How effective is your security awareness program?

An evaluation methodology.

Konstantinos Rantos
Dept. of Industrial Informatics
Kavala Institute of Technology,
Kavala GR-65404, Greece,
krantos@teikav.edu.gr

Konstantinos Fysarakis, Charalampos Manifavas
Dept. of Applied Informatics & Multimedia
Technological Educational Institute of Crete
Estavromenos, Heraklion, Crete 71500, Greece
fisarakis@epp.teicrete.gr,harryman@epp.teicrete.gr

Abstract

Security awareness is an important element of every security infrastructure since the human factor often proves to be the weakest link. Companies and organisations have developed programs that seek to promote security and enhance users' perception of the importance of exercising security. As raising awareness, however, is an on-going effort, the campaign has to be regularly evaluated so that corrective actions can be taken in order to achieve the best results. This paper addresses the importance of evaluating an organisation's awareness program and provides guidelines and a methodology that will help organisations assess their efforts. The proposed framework includes the evaluation of individual awareness-related processes via respective metrics as well as the aggregation of the aforementioned metrics to produce an overall evaluation score, usable both as a benchmark for future iterations of the evaluation program as well as a figure presentable to higher management.

Keywords
Security awareness; security management; evaluation methodology;

1. Introduction

In the context of an enterprise environment, security awareness refers to the knowledge and attitude employees possess regarding the protection of the physical and information assets of the organisation they work for. Security awareness is a key link in an organisation's security chain, as even the most efficient security mechanisms have little value in an organisation with no security culture. A desk full of confidential papers left over after working hours or computer monitors filled with reminder notes of user passwords are examples of a working environment with no security culture whatsoever; a workplace where employees are completely unaware of the risks pertaining to theft, damage or misuse of the organisation's assets, as well as the relevant safeguards. Even though there is a continuous improvement in the figures that represent the number of employees who receive at least one awareness or training session and, consequently, the budget allocated to said activities, it still represents a small fraction of the security budget. Moreover, a persistent, if not even slightly increasing, percentage of organizations do not engage in personnel awareness training at all, as demonstrated by yearly surveys (CSI/FBI, 2008)(CSI/FBI, 2009)(CSI/FBI, 2010/2011). The same surveys indicate that the majority of the organizations consistently consider the investments made in awareness training as inadequate. It is indeed surprising that awareness measures, which are subjectively evaluated as the most effective by organizations, are in fact applied to a considerably lesser extent compared to other security measures (see Figure 1). In addition, awareness studies are underrepresented within Information Security-related professional publications.

The need for more aggressive programs is sound and sometimes requested by the employees themselves. As (TELUS–Rotman, 2011) indicates, the lack of frequent awareness training has an impact on the organizations' satisfaction with their security posture. Technological advancements and the new behaviours that accompany them (e.g. working in public spaces) have outpaced employee awareness of the new risks they introduce (Deloitte, 2010). Based on all of the above, it comes as no surprise that 27% of the organizations participating in a relevant study (Deloitte, 2011) quote "Information Security Training and Awareness" as one of their top three security initiatives for 2011, preceded only by "Information security regulatory and legislative compliance" (30%) and "Data Protection" (28%).

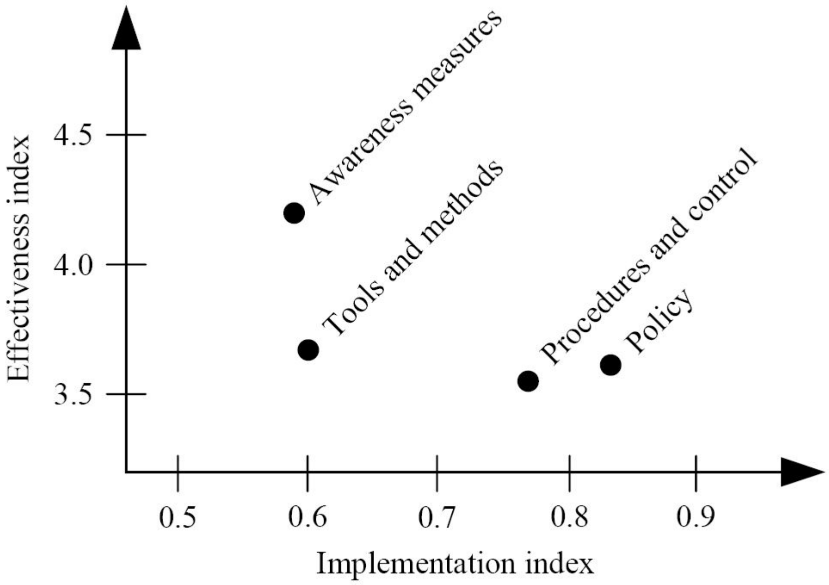

Figure 1. Implementation and effectiveness of organizational information security measures (Janne Merete Hagen E. A., 2008).

An awareness program should be tailored to the organisation's specific needs and environment, i.e. designed based on a needs assessment conducted for this purpose (European Network and Information Security Agency (ENISA), 2010)(National Institute of Standards and Technology (NIST), 2003). However, the effectiveness of the chosen strategy cannot be guaranteed, especially during the first years of program deployment since the campaign is not mature enough. It is therefore imperative for the awareness team to evaluate their efforts and identify weaknesses in the chosen strategy and methods. Again, relevant studies have shown that a significant percentage of the respondent organisations do not measure the effectiveness of their awareness programmes (see Figure 2) and, more worryingly, that there is no improvement in this aspect over the years (CSI/FBI, 2008)(CSI/FBI, 2009)(CSI/FBI, 2010/2011).

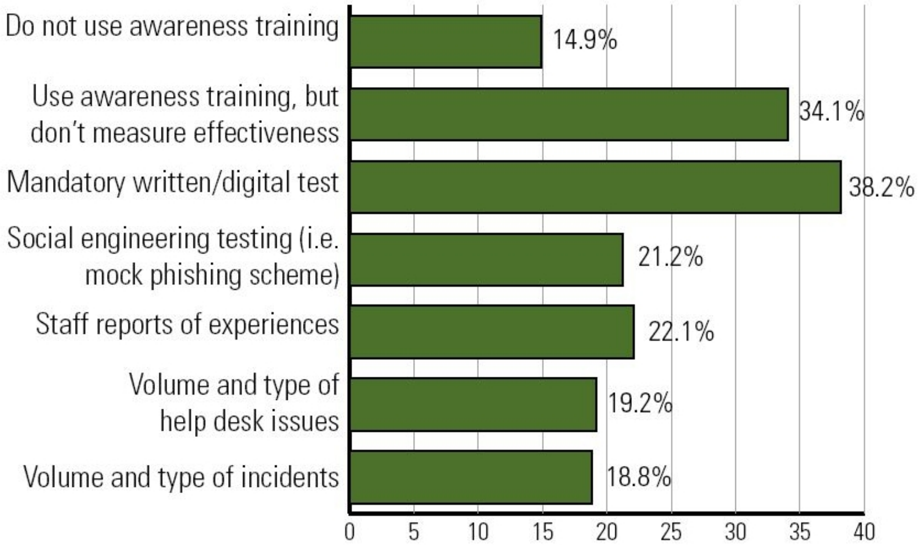

Figure 2. Techniques used to Evaluate Effectiveness of Awareness Training (CSI/FBI, 2010/2011).

