HIMIS: Human Impact Management for Information Security

A model for helping organizations foster Responsible Information Security Behavior amongst the workforce.

Version 1.2

License

Versions

1.0 - 14th of June, 2010
1.1 - 26th of June, 2015
1.2 - 25th of February, 2021

Author

Anup Narayanan, CISA
Founder and CEO, Security Quotient
anup@securityquotient.io

Official Reviewers

Version 1.0
Adriana Mileidy Carrillo Garcia
Email: mileidy.carrillo@hotmail.com

Table of Contents

1. Introduction

Awareness (knowledge) is the know-how of a topic. **Competence (Skill)** is the ability to perform a task, related to a topic, and, it could be acquired or natural. **Behavior** is the response to an event or external stimulus, and, more often than not, is an observable action. An example, in the context of Information Security can illustrate this quite succinctly.

Awareness: *Knowledge (e.g. What is Two-Factor Authentication and its benefits?)*
Competence: *Skill (e.g How to configure Two-Factor Authentication in an app?)*
Behavior: *Observable Action (Actual configuring of Two-Factor Authentication in an app)*

Behavior is influenced by both *Awareness (Knowledge)* and *Competence (Skills)*. Apart from Awareness and Competence, **Behavior is ultimately influenced by *Beliefs*** (the desire for *Rewards* or the aversion to *Penalties*).

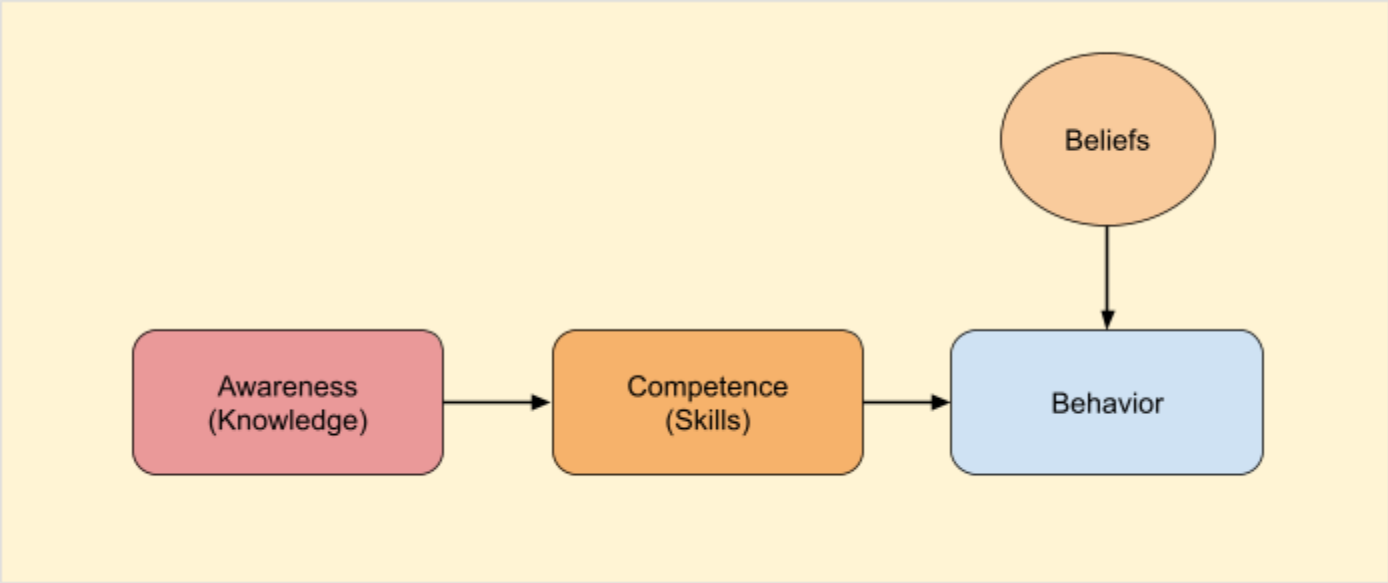

Fig 1. Behavior is influenced by Awareness, Competence and ultimately, Beliefs

If the individual believes that a specific behavior will be rewarded, it is repeated. If the belief is that the behavior will be penalised, it is not repeated.

