^k (F(x))^k (1 - F(x))^{n-k} \tag{8}$$

F(x) is a distribution function on [0,1], which is uniformly distributed, i.e.,

$$F(x) = \begin{cases} 0, & x < 0 \\ x, & x \in [0,1] \\ x^2, & x \in [0,1] \\ 1, & x \ge 1, \end{cases} \tag{9}$$

We have earlier determined [4] that security-awareness exhibits the hypergeometric probability distribution, i.e.,

$$\Pr(O \mid P) = \frac{\Pr(O \cap P)}{\Pr(P)} \text{ and } \Pr(M \mid P) = \frac{\Pr(M \cap P)}{\Pr(P)} . \tag{10}$$

In short, the above relationships mean that, the better the security objectives (O), the better the final security measure (M). Determination of these relationships is given in [3]. The quantitative approach given above is specific to success/failure observations, although a variety of approaches have been published in different contexts, e.g., [7]-[11].

Following this theoretical introduction and considering the data from Table II, assume that the probability of a moderate security solution from a set of 20 objectives is empirically determined as 0.48. Based on this and the preceding computations, we can estimate the probability of moderate or strong objectives in a new trial. Thus, for the uniform distribution, the probability ***f(x)*** that 10 moderate or strong objectives will be found in the sample of 20 objectives is *0.17,* and the corresponding cumulative distribution, ***F(x),*** is 0.66. Fig. 4 shows the plots of the functions ***f(x)*** and ***F(x)***.

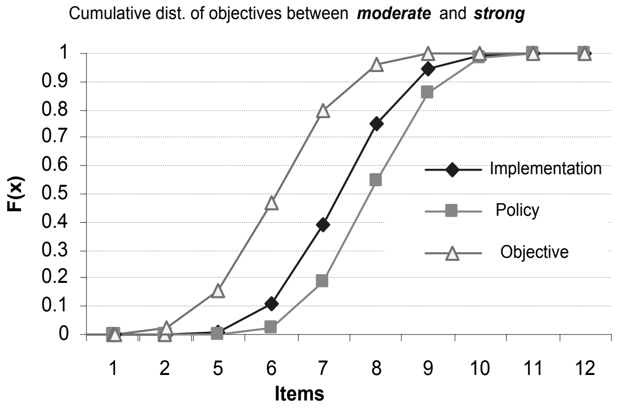

Fig. 4. The cumulative probability functions of moderate or strong objectives and their effects on policies and implementations.

Fig. 5 shows correlations among 20 different policy sets and corresponding security implementations. As shown in the scatter diagram, we have higher correlations between the objective items and policy items. Though the correlation between the policy and implementation items is slight, we can observe the effect of the policy reflected onto the final implementation. In short, we deduce that correct identification of security objectives (security awareness) will lead to efficient policy design and the resulting policy design will always lead to better security implementation.

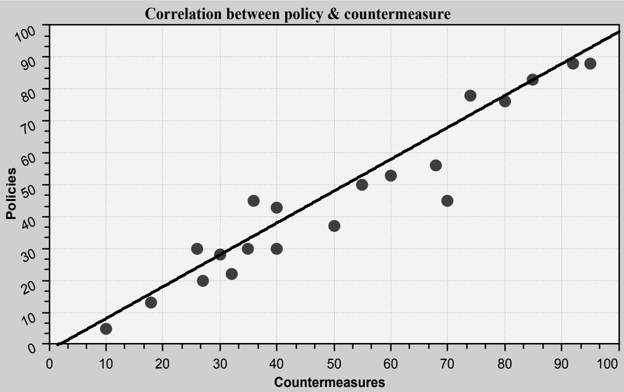

Fig. 5. Correlations among policies and their implementations

IV. CONCLUSIONS

Security in any system should be commensurate with its risks. However, the process of determining which security measures are appropriate and cost effective is frequently a complex and subjective matter.

A process based self-assessment approach is an efficient way to evaluate and demonstrate the vulnerability of the company network in order to increase security-awareness in both users and management. Therefore, third party risk analysis is an essential component in enabling this to be placed onto an objective basis, and thus allowing the risk to be managed effectively.

Besides, it is imperative that organizations understand that the human factor is the root cause of many security incidents and therefore needs particular attention. Therefore, an organizational framework is needed to ensure that, at policy level, end users are instructed and monitored, thus enhancing guidance and discipline when necessary.

V. REFERENCES

[1] R. M. Cooke and L. H. J. Goossens, "Expert judgment elicitation for risk assessments of critical infrastructures", *Jnl of Risk Research, T&F Group*, Vol. 7(6), pp. 643-656, 2004.

[2] *Common Criteria/ISO IS 15408, Version 2.1*, October 1999, http://csrc.nist.gov/cc/ccv20/ccv2list.htm.

[3] S. Kondakci, "A new assessment and improvement model of risk propagation in information security", *International Journal of Information and Computer Security*, Vol.1, No.3, pp. 341-366, 2007.

[4] S. Kondakci, "DARIS: A Probabilistic Model for Dependency Analysis of Risks in Information Security", in *Proc. International Conference on Security of Information and Networks* (SIN 2007), Trafford Publishing, ISBN:978-1-4251-4109-7, 2007, pp. 162-166.

[5] *The CERT Advisory CA-2001-26:* Nimda Worm, http://www.cert.org/advisories/CA-2001-26.html, accessed 2007.

[6] P. Moieni, A. J. Spurgin, A.. Singh, "Advances in human reliability analysis methodology", *Reliability Engineering and Systems Safety*, Vol 44, pg 27-55, Elsevier Science Ltd, 1994.

[7] D. M. Kienzle, W. A. Wulf, "A practical approach to security assessment", Proceedings of the 1997 *New Security Paradigms Workshop*, England, http://citeseer.nj.nec.com/kienzle97practical.html, September 1997.

[8] A. Vorster, L. Labuschagne, "A framework for comparing different information security risk analysis", *in Proc. SAICSIT 2005*, pp. 95-103, 2005.

[9] S. B. Guarro, "Risk analysis and risk management models for information systems security applications", *Reliability Engineering & System Safety*, Vol. 25, No. 2, pp. 109-130, 1989.

[10] G. Bao-Chyuan, L. Chi-Chun, W. Ping, H. Jaw-Shi, "Evaluation of information security related risks of an organization - the application of the multi-criteria decision-making method", in *Proc. of IEEE Annual International Carnahan Conference on Security Technology*, Elsevier Inc., pp. 168-175, 2003.

[11] A. M. Anderson, D. Longley, A. B. Tickle, "Risk data repository: a novel approach to security risk modelling", *IFIP Transactions A: Computer Science and Technology*, No. A-37, pp. 185-194, 1993.