Although awareness program deficiencies can be revealed through the evaluation of the organisation's overall information security program, an evaluation methodology which specifically targets the awareness campaign will be more effective.

Within this context, measuring the effectiveness of the awareness campaign is vital for ensuring program improvement and continuation through management support and, of course, for the evaluation of the awareness team’s efforts.

This paper proposes a methodology for evaluating the awareness program considering the most common and essential methods used for delivering awareness material. Section 2 aims to clarify what can be considered as program effectiveness and explain why an organisation’s level of awareness should not be directly compared to other organisations’ performance. Section 3 defines some prerequisites for the effectiveness of the program, and therefore, for the effort required to evaluate the program, while section 4 presents the methodology used for evaluating program components. Finally, section 5 presents a method for the evaluation of the program in total, which can act as a point of reference for future evaluations and a figure to present to senior management.

2. Defining “Program Effectiveness”

An awareness program evaluation aims to assess program's effectiveness and revealing weaknesses both in the methods used for delivering the required content as well as the content itself. It also helps justify the investment in security awareness initiatives and to encourage increased programme activity.

The evaluation of a program could be based on *qualitative* or *quantitative* techniques or a combination of the above.

a) *Qualitative techniques* are mainly used to capture employees' sensation regarding awareness and whether they truly exercise security awareness. Although the interpretation of the results obtained by these techniques can sometimes be subjective and might lead to speculations and conjectures, their significance should not be underestimated. Commonly deployed qualitative techniques include users' feedback, independent observations and silent monitoring of employees' reactions (e.g. during an awareness session).

b) *Quantitative techniques* attempt to present the evaluation results in a more objective way and provide benchmarks for future evaluations. Methods that can be deployed are metrics, namely key performance indicators (KPI), which can give a clearer view regarding the effectiveness of a program. However, there are neither universally accepted and validated methods nor exact figures in the industry that can classify a program as successful or not and, what is more, defining quantitative metrics appears to be very difficult for most organizations (European Network and Information Security Agency (ENISA), 2010). This is not surprising since these metrics often involve simplifying a complex socio-technical situation down to numbers or partial orders (Savola, 2008).

The evaluation methodology presented in this paper will focus on quantitative techniques. Quantifiable and repeatable results are an important factor to consider choosing an effective and useful set of metrics for any relevant evaluation, as indicated by all relevant guidelines (e.g. (National Institute of Standards and Technology (NIST), 2008)). Our work will also reference complementary qualitative metrics where possible. The latter will not be included in the evaluation framework, since mapping these qualitative values to exact numbers is an open issue and cannot be carried out in a structured and objective way. As a consequence, the framework’s grading would become very subjective in nature and the results would be of limited value as a benchmark for future iterations of the evaluation process. This issue will be further exacerbated if future evaluations are carried out by a different person/team, which is to be expected in most organisations. This approach by no means undervalues the importance of qualitative methods, which in some cases can be considered more important than quantitative ones.

2.1. Relevant work

At this point it is essential to reiterate that quantifying and generally measuring socio-technical issues like security awareness is not trivial, and this of course applies to information security in general. Various approaches can be found in the literature but no generally accepted and validated methodology has been introduced. It is even less common to find a complete framework (i.e. one with specific metrics, grading and aggregation of those metrics to produce a single evaluation score), excluding proprietary ones used by consulting companies which, in turn, have not been peer reviewed. On the other hand, there is no lack of recommendations and general guidelines of how a security program should be evaluated or how to produce the required metrics for said evaluation. This is not surprising since, in many cases, organisations have a regulatory requirement to measure their performance in general but also their information security performance in specific (e.g. Clinger-Cohen Act, Government Performance and Results Act (GPRA) and the Federal Information Security Management Act (FISMA) in the United States of America). (SANS Institute, 2006) presents the basic aspects in building a general security metrics program while (National Institute of Standards and Technology (NIST), 2008) provides a more thorough performance measurement guide for information security. Because of the large scope covered, the aforementioned references and all similar guidelines and recommendations only dedicate a small part of the whole measurement and evaluation process to security awareness.

It should also be noted that one can find alternative approaches to information security, like ones examining user psychology. (SANS Institute, 2011) details the proven effects a patient's psychology has on the progression of his/her illness and aims to identify similar links between employees' psychology and security risks and threats mitigation. More pertinent to security awareness are several alternative methods found in the literature, like the socio-cultural approach presented in (Teufel, 2003) or the psychological one examined in (Bilal Khan, 2011).

2.2. Effectiveness comparison

Measuring the effectiveness of an awareness program is not a process that requires the direct comparison of some metrics applied to the organisation with benchmarks related to other organisations' performance. As already noted, each awareness program is typically adapted to the unique organisation's needs and environment. Moreover, the degree of effectiveness of a program is a multi-factor issue and is affected by many organisational, architectural, and operational issues within the organisation. Therefore, straightforward comparison of figures between organisations or aiming for some figures similar to other organisations' performance is not the correct approach to measure the effectiveness of a program. The organisation should set its own benchmarks based on the performance results of previous programs.

The evaluation method presented in this paper could be used prior to the implementation of the new awareness program to establish a baseline (i.e. the current status). The benchmark for a successful program will be to improve upon this baseline to an extent that the organisation's management has pre-defined as satisfactory (i.e. the campaign objectives) (Johnson, 2006). Following initial implementation, progress evaluation requires applying the same measurement approach for each of the awareness program's periods, so that direct comparison of results is meaningful.

2.3. Continuous improvement is the key to success

Evaluation figures resulting from the application of the methodology detailed in this paper should demonstrate a continuous improvement. The latter is the most important indicator of success for the organisation's awareness program, even more so when the whole program is not mature enough (hence when there is significant room for improvement). The results of the previous program assessment can be a valuable benchmark for the current evaluation and, in due course, the degree of improvement over the various iterations can be used as a continuous improvement and, therefore, success indicator.

Note that although it is expected to have considerable improvement during the first years of the program's deployment, the degree of improvement is expected to decline as the whole program progresses throughout the years. When the program is mature enough, maintenance of the corresponding evaluation results at a satisfactory level should be the awareness team's aim. A way to take program maturity into consideration will be detailed later in this paper.

It should also be noted that achieving a 100% figure on these metrics cannot be considered realistic.

3. Program evaluation

Assessing the effectiveness of a program is not a trivial task; there is a number of factors which can affect the program's effectiveness and, thus, the results of an evaluation should be carefully examined in order to identify program deficiencies. Correctly identifying the weak points in order to try to improve upon them should be the main aim of the evaluation effort and not just how to produce some figures that the team can report to senior management.

Consider, for example, that the awareness team launches a campaign for the company's finance division which covers all IT users' topics (we assume that this requirement arose from the needs assessment conducted for this division). Let us further assume that the content is delivered exclusively through awareness sessions which are advertised on the intranet website, and that the team conducts surveys, in the form of questionnaires, in order to evaluate the results of this effort.

