HIMIS: Human Impact Management for Information Security

A methodology for managing the human risks to information security through “awareness” and “behaviour" management

Author - Anup Narayanan, Founder, First Legion Consulting

6/14/2010

Abstract: HIMIS is a methodology with an objective to reduce information security risks that occur due to human mistakes. To achieve this objective, HIMIS views the human factor as two distinct, but interdependent components, viz. “awareness” and “behaviour”. Awareness is “to know” and behaviour is “to do or to react”. Awareness and behaviour are not the same, though they are interdependent. High awareness does not mean that information security risks due to human mistakes are less. Positive change in behaviour is the key.

To achieve confidence that information security risks due to human risks have reduced, it is necessary to have more security awareness and responsible behaviour from the workforce while handling information. HIMIS helps you to first, *define* the information security awareness and behaviour requirements, second, build a *strategy* for awareness and behaviour management, third, *deliver* the program and four, *verify*, whether the awareness has increased and whether behaviour of the workforce has improved while handling information. The HIMIS methodology is built on the belief that the true reward of a good information security awareness program is positive change in behaviour.

License

Version

1.0 – 14th of June, 2010

Author

Anup Narayanan

CISA, CISSP

Founder and Senior Consultant, First Legion Consulting

anup@firstlegion.net

www.firstlegion.net

HIMIS Website

http://himis.isqworld.com

Official reviewers

Name: Adriana Mileidy Carrillo Garcia
Email: mileidy.carrillo@hotmail.com

Contents

1. Introduction

Information security management systems (ISMS) consist of 3 principal components, people, process and technology. The technology and process components are only as good as the people who use them. Often, organizations do not get the expected benefits from an information security management system, though they have invested resources on processes and technology, due to poor people approach or attitude, which results in risks.

HIMIS (Human impact management for information security) is a methodology for managing the human (people) aspect of information security. The objective of HIMIS is to reduce information security risks that occur due to human mistakes. In order to reduce these risks, HIMIS views and manages the human aspects of information security through two *distinct but interdependent* components viz.

1) Awareness: To know
2) Behaviour: To do (to react)

The ultimate goal of any information security manager managing an ISMS is to have the people under the system to be "aware" about protecting business information and to "behave" in a responsible manner while handling business information and ensure it's protection.

1.1. The problem statement

The current problems in managing the human factor in information security are:

1. **"Awareness" is not "behaviour", but the distinction is not clearly understood**: Awareness and behaviour are not the same, though they are interdependent. It is possible that a person may be aware, but may not behave appropriately. A good real life example is the way drivers break traffic rules. They may be aware of the traffic rules, but they still break it due to various reasons.

2. **High awareness does not mean lesser risks:** By achieving high levels of information security awareness, it is not necessary that the information security risks have reduced. But, information security practitioners often stop at "awareness" and do not view "awareness" as the firsts step towards creating "better" behaviour nor do they measure whether awareness has helped in creating better behaviour.

3. **Information security awareness and behaviour management is not well defined:** Though information security practitioners understand that the "people" aspect of information security is important, currently there exists no formal framework for providing guidance regarding the management of the

human factor in information security. By framework it is intended that, there must be a process for identifying the business reasons for information security awareness and responsible information security behaviour, a strategy guidance, a delivery guidance and a verification process to check whether awareness has increased and behaviour has improved.

1.2. The HIMIS approach and solution

HIMIS provides a solution for managing the human risks to information security.

The HIMIS approach is,

1. To reduce information security risks due to people mistakes, first people must be made aware about the importance of information security and good information security practices
2. Next, the people must practice (behaviour) what they know (awareness). In order to achieve positive information security behaviour, it may be necessary to introduce motivational, enforcement or corrective strategies by the organizations' management.
3. There must be a continuous process to introduce new awareness and behaviour requirements and spread it in the organization. Existing awareness and behaviour requirements may have to be optimized.