It is important to reiterate that Awareness, Competence and Behavior are distinct but interdependent entities. An example can illustrate this well;

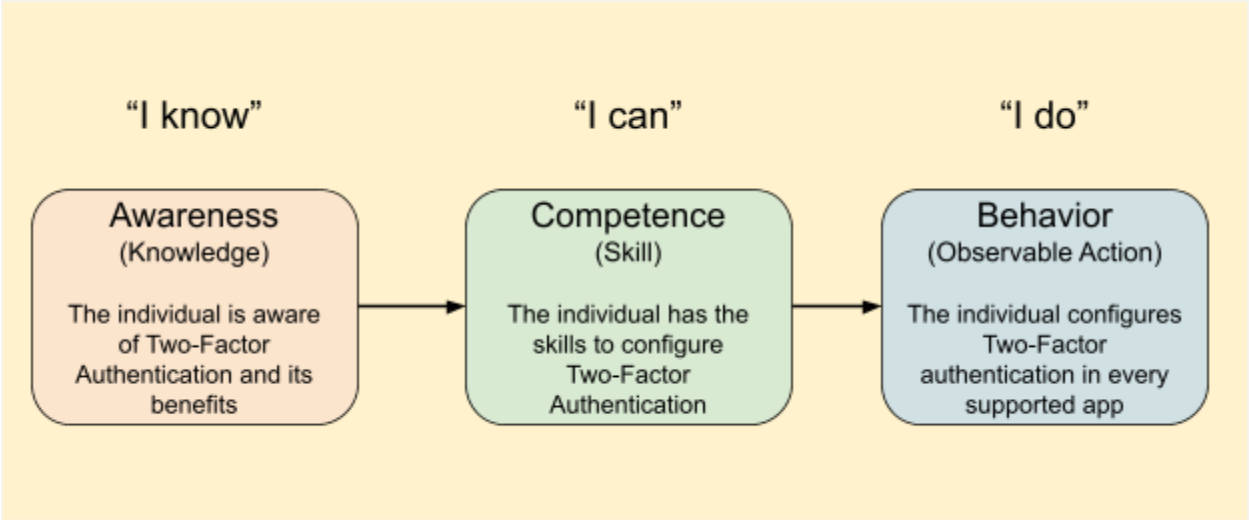

Fig 2. The difference and interdependence between Awareness, Competence and Behavior

Hence, any framework or model that aims to influence or modify behavior must consider the above differences and interdependencies while developing training programs. In deference to the above, HIMIS provides precise guidance on Awareness as well as Competence Training along-with guidance on Behavior Modification.

2. Problem Statements

The creation of HIMIS was motivated by the identification of the following problems. They are illustrated as statements below.

Statement 1: *Awareness*, *Competence* and *Behaviour* are distinct components, but the distinction is not clearly understood

It is possible that a person may be *aware*, but may not behave appropriately due to weak skills or negative beliefs. An example is the consumption of junk food. The individual may be *aware* of the ill effects, but they may still continue to consume (*behave*) the same because they are yet to experience the ill effects.

Statement 2: High awareness does not necessarily lower risks

High levels of information security awareness does not necessarily mean that information security risks have reduced. In fact, high awareness scores (measured through assessments or quizzes) are often easier to attain. Furthermore, these scores may satisfy compliance requirements, but the underlying risks in "competence" and "behavior" remain.

Statement 3: Training programs stop at ""Awareness"

Information security practitioners often stop at "awareness" and do not view "awareness" as the firsts step towards building "competence" and fostering "behavior".

Statement 4: A process-based approach for managing human risks to Information Security is absent

Though information security practitioners understand that the "human" aspect of information security is important, currently there exists no model for providing guidance. By model it is intended that there must be a process to *define* a strategy, *implement* the strategy and *measure* the effectiveness.