The hypothetical survey reveals that the campaign did not have the anticipated results. Is this due to inadequate presentation content or the presenter's inefficiency? Careful examination of the survey results shows that those who attended the sessions demonstrated satisfactory progress but the attendance was very low compared to the total number of employees in the division. So, in this case, the team should mainly focus on two areas: management support and campaign advertisement. Management support can guarantee that the target audience has an excellent incentive in attending the campaign, while advertising will ensure that all employees are aware of the team's initiatives.

What about a scenario where both attendance and questionnaire performance was good but the on the job security performance of employees remained poor? This could indicate an issue with the awareness content itself or the delivery methods.

The evaluation of the program can, therefore, reveal weaknesses in the awareness content itself, in the mechanisms deployed to deliver the content as well as in the support the awareness effort enjoys throughout the organisation. In the latter category fall:

a) management's support
b) program funding
c) program marketing, and
d) program management

3.1. Program support must be sound

Sound support of the awareness team's activities is a prerequisite to the success of the program. Without management support, adequate funding, proper marketing and efficient program management the whole awareness effort is jeopardised, therefore it should not come as a surprise that said support is quoted as a pillar of success in all relevant recommendations (e.g. (National Institute of Standards and Technology (NIST), 2008)). The above have to be ensured, in order for the evaluation of the corresponding deployment methods to be meaningful. Although, in theory, the awareness team should not consider the evaluation of these factors, they should not be taken for granted. Therefore, evaluating program support is also required for effectively identifying program weaknesses.

3.1.1. Management's support

Management, at all levels, can demonstrate program support through their behaviour or actions. Both of these should be scrutinised in order to assess manager's contribution to the awareness effort. Although there are methods that can reveal the level of support the management provides to the program (e.g. security related emails that managers send to their employees), assessing management's behaviour towards security and the program should actually be part of the management's evaluation. This is not a trivial task, however, and the only way to conduct such an evaluation is hierarchically. Still, as employees can and should be assessed regarding practicing security, the same applies to managers, all the way to the top of the organisations hierarchy.

3.1.2. Program funding

The awareness team should assess the adequacy of funding based on the requested financial support and the team's budget, i.e. the money allocated to the team's needs. The request for funding should be based on the requirements that arise from the needs assessment process.

3.1.3. Program marketing

The evaluation of the program marketing is another value which is not easy to quantify. An unsatisfactory campaign can be the result of many factors and, therefore, pinpointing a specific issue as the negative contributor is not always feasible. An effective way to evaluate program marketing is through elimination, i.e. if none of the other measures or methods are proven to have significant defects, marketing should be considered as one of the negative factors.

3.1.4. Program management

Efficient management is one of the foundations to a successful program. The awareness team should evaluate its practices against the identified needs and the ability to deliver based on the detailed plan formulated prior to the launch of an awareness campaign. It is recommended that the campaign periods are annual so that at the end of each campaign an evaluation can take place to assess the effectiveness of the launched program.

4. Program evaluation methodology

Measuring the effectiveness of the awareness campaign entails consideration of the following issues:

a) *Whether the information has reached the target.*

Certain methods provide assurance that the information is bound to reach the target while others rely on the deployment strategy. More specifically (note that for the purposes of this paper we assume use of the most common communication channels for delivering awareness material:

a.1.*Awareness sessions.* Non-compulsory sessions’ effectiveness depends on the program's advertisement, on managers' support and on the target audience's perception of security. The awareness team should by no means assume that all members of the target group will attend a session; hence, not all of them will receive the awareness material.

a.2.*e-learning program.* As this is not a push method the only way for the information to reach the employees is if they visit the corresponding website and register for the program.

a.3.*Awareness/Security Days.* A large amount of information delivered through these events reaches the people who attend them. However, it would be interesting to check the percentage of the target group's members who actually participate in these activities.

a.4.*Brochures and leaflets.* Effectiveness depends on the delivery method. Asking a person to hand them personally to each employee is certainly more effective than leaving them on a desk and asking employees to collect them.

a.5.*Posters.* Even if they are widely deployed, awareness posters might go unnoticed by many employees who will simply walk by without going through the displayed information.

a.6.*Emails.* Information sent by emails is bound to reach the target, so emails provide a very reliable means of delivering information to all employees. Moreover, they constitute an easy way for selectively addressing issues related to specific groups. On the other hand, it is possible the content will be ignored by some employees.

a.7.*iNotices.* Messages delivered via iNotices, i.e. messages displayed on computer screens during users' logon, are bound to reach the target. Still, , as with emails, there is no warranty that the message will not be ignored.

a.8.*Monthly e-bulletins/newsletters.* Even though the delivery method of e-bulletins might vary from distribution via emails to posting on a website, the most effective way for them to reach their target audience is via emails.

b) *Whether the information has touched the target.*

This is the most important aspect in awareness program evaluation as it assesses how many people actually absorbed the delivered information and, therefore, whether the main aim of the program, which is to create security aware and conscious people, has been achieved. Simply counting the number of people that attended an awareness session or received a leaflet is by no means a reliable measure of the program's effectiveness. For example, even if brochures are personally delivered, there is no way to ensure that they will not be ignored. The same applies to emails which always reach the target but may still be immediately deleted without being read.

An awareness program evaluation should focus on the number of people that actually benefited from the program. The most common approach is to measure the effect that either individual modules or the whole program had on employees. Attendance statistics can expose the number of employees who received the information, while surveys and questionnaires can be used for measuring the effect that this session had on them; though it should be noted that this does not reveal if and how that information will affect their daily routine. In the following sections we detail the methods used for evaluating the program in total, as well as the effectiveness of individual content delivery methods.

4.1. Evaluating the program in total

Evaluating the effectiveness of the overall program typically requires the design and implementation of a feedback strategy. Note that any methods used for measuring the effectiveness should be deployed discreetly and not overwhelm the user, in order to avoid any negative implications. Methods that can be deployed for this purpose include the following.

4.1.1. Surveys

Questionnaire-based surveys conducted on technical and security policy issues are one of the most reliable means in measuring the effectiveness of the program. This should be an annual effort, to follow the frequency of evaluation process itself which, as recommended, and often dictated, by organisations like NIST (e.g. (National Institute of Standards and Technology (NIST), 2009)), should be at least annual. It should be noted that surveys used for measuring the effectiveness of individual modules can and should be conducted more often (e.g. monthly). The team should consider the following for the survey preparation:

a) Issues covered in surveys should be chosen from the range of topics addressed throughout the year and should reflect security policy issues.
b) There should not be a single questionnaire for all employees. The content should be adapted to different roles within the organisation so that issues that fall within a specific role can also be addressed.
c) Questions raised during a survey should be unambiguous and unbiased, eliminating the risk of being misinterpreted and leading to results that do not reflect the true picture.
d) Queries regarding how employees’ awareness training has, if at all, affected their daily routine may provide an indication of whether gained knowledge is actually applied on the job.
e) The awareness team should ask for employees' feedback in the form of comments on the awareness program, including suggestions for enhancement.
f) Monthly surveys should, ideally, be addressed at different target groups/modules each month, to avoid employee fatigue. On the months that the annual surveys are deployed, there should be no monthly/specific module survey assigned.