In order to execute the HIMIS approach, HIMIS provides a method for,

1. Identifying and creating information security awareness and behaviour requirements and linking them to business goals
2. These information security awareness and behaviour requirements are classified into ESP's(Expected Security Practices). Each ESP has an "awareness" component and a "behaviour" component. For example,
    a. Logical access control can be considered as an ESP
    b. The "awareness" component of this ESP is "passwords must not be shared in any form"
    c. The "behaviour" component of this ESP is "the user does not share password under duress or does not write it anywhere or share"
3. Building a strategy for implementing these ESP's through awareness creation and behaviour modification strategies for the target workforce
4. Delivering these strategies to the target workforce
5. Measuring the effectiveness of the program through audits (ESP audits) that measure increase in awareness and change in behaviour
6. Correcting and improving the program based on the audit findings

HIMIS methodology is built on the belief that the true reward of a good awareness campaign is positive change in behaviour.

2. Usage, terms and definitions

HIMIS uses certain usages, terms and definitions and they are explained below.

Workforce: Indicates the people that come under the information security awareness and behaviour management program. Usually includes employees, contractors, clients, partners or a combination of one or more of them.

Users: Indicates workforce

Awareness or security awareness: Indicates information security awareness (for example, passwords should not be shared)

Behaviour or security behaviour: Indicates responsible information security behaviour (for example, not sharing passwords)

Practice(s): Indicates behaviour or security behaviour or information security behaviour

Messages: Indicates information security awareness content and messages from the top management for behaviour enforcement

Program: Indicates the information security awareness or behaviour management program or the entire implementation of the HIMIS model

3. The HIMIS implementation model: Overview

The HIMIS implementation model consists of 4 steps, viz. *Define, Strategize, Deliver* and *Verify*. The 4 steps are aligned to Deming model (Plan-Do-Check-Act) to maintain compatibility with existing information security management systems such as ISO 27001.