3 Responsible Information Security Behaviors (RISBs)

Responsible Information Security Behavior (RISB), in the context of HIMIS are positive responses or actions that an organization expects from employees when exposed to Information Security Scenarios, Events or Threats. By positive responses, it is intended that the behavioral action is oriented towards protecting the information from unauthorized access, unauthorized modification or destruction.

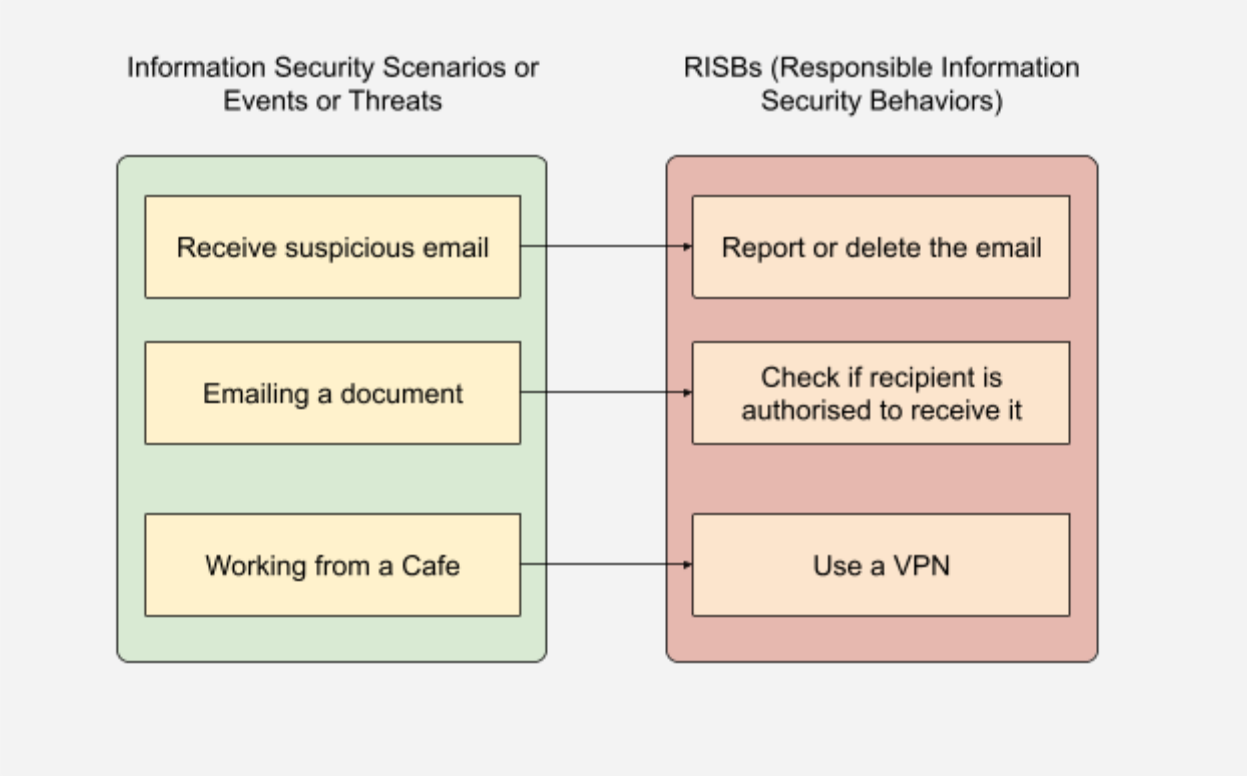

Fig 2. RISBs are the desired responses to Information Security Scenarios, Events or Threats.

RISBs are valuable to strengthen the Information Security Posture organizations, especially when technical or process-oriented controls fail. A few examples of such scenarios include new phishing variants or zero-day malware attacks.