Interpretation of survey results can provide valuable information regarding the program's progress. Wrong answers can reveal a program's deficiencies and highlight the issues that the team needs to focus on in order to improve next year's program. Statistical methods can be used to draw the overall picture. It is anticipated that the number of employees that demonstrate familiarity with the subject should constantly increase, until reaching a point of satisfaction.

Survey based quantitative methods that can be deployed for the evaluation of the program in total are listed in Table 1.

Table 1. Quantitative methods based on surveys

Metric	Success factor
M1: *Statistical analysis of monthly surveys on specific organisation’s divisions* $\frac{\textit{Number of correct answers}}{\textit{Number of questions} \text{ x } \textit{Number of participants}} \text{ x } 100$	Monthly surveys enable the team to take corrective actions as the program progresses. They should target different groups each month to avoid overwhelming the employees. This figure is expected to rise in due time.
M2: *Statistical analysis of annual surveys* $\frac{\textit{Number of correct answers}}{\textit{Number of questions} \text{ x } \textit{Number of participants}} \text{ x } 100$	This figure should constantly increase regardless of the fact that new issues might have been addressed during the program. The point of the statistical analysis is to evaluate the overall picture regarding employees’ security behaviour and this is expected to improve.

Users’ suggestions and recommendations can reveal major weaknesses in the program and the corresponding delivery methods and can thus be considered an efficient qualitative method. It is expected that users’ negative views and recommendations for program design issues will decline as the program progresses.

4.1.2. Awareness/Security Days

Security days offer a unique opportunity for the awareness team to directly communicate with employees and get their feedback:

a) Attendance should not be compulsory; hence, employees' reaction in an invitation to attend the event can provide the means to evaluate the program's impact. Typical registration of the attendees can be used in order to get a clear view on the number of people who are interested in enhancing their skills and knowledge. This number should be compared to the total number of people expected to appear given the event's location and scope.

b) Attendees can be provided with anonymous questionnaires addressing security awareness program related issues. The aim is not to assess employees' skills and knowledge but rather provide an easy way for the attendees to
b.1.express their opinion/feelings regarding the current program,
b.2.address issues that they would like to see in future programs, and
b.3.propose new ideas on content delivery.

c) It is anticipated that the number of negative views will be considerably low, given that the majority of people expected to attend the event are those who have already established a positive view towards security; there will be only a fraction of potential attendees who will come just to satisfy the management's request.

d) The organising committee should consider setting up groups with people from different business units and address subjects that affect all participants within the group. The aim is to see how the awareness material affected the group and acquire an understanding on whether the program needs to focus more on a specific group or on all employees. Any opinions expressed during these discussions should be noted and carefully considered.

e) Conduct discretionary independent interviews encouraging the interviewees to express their opinions, feelings, impressions or even worries about the program without any hesitation.

If a supplementary qualitative method is needed, the suggestions provided in forms or drawn from discussions within focus groups or interviews could be analyzed (in conjunction with the overall picture regarding awareness program effectiveness, drawn using other methods). If the overall picture is encouraging there is no need for further action. The awareness group should focus on major design issues or content delivery suggestions made by the majority of employees rather than isolated minor comments that do not actually enhance the program.

Security-day-based quantitative methods that can be deployed for the evaluation of the program in total are listed in Table 2.

Table 2. Quantitative methods based on security days

Metric	**Success factor**
M3: *Statistical analysis of security days attendance* $\frac{\textit{Number of participants}}{\textit{Total number of employees}} \times 100$	The number of attendees in these events is expected to constantly rise as the program progresses. However, attendance is also a result of the success of previous events in terms of employees' satisfaction.

4.1.3. Independent observations

Independent observations on the security behaviour of employees should be carried out silently by awareness team members or representatives that have been assigned to this task. There is no need to alert people and, for example, clean desk policy, which is one of the targets of independent observations, can be performed outside working hours so that it will go unnoticed.

The awareness team should also produce status reports on a regular basis providing their evaluation on their corresponding groups' behaviour. Although metrics can be used for this process the team should also consider the use of qualitative methods. Observers can also deploy electronic means to silently evaluate users' behaviour (i.e. whether staff follow procedures), making sure the chosen methods do not breach employment or data protection laws. All results and observers' conclusions should be documented for future reference. Examples of methods that can be used to accomplish the aforementioned goals include the following:

a) Following a campaign on email security, the team can send out an email to all employees, using an internal email account, with an attachment that looks suspicious, and count the number of recipients that opened the attachment. The expected number should be very low. A similar phishing-based evaluation approach is proposed and detailed in (Ronald C. Dodge, 2007). Variations could be examined, either as an alternative or in conjunction with the above. For example, a similar method could be used after a session which focused on password security involving calling employees (supposedly from the technical department) and asking for their passwords or having the system manager run password-cracking programs against the employee's passwords.

b) The team can take advantage of newly identified threats and spread this information to all employees, or at least to appropriate ones based on their roles, via an email which will contain a link to information about the new threat or security issue. The number of visitors to the provided link can be counted and compared with the overall number of recipients. This metric can be used to measure how security conscious the employees are and their willingness to be informed on security related issues.

Table 3 lists quantitative methods based on independent observations. Some examples of qualitative methods would include the observation of users' behaviour regarding security (an improvement should be apparent) and detailed reports from awareness group representatives (which should demonstrate advances in employees' behaviour as the program progresses).

Table 3. Quantitative methods based on independent observations

Metric	Success factor
***M4:** Statistical analysis of unsuccessful mock phishing attacks* $\frac{\textit{Total number of failed phishing attacks}}{\textit{Total number of phishing attacks deployed}} \times 100$	This figure is expected to rise as the program progresses since employees are expected to demonstrate their understanding of the importance of email security and how to identify suspicious content.
***M5:** Statistical analysis of new threat bulletin's readership* $\frac{\textit{Total number of visitors to link}}{\textit{Number of employees informed via email}} \times 100$	The number is expected to rise as the program progresses and the employees become aware of the importance of keeping up to date with recent threats and security issues.

4.1.4. Audit department reports

Auditing can be used to determine if security awareness related incidents identified by audits are declining. Although reports from the audit department provide an acceptable metric for measuring the effectiveness of the program in overall, careful observation of these reports can also provide valuable information regarding the areas that the awareness team needs to focus. Moreover, it can bring up issues that the group should have addressed in the first place but were left out of the program; this can be used to assess the awareness group's formulated strategy.

Audit department reports based quantitative methods that can be deployed for the evaluation of the program in total are listed in Table 4. Note that this figure should not include issues that fall within specific roles responsibilities and require training and education as opposed to awareness (National Institute of Standards and Technology (NIST), 2003)(National Institute of Standards and Technology (NIST), 1998).

Table 4. Quantitative methods based on audit department reports

Metric	Success factor
M6: *Number of security issues related to employees security behaviour identified by the audit department*	The volume of the identified issues should be declining throughout the program's progress.

4.1.5. Risk department reports

Input from the risk department can be used to identify risks related to security awareness. It should be expected that risks identified during previous risk assessments should be eliminated.

Quantitative methods based on risk department reports that can be deployed for the evaluation of the program in total are listed in Table 5.

Table 5. Quantitative methods based on risk department reports

Metric	Success factor
M7: *Number of security issues related to employees security behaviour identified by the risk department.*	It is expected that the number of issues identified by the risk department will decline as the program progresses.