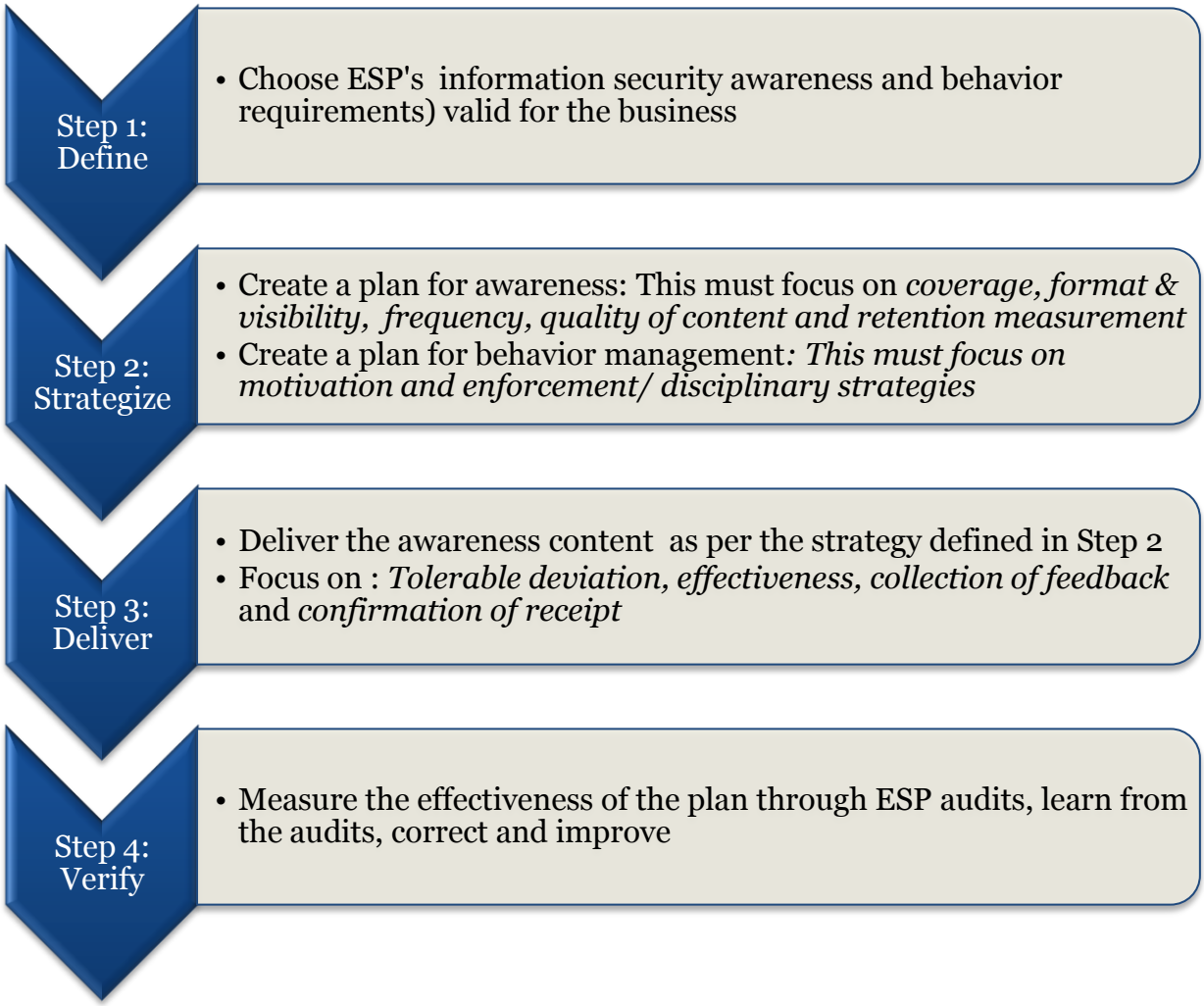

Fig 1: The HIMIS model

4. Step 1: Define

This is the first step of the HIMIS implementation model.

4.1. Selection of ESP's valid for the business

In this step, the organization chooses a set of ESP's (Expected Security Practices) that is valid for the business. An ESP consists of 2 components, viz. an awareness component and a behaviour component. An example is provided herewith.