RISBs can be fostered through;

1. Information Security Training, with focus on both;
    a. Awareness (Information Security knowledge), and,
    b. Competence (Information Security skills)
2. Fostering positive beliefs around Information Security by creating a conducive organizational environment that rewards positive Information Security Behavior while penalising the opposite (poor Behavior)

RISBs could be **common** across industry verticals or could be **specific**. Provided below are few examples of common RISBs;

Information Security Scenario, Event or Threat	**RISB (Responsible Information Security Behavior)**
Creating or storing information (e.g. storing a document in a system or cloud)	Configure access control (restrict access to unauthorised individuals, least privilege to authorised individuals)
Creating a new online account	- Using Password Managers to create and securely store highly complex passwords - Use Two-Factor Authentication
Using a browser	Using browser extensions to prevent tracking

Table 1 - Examples of common RISBs

Specific RISBs could be created in response to contractual specifications or regulatory requirements or other valid reasons. Here are a few examples;

Information Security Scenario, Event or Threat	**RISB (Responsible Information Security Behavior)**
Handling customer credit card data	Follow organization-specific categorization and storage criterion (linked to PCIDSS)
Using customer data (Personally Identifiable Information) for deep analytics	Obtain permission from customer

Sharing customer data with third party organization	Obtain permission from customer

Table 2 - Examples of organization-specific RISBs

The HIMIS model provides the following guidance on RISBs;

- Section X helps with creating an RISB check-list
- Appendix 1 provides an inventory of RISBs

3 The HIMIS Model

The HIMIS model provides step-wise guidance to help organizations foster Responsible Information Security Behavior (RISBs) amongst the workforce through *Awareness* (Knowledge) and *Competence* (Skills) training by creating an ecosystem that *rewards* positive Cyber Security *Behavior* or *penalises* negative Cyber Security Behavior.

Note - The RISBs are usually derived from business, regulatory or client-specific requirements (Section X explains the steps in creating a list of RISBs that are specific to your organization).

3.1 The Approach

HIMIS adopts the principle that Behavior is fostered through Awareness, Competence and Beliefs (*refer Section 1 - Introduction*). HIMIS adopts this approach with suitable enhancements for Information Security.