A qualitative approach could entail risk department reports, listing security awareness related risks that have not been mitigated, excluding risks identified in previous reports.

4.1.6. Security incidents

Security incidents are a valid point of reference regarding awareness program evaluation, and their processing should go beyond a simple check on the volume of incidents, as these can demonstrate two things:

a) The volume and nature of confirmed security incidents can be an indicator of whether employees exercise security-aware working behaviour. The number of incidents is expected to constantly drop as the awareness program evolves. Moreover, the incidents reported should fall outside the scope of the content delivered with the current program.

b) The number of reported, yet unconfirmed, i.e. false, security incidents can demonstrate whether employees remain vigilant during their everyday work.

Therefore, an increase in the number of reported incidents can also have positive implications regarding the effectiveness of the awareness program. This should be examined in conjunction with the number of security incidents that could have been reported by the employees but went unnoticed. This figure can help determine the employees' level of alertness and is expected to drop throughout the program's progress.

Quantitative methods based on security incident reports which can be deployed for the evaluation of the program in total are listed in Table 6.

Table 6. Quantitative methods based on security incidents

Metric	Success factor
M8: *Number of employees who are the source of at least one security incident that stems from non secure behaviour (out of the total number of employees).*	It is expected that this number will decline throughout the program's progress.
M9: *Number of employees who are the source of at least one security incident that falls within their responsibilities but were not identified by them (out of the total number of employees).*	The figure is expected to decline throughout the program's progress as the level of vigilance should be rising.

Scrutinizing security incidents to assess whether these could be prevented through security awareness can be considered an effective qualitative method in this area. Issues that have not been addressed during the current awareness program should be considered for upcoming programmes.

4.2. Measuring the effectiveness of individual modules

Methods deployed for delivering awareness material cannot be equally effective. Assessing the effectiveness of each method can provide useful information to the awareness team regarding the approach taken and can guide the team to the following:

a) It can provide directions regarding the amount of effort required to improve the corresponding module, i.e. whether the module requires minor improvements or major modifications (e.g. revised deployment strategy).

b) It can help determine whether it is meaningful to keep investing on the corresponding method or, perhaps, abandon it altogether and focus on other, more effective, approaches. The team should not be reluctant to refrain from investigating on a method that is proven to be ineffective.

c) It can help fine-tune the extent to which each module's evaluation marks affects the programme's total evaluation mark (i.e. mark weights – more on this in Paragraph 5.2) for current and future iterations.

Measuring the effectiveness of individual methods is accomplished, mostly, via metrics. For content delivered electronically the awareness team should consider taking advantage of the fact that feedback can be dynamically provided by the employees. This is very important as the team has the opportunity to adapt dynamically to emerging requirements or users' recommendations.

The approaches taken for measuring the effectiveness of each content delivery method are defined in the following sections.

4.2.1. Awareness sessions

This is considered one of the easiest methods to evaluate given the existence of multiple communication paths for getting the required feedback. There are both qualitative and quantitative methods that can be deployed for this purpose.

a) *Audience satisfaction:* This is clearly expressed by the attendees' expressions and reactions during the session (attendees temporarily leaving the room, constantly chatting with colleagues, or sketching on their notes are not encouraging reactions). Feedback forms can be provided as well, preferably anonymous, so that employees can write down their opinion on the session, the instructor, and the corresponding content. Moreover, attendees should be encouraged to provide suggestions on improving the effectiveness of these sessions or the awareness program itself. Note, however, that incorporating these suggestions should be carefully considered so that the final result will be to the benefit of the program, i.e. they will not negatively affect or jeopardise the method.

b) *Tests in the form of questionnaires:* A simple questionnaire provided at the end of the session, covering some of the key issues addressed during the session, can be a very reliable way to assess the session's effectiveness. Use of a preliminary survey or a pre-session test and comparison of the pre- and post-session tests can assist in determining the session's impact.

Quantitative methods that can be deployed for the evaluation of awareness sessions as a content distribution method are listed in Table 7.

Table 7. Quantitative methods for the evaluation of awareness sessions

Metric	Success factor
M10: *Statistical analysis of sessions attendance* $\frac{\textit{Number of attendees}}{\textit{Total number of expected attendees}} \times 100$	This figure is expected to rise throughout the program's progress as more employees are expected to demonstrate their interest on security awareness. Note that the team should not expect the employees to attend a session more than once.
M11: *Statistical analysis of sessions effectiveness* $\frac{\textit{Total number of correct answers}}{\textit{Number of questions} \times \textit{Number of attendees}} \times 100$	The number is expected to rise as the program progresses as it is not only affected by the quality of the current session but also by the overall attitude of employees towards awareness, which is also expected to advance.

In terms of qualitative methods that could be utilized for the evaluation of awareness sessions, the assessment of attendees' reactions during the sessions can be an effective approach. Attendees should demonstrate interest on the topic(s) addressed during the session by asking questions, providing answers and feedback to instructors' questions through an interactive delivery of content. Moreover, the suggestions expressed by employees through feedback forms could be processed. The quality of said suggestions is a good indicator of the level interest and adoption of a security awareness culture.

4.2.2. Information security website

The number of employees who visit the website where information security related content is posted demonstrates user's interest in the corresponding topics. However, this number has to be interpreted with care as it can lead to false results. The formulated number of visits is a factor of the number of employees who adopt security behaviour and want to find more information on the corresponding issues, but is also affected by the following:

a) Whether the provided content is useful and easy to follow.
b) The amount of information that is new to visitors (if employees familiarize themselves with the content the number of visitors is bound to decline in due time).
c) The number of revisits by a small group of employees who demonstrate special interest in the content.

A small feedback-form provided to visitors can help clarify the origins of the formulated number.

Quantitative methods that can be deployed for the evaluation of the information security website as a content distribution method are listed in Table 8. Note that this statistical analysis should be an annual effort.

Table 8. Quantitative methods for the evaluation of the information security website

Metric	Success factor
M12: *Statistical analysis of information security website visits* $\frac{\textit{Number of employees that visited the site}}{\textit{Total number of employees}} \times 100$	This figure demonstrates the importance of the information security website on delivering security awareness material. A decline in the number of visits however should not be considered as method's ineffectiveness.

In case a supportive qualitative method is required, the inspection of users' feedback is a valuable source of comments on the structure and the content of the information security website. Moreover, the visitor patterns of the website can be used to extract other useful information (e.g. "How many users have accessed the contingency plan material in the past year?") (Noticebored, 2008).

4.2.3. e-learning

Statistics can provide useful information regarding the number of employees visiting, registering, and completing the e-learning program. In specific:

a) Comparing the number of visitors with the number of registrants can give an indication to the number of people who were interested or curious enough to have a look at the program, yet the initial impression they got from the web site was not satisfactory enough to register for the program. The number of visitors who did not end up registering should not be very high, otherwise the team should consider redesigning the e-learning site.
b) Comparing the number of registrants with the number of those that completed the program provides useful information regarding the content of the e-learning

program and the way it is delivered. If employees are not given incentives to complete the program they are bound to abandon it as soon as they feel tired of it or bored. Reasons for abandoning the program include the following.

b.1.The program is too long to finish in one session. Although this is acceptable given the amount of information that has to be delivered, it is important to examine the reasons why the employees that temporarily leave a session do not come back to finish the program.

b.2.The content is considered not interesting enough or difficult to follow.