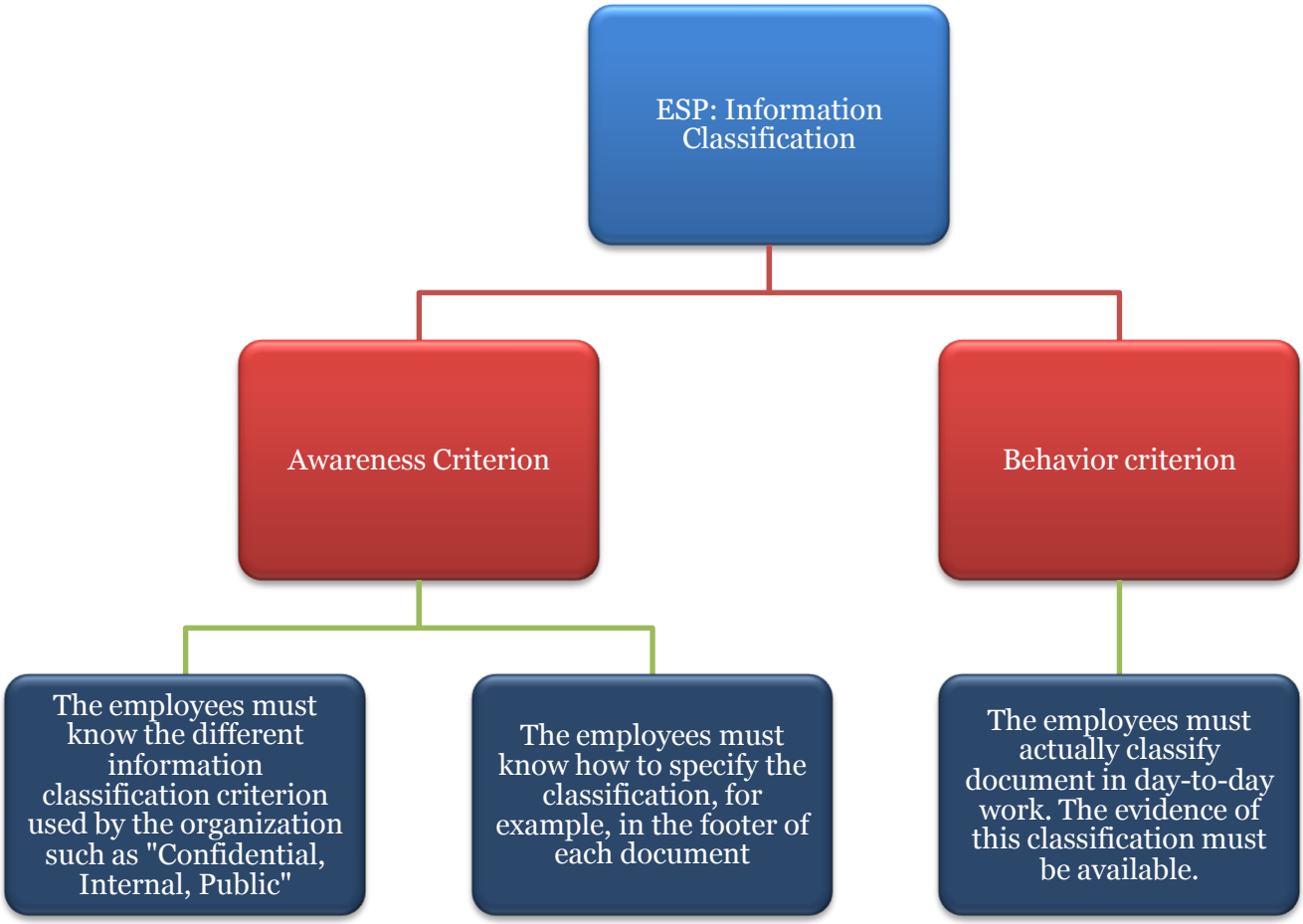

Fig 2 – ESP (Expected Security Practices) Structure

The organization can choose ESP's based on the following criterion or ESP's can be chosen for specific requirements that the organization has.

1. Information security best practices (for example, users' must not share passwords)

A list of ESP's with awareness and behaviour component specifications can be downloaded here.

2. To solve information security risks identified through risk analysis (for example, users' must not disclose sensitive business information on social networks)
3. To satisfy client requirements (for example, client data must always be stored in encrypted format)
4. To satisfy regulatory requirements (for example, patient health records must not be disclosed)

4.2. Review and approval of ESP's

The selected ESP's must be presented to the interested parties. Interested parties here mean, people who have an interest or benefit in the outcome of the awareness and behaviour management program. This may include stakeholders (senior management executives), function heads, risk, compliance and audit function heads.

The ESP's must be approved by the interested parties. The approval process is important to ensure,

1. A clear link between the program and business objectives
2. A clear gap between the implementers and the reviewers
3. A mechanism to provide objective feedback
4. A mechanism to suggest corrections and improvements

4.3. Baseline ESP assessment

The organization can consider an initial baseline assessment of the selected ESP's and understand current levels of information security awareness and behaviour. The assessment approach is mentioned in "Step 4 – Verify". If a baseline assessment is conducted initially, the next round of verification helps in better comparison between the initial state and current state.

5. Step 2: Strategize

The strategy must address both "awareness" and "behaviour". Guidance for strategizing is provided herewith.

5.1. The information security awareness strategy

The information security awareness strategy must address the following components viz. coverage, format & visibility, frequency, quality of content and retention measurement.

5.1.1. Coverage

"Coverage" indicates the target workforce (employees, contractors, partners and other interested parties) that must be covered under the information security awareness program. The covered workforce must receive the information security awareness content in the identified format.

5.1.2. Format and visibility

"Format" indicates the different types of information security awareness content. "Visibility" indicates the channel through which the content is delivered. Channels are selected in order to put information security awareness content where maximum amount of visibility (eyeballs) can be gained. Examples are provided below.