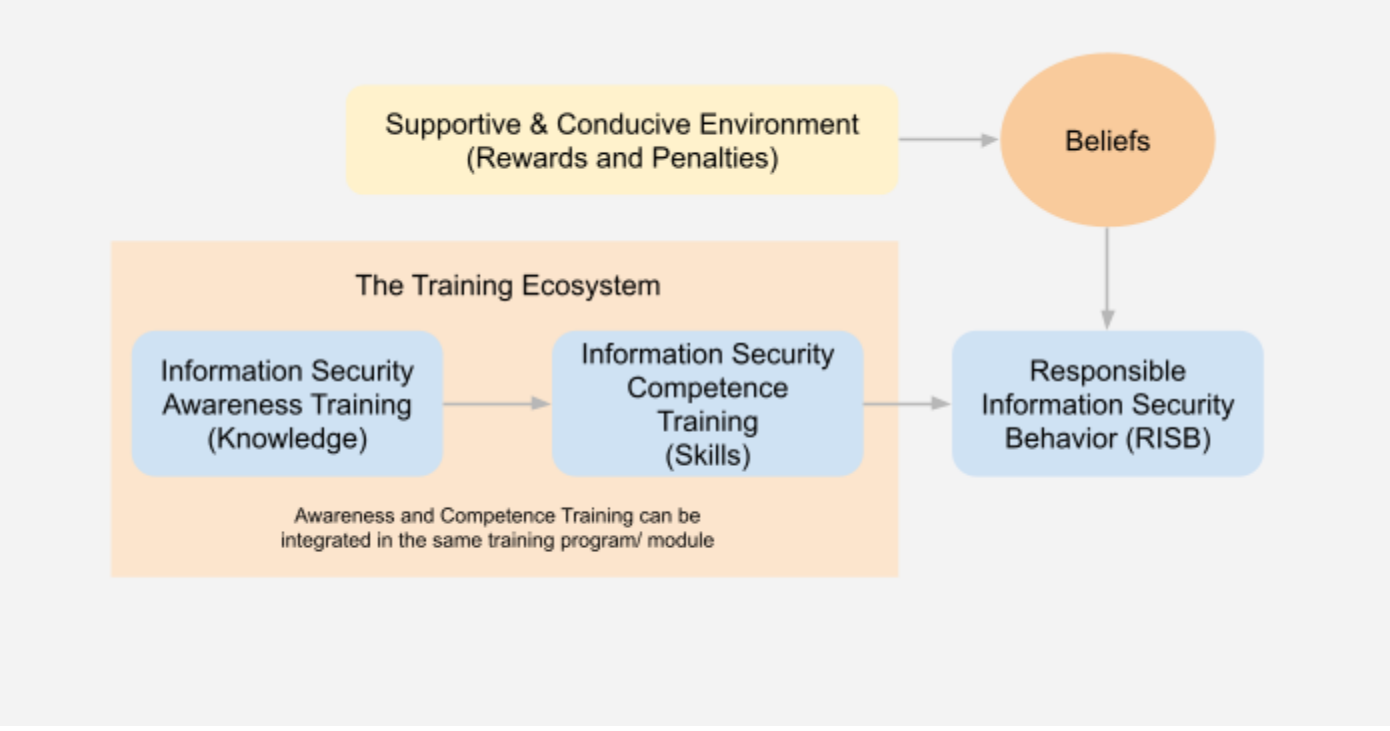

Fig 3. The HIMIS Approach

3.2 The Model

The HIMIS approach is condensed into a 4-step model consisting of four phases viz. ***Define***, ***Deliver***, ***Measure*** *and* ***Optimise***, developed in alignment with the Deming (Plan-Do-Check-Act) model.