A short form should be provided on each page (it does not have to be different for each page) or pop-up upon exit, so that the user can comment on the reasons for leaving/abandoning the e-learning program. Carefully chosen questions can provide valuable information regarding the reasons why the employees do not finish the program. The amount of input required by the employee should be kept to a minimum thus increasing the likelihood of getting the required feedback.

Quantitative methods that can be deployed for the evaluation of the e-learning program are listed in Table 9. Note that the statistical analysis should be an annual effort.

Table 9. Quantitative methods for the evaluation of the e-learning program

Metric	Success factor
M13: *Statistical analysis of e-learning program visits* $\frac{\textit{Number of visitors}}{\textit{Total number of employees}}$ x 100	This is expected to rise as the program progresses, especially if management's support is sound.
M14: *Statistical analysis of e-learning program registrations* $\frac{\textit{Number of registrants}}{\textit{Total number of visitors}}$ x 100	It is expected that the number of registrants will be very close to the e-learning site visitors. If this is not demonstrated by the corresponding metric the team should consider restructuring the site so that the first impression will not disappoint visitors.
M15: *Statistical analysis of completions* $\frac{\textit{Number of completions}}{\textit{Total number of registrants}}$ x 100	Assuming that the program will be undertaken annually, the number of registrants that complete the e-learning program should constantly rise.

Users' feedback on the e-learning program can provide valuable comments on program enhancement and can be considered an auxiliary qualitative method.

4.2.4. Emails

Awareness content delivered through emails is bound to reach the target. However, as already mentioned, there are no guarantees that the email will not be ignored. For content provided using emails a simple method can be used to measure the method's effectiveness: the email content should be structured in such a way so that a link is provided at the end of the email for more information regarding the subject addressed, information which should be crucial for getting a complete overview of the subject. Thus, the team can count the hits to the provided link, as an indication to the number of employees that actually went through the content and did not simply ignore it. Assuming that the email is only sent to employees to whom the included content applies to, the closer this number gets to the number of recipients, the more encouraging the results regarding the effectiveness of this approach. It is almost certain that there will be a number of people who will go through the email but not follow the link, but this method can give an indication regarding the number of users that demonstrate interest in the content delivered through emails.

Quantitative methods that can be deployed for the evaluation of emails as a content distribution method are listed in Table 10.

Table 10. Quantitative methods for the evaluation of emails

Metric	Success factor
M16: *Statistical analysis of email views* $\frac{\textit{Number of recipients that followed the link}}{\textit{Total number of recipients}} \text{ x } 100$	The number is expected to rise in the first steps of the project while ups and downs should also be expected. If the number is not satisfactory for long periods of time, restructuring the way the content is delivered should be considered.

4.2.5. iNotices

As with emails where content is delivered electronically, links can be provided in iNotices for follow up information. For instance if the delivered message addresses the need for use of strong passwords, the link can give hints on how to use a strong yet memorable password. The number of employees following the provided link should be counted and compared to the number of employees that logged in during the day, or the total number of employees. If the percentage is significantly low then there is a strong indication that people might be simply ignoring the message.

Quantitative methods that can be deployed for the evaluation of iNotices as a content distribution method are listed in Table 11.

Table 11. Quantitative methods for the evaluation of iNotices

Metric	Success factor
M17: *Statistical analysis of iNotices readings* $\frac{\textit{Number of recipients that followed the link}}{\textit{Total number of recipients}} \text{ x } 100$	The number is expected to rise in the first steps of the project while ups and downs should also be expected. If the number is not satisfactory for long periods of time, restructuring the way the content is delivered should be considered.

4.2.6. Posters

Measuring posters contribution to the awareness program is not a trivial task and can, in general, be accomplished by independent observations. However, there are more straightforward ways that can provide clues regarding the impact that posters have on employees. This can typically be done by providing a link where the same posters can be found in electronic form so that employees can download and use as screensavers or as backgrounds on their personalised desktop. Note, however, that potential limited downloads of the aforementioned material does not necessarily mean that the method is unsuccessful. It might be the result of unattractive material displayed on them.

Quantitative methods that can be deployed for the evaluation of posters as a content distribution method are listed in Table 12.

Table 12. Quantitative methods for the evaluation of posters

Metric	Success factor
M18: *Statistical analysis of poster downloads* $\frac{\textit{Number of employees who downloaded a poster}}{\textit{Total number of employees}} \text{ x } 100$	This figure is expected to rise throughout the program's progress, as more employees are expected to demonstrate their interest on security awareness.

5. Metric aggregation - Overall evaluation

5.1. An overall evaluation of the program cannot provide any useful conclusions regarding the respective program modules, but can be used as a valuable point of reference for future assessments and a figure that can be presented to management for reporting and securing the required support.Marking Scheme

The method presented in this section takes into account the results of individual metrics (only the quantitative ones, which have a more straightforward grading), as these were analysed in the previous sections. For each of these metrics a performance scale is defined that will allow the formulation of the desired performance figure.

It should be clarified these scales are flexible and the final marking scheme must be adjusted to each organisation's case, depending on their current security posture, program's goals etc. It is, for example, particularly evident that marks regarding the number of security issues identified by the audit and risk departments (i.e. M6, M7) unquestionably depend on the organisation's size and risk appetite. It is therefore essential that higher management, in cooperation with the awareness team, adjust the marking scheme prior to the evaluation program's implementation.

Table 13 presents an initial marking scheme for all metrics used for the awareness program evaluation. All marks range from 1 to 10, unless otherwise specified, where 10 is given for the best possible result. The scales were chosen with the easiness of the program effectiveness assessment process and the comparison of the corresponding elements progress evaluation in mind.

Table 13. Marks definitions

Metric	Mark	Comments
M1: Statistical analysis of monthly surveys on specific organisation's divisions	*M1/10*	The mark is based on the total number of correct answers received by the participants.
M2: Statistical analysis of annual surveys	*M2/10*	The mark is based on the total number of correct answers received by the participants
M3: Statistical analysis of security days attendance	*M3/10*	The mark is based on the percentage of employees, who participated in the awareness/ security day, out of the organization work force for the specific region.
M4: Statistical analysis of unsuccessful mock phishing attacks	*M4/10*	The mark is based on the percentage of employees who did not fall victims to the attack out of the total number of potential victims among employees.
M5: Statistical analysis of new threat bulletins' readership	*M5/10*	The mark is based on the percentage of employees who read the new threat/security issue bulletin out of the total number of employees who were asked to visit the bulletin.
M6: Number of security issues related to employees security behaviour identified by the audit department	$\begin{cases} 10 - M6 & \text{for } 0\leq M6\leq 10 \\ 0 & \text{for } M6>10 \end{cases}$	The mark is based on the number of types of issues identified by the audit department. It is assumed that a number of 10 issues is the worst case.
M7: Number of security issues related to employees security behaviour identified by the risk department.	$\begin{cases} 10 - M7 & \text{for } 0\leq M7\leq 10 \\ 0 & \text{for } M7>10 \end{cases}$	The mark is based on the number of types of issues identified by the risk department. It is assumed that a number of 10 issues is the worst case.
M8: Number of employees who are the source of at least one security incident that stems from non secure behaviour (out of the total number of employees).	*10 – M8/10*	The mark is based on the percentage of employees who are the source of at least one security incident but have actually reported it.
M9: Number of employees who are the source of at least one security incident that falls within	*10 – M9/10*	The mark is based on the percentage of employees who are the source of at least one security incident but