Format	Visibility (with examples)
Verbal	Trainer led classroom sessions, personal interactions
Paper	Posters, cards, quizzes or surveys
Electronic	Videos, Emails with messages, Animated games, Screensavers Quizzes or surveys

***Note**: Quizzes and surveys can also be a mechanism to measure retention, but they also provide awareness through the interactive learning process.*

The organization can choose one or more of the visibility channels to ensure maximum coverage. For example, for organizations that have a large workforce, classroom sessions may not be effective as it is may not be possible to get all members of the workforce into the classroom. In such cases, the organization may use classroom sessions for executive managers and use electronic training sessions for the rest of the workforce.

5.1.3. Frequency

"Frequency" indicates the gap between any two deliveries of information security awareness content. Frequency is critical because it influences "retention". If the

frequency is low (i.e. gap between two information security awareness deliveries is high), the program loses momentum and the workforce remembers less about the importance of information security. A very high frequency is also unnecessary as it leads to overkill. An optimum frequency must be defined, by linking to the type format and visibility factors. For example,

Format	Visibility (with examples)	Frequency (examples)
Verbal	Trainer led classroom sessions, personal interactions	Once every 6 months
Paper	Posters, cards, quizzes or surveys	Posters to be changed every 60 days
Electronic	Videos, Emails with messages, Animated games, Screensavers Quizzes or surveys	e-Learning modules every 90 days Screensavers change every 15 days

5.1.4. Quality of content

"Quality of content" indicates the following factors,

1. **Impact visualization**: Probably the most important factor. It is essential that the information security awareness content captures the "impact" of poor security awareness and behaviour and visualize the same to the learner. Usually information security professionals can visualize the impact of poor security awareness and practices, due to their knowledge in this domain. But, the workforce may not be able to visualize the impact. Hence, the information security professional must endeavour to incorporate "impact visualization" as much as possible in the information security awareness content.

   An example of impact visualization is visually depicting the damage (stealing a laptop, stealing valuable documents) that an intruder can cause by tailgating.

2. **Business relevance**: The information security awareness program, specifically the content must capture the business requirements of information security. While there are certain information security awareness topics that are industry best practices, the awareness program must capture information security practices as required by the business such as regulatory requirements, client expectations about information security and more.

3. **Clarity and ease of understanding**: Style must not be sacrificed for substance, though this happens frequently. Emphasis must be given to conveying the message in a simple and clear manner first. Building style around the message should be done without diluting the message or making the content complicated.

4. **Consideration of cultural factors**: It will be useful to consider cultural factors such as,

   a. Language or terms used (usage of colloquial terms may be more effective),
   b. Colour and design,
   c. Characters represented

While designing the information security awareness content, the above cultural factors can be considered. This has a significant impact on the way the workforce understands the content.

5.1.5. Retention measurement

"Retention measurement" indicates a method to measure how much the workforce has "**understood and remembers**" after the information security awareness delivery. Retention measurement methods must be determined beforehand and must be used during "Step 4 – Verify". The retention measurement methods that can be used are,

a. Personal interviews
b. Surveys
c. Quizzes

5.2. The information security behaviour management strategy

The information security behaviour management strategy is based on the approach that "**users will repeat good behaviour if there are positive consequences and will not repeat poor behaviour if the consequences are negative**". The following strategies shall be considered.

a. **Motivational strategies**: This approach focuses on conveying a "positive-tone" message from the top management to the entire workforce on the benefits of information security and the role the workforce plays in achieving a good information security management system.

b. **Enforcement or disciplinary strategies**: This approach focuses on specifying the penalties for non-compliance. Non-compliance here means a deviation from the ESP (awareness or behaviour component). Often, enforcement or disciplinary strategies have a "tone of repercussion", but it is often essential.

An organization must judiciously combine motivational strategies with enforcement or disciplinary strategies and convey the same with clarity to the workforce before the launch of the awareness and behaviour management program.

Once the strategy is defined, the "delivery" begins. This is explained in the next section.

6. Step 3: Deliver

In this step, the information security awareness content is delivered. Further, the behaviour management strategy is implemented and communicated to the entire organization.

6.1. Delivery of information security awareness

The following factors must be considered while delivery of information security awareness content.

6.1.1. Define tolerable deviation

Though the aim is to attain 100% coverage through the step of delivery, it may not be possible due to various factors. These factors could be technical, procedural, related to lack of time, poor attitude etc. Hence, it makes sense to properly evaluate and follow "Step 2 – Strategize" in order to minimize these factors. Still, in spite of best efforts, it may still not be possible to attain 100% coverage. Considering this, the organization must specify a tolerable deviation in terms of percentage (%).

For example, the organization can state that, "80% coverage of the target workforce is sufficient for the first 6 months. After the 6th month, the target coverage will be 85%". Setting tolerable deviations allows the organization to aim for a fixed target and analyze the reasons for not attaining the target.

6.1.2. Efficiency

The channels through which the delivery is scheduled must efficiently deliver the program. For example,

1. If emails are used to convey the messages, then the emails must reach the target workforce
2. If streaming videos are used to convey the messages, then the videos must stream at an optimum speed
3. If classroom sessions are used to convey the messages, then the trainer must be well versed in the subject, should be able to articulate the topics well and suitable tools must be used to make the messages well-understood

6.1.3. Collection of feedback

A feedback from the learner must be collected from the learner after the delivery. Please note that "collection of feedback" must not be confused with "retention

measurement". The collection of feedback focuses on the learners' opinion on the content. This could include

1. The clarity of the content in conveying the intended message
2. The business relevance of the content
3. Impact visualization
4. The quality of the trainer or the efficiency of the delivery channel
5. *Other factors*

The feedback mechanism is linked to "Step 2 – Strategize", specifically the section on "Quality of content". A good feedback mechanism helps to continuously improve the quality of the content and the quality of the program.

6.1.4. Confirmation of receipt

An important component that makes delivery to be termed successful is confirmation of receipt of the message. This could be attained as follows,

1. A simple "attendance ledger" that can be used for classroom training sessions
2. A SCORM or similar system can track attendance if the content is delivered through an electronic LMS (Learning Management System)

Note *- Some content in the form of posters, screen savers etc. may not facilitate measurement of "how" many people saw the content.*

After the delivery, it is time to "verify" whether the program has been effective or not.

7. Step 4: Verify

In this step, the effectiveness of the program is audited and measured. The guidance prescribed below can be used for verification.

> The verification steps can be performed at the beginning of the project to measure the current levels of awareness and behaviour. In such cases, the 2nd round of verification will help to compare the initial state and current state.

7.1. Verification approach

The verification approach uses ***audits*** to measure improvement or lack of the same in information security awareness and responsible information security behaviour. This works as follows,

1. First, an ESP or a set of ESP's must be selected for verification
2. The awareness component of the ESP must be audited
3. The corresponding behaviour component of the ESP must be audited
4. The reports are created based on the audit findings and submitted to interested parties
5. Decisions based on the audit reports are taken and implemented

> Download the ESP document with audit guidance here.

7.2. Audit strategy

The following points must be considered while designing the audit strategy

7.2.1. Selection of ESP's

The ESP's that will be audited must be selected beforehand. It is important to inform the interested parties about the schedule of the audit and the type of audit methods that will be used. This is important because some of the audit methods such as "social engineering" may require prior approval.

7.2.2. Define sample size

The auditor must choose a reasonable sample size in order to derive maximum confidence in the audit results. It must be noted that a large sample size for

awareness audits is possible as quizzes and surveys can be delivered electronically. A large sample size for behaviour audits may not be possible and in many cases the concept of sample sizes may not be valid. For example,

- It is possible to specify a sample size for violation of internet access policy (unauthorized download of freeware). In this case, the sample size will be all users' who have internet access and violations can be detected from the internet access control system.
- It is not possible to specify a sample size for "identifying instances of tailgating" because it is "instant".