their responsibilities but were not identified by them (out of the total number of employees).		were not vigilant enough to identify and report it.
M10: Statistical analysis of sessions attendance	*M10/10*	The mark is based on the percentage of employees who attended the sessions, out of the total number of targeted employees.
M11: Statistical analysis of sessions effectiveness	*M11/10*	The mark is based on the percentage of correct answers on surveys conducted after the session.
M12: Statistical analysis of information security website visits	*M12/10*	The mark is based on the percentage of employees who visited the site at least once during a year’s period.
M13: Statistical analysis of e-learning program visits	*M13/10*	The mark is based on the percentage of employees who visited the e-learning program site.
M14: Statistical analysis of e-learning program registrations	*M14/10*	The mark is based on the percentage of visitors who registered for the e-learning program.
M15: Statistical analysis of completions	*M15/10*	The mark is based on the percentage of registrants who completed the program.
M16: Statistical analysis of email views	*M16/10*	The mark is based on the percentage of email recipients who followed the provided link.
M17: Statistical analysis of iNotices readings	*M17/10*	The mark is based on the percentage of iNotices readers who followed the provided link.
M18: Statistical analysis of poster downloads	*M18/10*	The mark is based on the percentage of employees who downloaded at least one poster in electronic form.

Even though similar scales could be defined for qualitative measures, they were intentionally left out of this evaluation methodology. As already mentioned, grading in that case would become even more subjective and would be of limited use for future reference unless the same person or team undertakes the evaluation process, which of course can not be guaranteed in any organization.

5.2. Weights

The individual metrics used for evaluating the awareness campaign cannot be considered as equally important in the process of evaluating the program in overall; hence weights have to be assigned to them to ensure that evaluation using this method will not lead to the wrong conclusion.

Table 14 presents some preliminary weights for the awareness program evaluation modules as well as their corresponding elements. For each element a weight has been assigned to demonstrate its importance in module effectiveness evaluation. The same approach has been used for all modules in order to evaluate the whole program.

Table 14. Evaluation criteria assigned weights

Assessment module	Module Weight	Element Weight
Surveys	15%	
M1		30%
M2		70%
Awareness/Security Days	5%	
M3		100%
Independent Observations	10%	
M4		60%
M5		40%
Audit Reports	10%	
M6		100%
Risk Reports	10%	
M7		100%
Security Incidents	10%	
M8		70%
M9		30%
Awareness sessions (workshops)	10%	
M10		50%
M11		50%
Information Security Website	5%	
M12		20%
E-learning	10%	
M13		20%
M14		30%
M15		50%
Emails	5%	
M16		100%
iNotices	5%	
M17		100%
Posters	5%	
M18		100%

It should be reiterated that the numbers above can be considered placeholder values. They can, of course, be used as a basis for an initial evaluation but, optimally, these should be re-distributed by higher management in cooperation with the awareness team prior to the initial evaluation. Moreover, whatever the exact percentages decided upon initial evaluation, further fine tuning is to be expected and, in fact, necessary to optimize the accuracy and efficiency of the evaluation method as the program progresses and new iterations are deployed.

The adjustments of weights' distribution should not only be based on management's subjective evaluation of the individual modules but also as a response to issues identified by the method itself (e.g. inefficiency of a certain training module). Moreover, adjustment of weights could be used as a compensation for other issues, like the aging of certain components. For example, the percentage of correct answers in monthly surveys (metric M1) is expected to rise as employees' awareness and participation in the programme increases. Even so, if the topics covered and questions included in these monthly surveys are not updated often, the meaning of the metric will be degraded (Henning, 2002). This should be reflected on its weight which should be lowered; at least until appropriate measures are in place (i.e. the awareness team ensures timely and frequent updates of monthly surveys).

Other than the management's requirements and evaluation, current state-of-the-practice techniques and technologies and state-of-the-art research pertaining to security can provide additional input to assist in the distribution of the weights; an organisation is, after all, expected to establish and maintain contact with entities which can provide such input (e.g. special interest groups, specialized forums, professional associations) (National Institute of Standards and Technology (NIST), 2009). For example, (Albrechtsen, 2006) demonstrates that users themselves perceive a user-involving approach as the most effective tool for influencing individual security awareness and behaviour, e.g. by e-learning interactive software or information security workshops. Moreover, mass-media based awareness campaigns have a low degree of influence on users, while documented rules and guidelines for expected behaviour are experienced as valueless by the users. (Janne Merete Hagen E. A., 2009) confirms that e-learning tools result in significant short-term improvement in security knowledge, awareness and behaviour and, according to (Janne Hagen, 2011), more than half a year after the session these improvements on employees' security awareness and behaviour partly remain (even though detailed knowledge on security issues is diminished). It is therefore important to continuously perform such sessions to refresh that knowledge, a practice which is in line with various authorities' recommendations (e.g. (National Institute of Standards and Technology (NIST), 2009)), which suggest frequent (i.e. at least annual) security awareness training.

Another aspect to consider is that of the relative weights between modules. Employees might attend all training sessions, frequently visit the security website and even score well in post-training questionnaires, which would lead to high evaluation numbers in the respective modules, indicating an effective program and a healthy security awareness culture among the organisation's employees. Unfortunately, the abovementioned positive indications do not necessarily correlate with critical security-related changes in on-the-job behaviour (Schultz, 2004)(Sademies, 2004). Arguably, this can provide a solid basis for assigning higher weights to behaviour-related modules (e.g. Security Incidents, Audit Reports) compared to survey and attendance-based modules, since they provide direct evidence of the actual state of employees' awareness.

Still, non-technical metrics like attendance, surveys and questionnaires should not be undervalued. Recent research validating awareness training with technical and non-technical audits has shown there is a direct link between a rigorous and thorough awareness program and user's actual on-the-job security behaviour (Eminağaoğlu, 2010); though it should be noted the focus of the program referenced above was relatively narrow, focusing mostly on password usage. Moreover, individual behavioural metrics (e.g. M4 regarding phishing attacks) examine a specific aspect of employees' behaviour but an awareness program aims to change a number of behaviours i.e. the organisation's security culture in total. Covering even the most important behavioural traits means introducing a number of metrics (some of which might require additional investment in surveillance tools, audits etc.), which can be considered inefficient (European Network and Information Security Agency (ENISA), PricewaterhouseCoopers LLP (PwC), 2007). It is clear that good practice is still evolving in this area.

Assuming all of the above have been fine-tuned and executed according to plan, the final stage in the evaluation is to aggregate all the individual module scores to an overall mark. A highly controlled and structured methodology for assigning weights and computing a final (i.e. overall) mark which could be combined with our evaluation program is presented in (Kruger, 2006). The evaluation data must be organized in a tree form, a generic structure of which can be seen in Figure 3.