7.2.3. Audit methods

Audit methods are ultimately dependent on the creativity of the auditor. But, the following methods can be considered.

- For auditing information security awareness component of the ESP:
  - Interviews
  - Surveys
  - Quizzes
  - Mind-map sessions
- For auditing the behaviour component of the ESP:
  - Observations: *For example, observe for tailgating, observe how many meeting rooms still have sensitive information on the board after the meeting*
  - Log review: *For example, browsing and email patters can be observed through log reviews of corresponding systems*
  - Data mining : *For example, Mine through internet search engines to see how much sensitive information about the company is available online*
  - Incident report review: *For example, review of incident reports may show how many laptops were lost and a further investigation may reveal the cause as carelessness (poor behaviour) or not (may be the user was physically attacked).*

7.2.4. Reasonable limitations in audits

The audits may be subjected to limitations that the auditor must consider. For example, it may not be possible to audit the behaviour component of ESP's like "mobile computing security". The behaviour component of this ESP may specify that *"the user must not leave mobile computing devices unattended while travelling"*. Since the environment that the user travels in is outside the office, the auditor may not be able to audit the behaviour. In such circumstances, incident reports of lost laptops can be used as a behaviour indicator.

7.2.5. Behaviour may not be always visible

The reason why audit methods include "data mining, review of incident reports and log review" is because it is not necessary that the auditor may be able to see poor information security behaviour in front of their eyes. Often the behaviour may be exhibited elsewhere. Hence, it is necessary to look for behaviour indicators through strategies such as data mining, review of incident reports and log review as indicated in the "Audit methods" section with examples.

7.3. Quantification and presentation of audit reports

Quantification of the findings and presentation of reports is a very important part of the program. This sections offers guidance on the same.

7.3.1. The question of quantification

When presenting audit reports, there is always the question of quantification. In the case of HIMIS, the obvious questions could be,

1) What is the current awareness and behaviour score?
2) How much percentage has awareness and behaviour increased?

Download a sample ESP behaviour quantification tool here.

HIMIS does not aim to be prescriptive in it's approach and does not suggest absolutes. It is up-to the practitioner to choose the methods they prefer to quantify the scores in a manner they seem fit. But, the following must be kept in mind.

1) It is easy to quantify awareness. For example, taking the average score of a quiz to measure awareness from 100 users' reasonably indicates an average awareness score
2) Quantifying behaviour may not be possible directly and indirect methods may have to be used. For example,
    a. Number of violations found for an ESP
    b. Impact of the violation
    c. *A score derived by consideration of "a" and "b" above*

7.3.2. Contents of the audit report

The following content, presented in a neat and clean manner, will present a good audit report to the interested parties.

1) Introduction with reasons for the information security awareness and behaviour management program

2) List of ESP's and the reasons for the selection of each ESP
3) Strategy for the program
4) Delivery models
5) Average awareness score (from averages of each ESP awareness score)
6) Average behaviour score or text description (from analysis of behaviour audit report). *Please note that behaviour quantification is not a straight-forward process, but it may be attempted with clear indication on degree of confidence. Refer the text box in this page to download a sample behaviour scoring tool*
7) Root cause analysis for poor awareness and behaviour
8) Recommended corrective actions

8. HIMIS resources

Website: http://himis.isqworld.com

The HIMIS website consists of resources for implementing HIMIS. While this document is a methodology and cannot go in-depth into HIMIS implementation details, the website offers resources that can be used for implementing an HIMIS compliant system. The resources available include,

1) Quick tutorials about HIMIS
2) ESP's with audit and scoring guidelines
3) Awareness assessment questionnaire
4) Sample behaviour quantification tool

9. Acknowledgment and references

Bruce Schneier – The Psychology of Security - http://www.schneier.com/essay-155.pdf

The Information Security Management Maturity Model (ISM3) – www.ism3.com