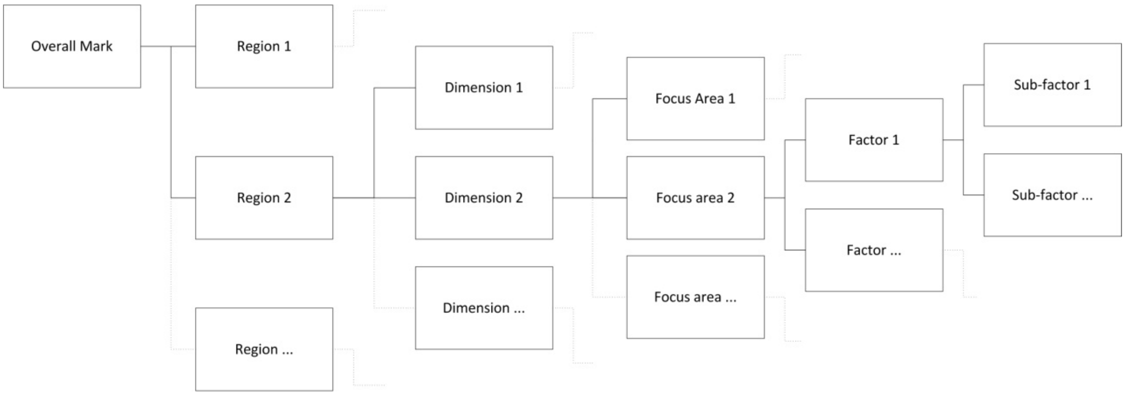

Figure 3. Generic tree structure of the awareness evaluation problem.

Based on the analytic hierarchy process (AHP) (Saaty, 1980) and pair-wise comparisons, it provides a subjective evaluation of factors based on management's professional judgement and opinion. The end result of the method is a numerical measure of the decision-makers' perception of the relative value of the evaluation criteria. Moreover, the methodology includes a consistency index to detect potential inconsistencies in the pair-wise comparisons.

6. Conclusions

Measuring the effectiveness of an awareness program is not limited to the use of quantitative methods; qualitative methods can also contribute to the evaluation. The benefit of using quantitative methods however, other than the fact that they are not as subjective as qualitative methods are, is that they can be used to better assess if the program has met its targets as well as for future reference. This is vital as the key to a successful awareness program is continuous improvement and this can only be proven by applying the same effectiveness measurement approach. The awareness group can set targets for the next awareness program based on the results drawn from the current program's evaluation. These desired targets, however, are only feasible if the supportive measures are secured, as otherwise the whole program is put at risk. This paper presented a methodology for evaluating the awareness program in total, as well as assessing the effectiveness of individual modules. Using the defined methodology the awareness team will have an effective tool for presenting the results of their efforts to senior management, secure the continuation of the program and, moreover, gain the means to take corrective actions to ensure the best possible result for their efforts.

7. References

Albrechtsen, E. (2006). A qualitative study of users' view on information security. *Computers & Security*.

Bilal Khan, K. S. (2011). Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management, 5*(26), 10862-10868.

CSI/FBI. (2008). *13th Annual CSI/FBI Computer Crime and Security Survey.* Retrieved July 15, 2012, from www.gocsi.com

CSI/FBI. (2009). *14th Annual CSI/FBI Computer Crime and Security Survey.* Retrieved July 15, 2012, from www.gocsi.com

CSI/FBI. (2010/2011). *15th Annual CSI/FBI Computer Crime and Security Survey.* Retrieved July 15, 2012, from www.gocsi.com

Deloitte. (2010). *Global Security Survey.* Retrieved July 15, 2012, from www.deloitte.com

Deloitte. (2011). *Global Security Survey.* Retrieved July 15, 2012, from www.deloitte.com

Eminağaoğlu, M. U. (2010). The positive outcomes of information security awareness training in companies – A case study. *Information Security Technical Report*, 223-229.

European Network and Information Security Agency (ENISA). (2010). *The new users' guide – How to raise InfoSec Awareness.* Retrieved July 15, 2012, from http://enisa.europa.eu

European Network and Information Security Agency (ENISA), PricewaterhouseCoopers LLP (PwC). (2007). *Information security awareness initiatives: Current practice and the measurement of success.* Retrieved July 15, 2012, from http://www.enisa.europa.eu

Henning, R. e. (2002). Information System Security Attribute Quantification or Ordering. *Proceedings of Workshop on Information Security System, Scoring and Ranking, MITRE.* Williamsburg, Virginia.

Janne Hagen, E. A. (2011). The long-term effects of information security e-learning on organizational learning. *Information Management & Computer Security, 19*(3), 140-154.

Janne Merete Hagen, E. A. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*, *16*(4), 377 – 397.

Janne Merete Hagen, E. A. (2009). Effects on employees' information security abilities by e-learning. *Information Management & Computer Security, 17*(5), 388-407.

Johnson, E. C. (2006). Security awareness: switch to a better programme. *Network Security, 2006*(2), 15-18.

Kruger, H. &. (2006). A prototype for assessing information security awareness. Computers Security. *25*(4), 289-296.

National Institute of Standards and Technology (NIST). (1998). *Special Publication 800-16: Information technology security training requirements: a role- and performance-based model.* Retrieved July 15, 2012, from http://csrc.nist.gov

National Institute of Standards and Technology (NIST). (2003). *Special Publication 800-50: Building an information technology security awareness and training program.* Retrieved July 15, 2012, from http://csrc.nist.gov

National Institute of Standards and Technology (NIST). (2008). *Special Publication 800-55, Revision 1: Performance Measurement Guide for Information Security.* Retrieved October 28, 2012, from http://csrc.nist.gov

National Institute of Standards and Technology (NIST). (2009). *Special Publication 800-53, Revision 3: Information Security, Recommended Security Controls for Federal Information Systems and Organizations.* Retrieved July 15, 2012, from http://csrc.nist.gov

Noticebored. (2008). *Generic Business Case for an Information Awareness Program.* Retrieved July 15, 2012, from http://www.noticebored.com

Ronald C. Dodge, C. C. (2007). Phishing for user security awareness. *Computers & Security, 26*(1), 73-80.

Saaty, T. L. (1980). *The Analytic Hierarchy Process.* NY: McGraw Hill.

Sademies, A. (2004). Process Approach to Information Security Metrics in Finnish Industry and State Institutions. *VTT Publications*(544), 89 p. +app. 2 p.

SANS Institute. (2006). *A Guide to Security Metrics.* Retrieved October 28, 2012, from http://www.sans.org/

SANS Institute. (2011). *Measuring Psychological Variables of Control in Information Security.* Retrieved October 28, 2012, from http://www.sans.org/

Savola, R. (2008). A Novel Security Metrics Taxonomy for R&D Organisations. *Proceedings of the ISSA 2008 Innovative Minds Conference.*

Schultz, E. (2004). Security training and awareness—fitting a square peg in a round hole. *Computers Security 23*, 1-2.

TELUS–Rotman. (2011). *Joint Study on Canadian IT Security Practices.* Retrieved July 15, 2012, from http://www.rotman.utoronto.ca/securitystudy/

Teufel, T. S. (2003). Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture. *In Proceedings DEXA Workshops*, (pp. 405-409).