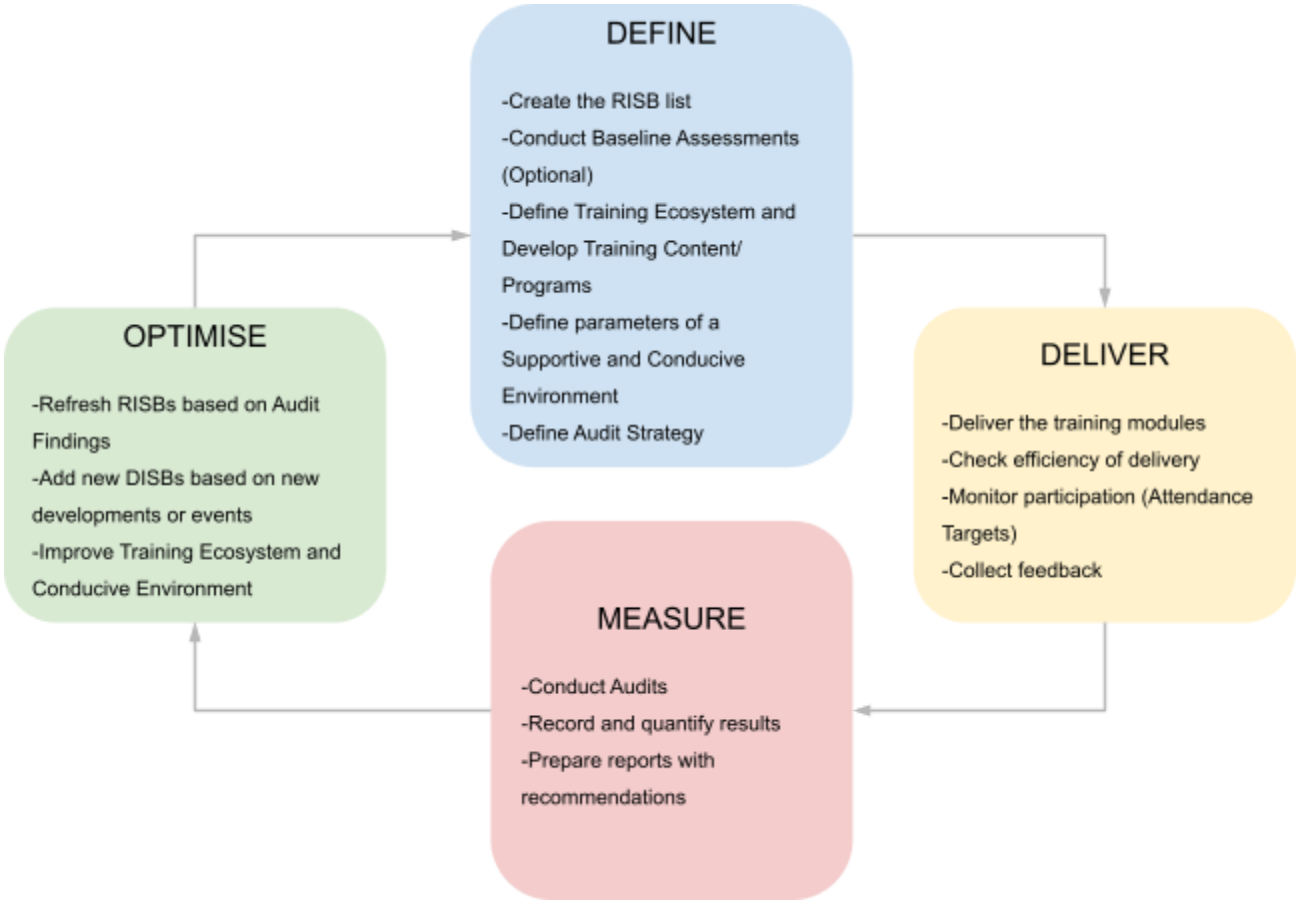

Fig 4. The HIMIS model

The Define Phase

This is the most important phase as it concerns itself with laying a strong foundation of the model. This phase covers;

1. Creating a list of Responsible Information Security Behaviors (RISBs)

2. Conducting **Baseline Assessments** to assess the current levels of Awareness, Competence and Behavior
3. Defining a **Training Ecosystem** for **delivering Cyber Security Training**, with precise focus on both;
    a. Awareness (Knowledge) Training, and,
    b. Competence (Skills) Training
4. Defining the parameters of a **supportive and conducive organizational environment** which rewards positive Information Security behavior and penalises poor behavior
5. Defining an **Auditing Framework** to measure the effectiveness of the model

Refer Section X for more information on the Define Phase

The Deliver Phase

This phase focuses on the actual delivery of the training program or content along-with the following parameters. Specifically;

1. Deliver the training program or content
2. Check efficiency of delivery
    a. Receipt of content
    b. Efficiency of the delivery/ Quality of the trainer
3. Feedback collection
4. Monitoring attendance/ participation

Refer Section X for more information on the Deliver Phase

The Measure Phase

In this phase, the Auditing Framework defined in the first phase (Define) is put to work. The audit will be done on a sampling basis and will focus on;

1. Efficiency and Quality of Training

2. Observable change in;
    a. Awareness
    b. Competence
    c. Behavior
3. And, other observations

It is important to note that the Audits will clearly differentiate between "Awareness, Competence and Behavior".

Refer Section X for more information on the Measure Phase

The Optimise Phase

In this final phase, the audit reports are analysed. Following the analysis, these actions could follow.

1. Refinement or addition of RISBs
    a. Based on business needs (Contractual requirements, Regulations)
    b. Triggered by new security events (new Cyber Attacks)
    c. Triggered by new technologies (5G, IoT)
2. Change in strategy for training
3. Change parameters of the organizational environment by refining rewards and penalties for Information Security Behavior

Refer Section X for more information on the Optimise Phase

4. The Define Phase

The “Define” phase is the most important part of the model as it concentrates on establishing the foundation. The robustness and efficiency of all subsequent phases depend on how well the “Define” phase is established. This phase covers -

1. Creating the RISB (Responsible Information Security Behavior) list
2. Conducting Baseline Audits (optional),
3. Defining the Training Ecosystem
4. Developing Training Content
5. Defining the parameters of a supportive and conducive environment, and,
6. Defining the Auditing Framework.

4.1 Creating the RISB (Responsible Information Security Behavior) list

Creating the RISB answers the question - *How do I expect my employees to react or respond when facing an Information Security event, scenario or threat?* RISBs can be created by considering various inputs.

Fig 5. Inputs for creating RISBs

The table below provides examples of RISBs for each input category.

Information Security Scenario, Event or Threat	Type	RISB (Responsible Information Security Behavior) example
Receiving a suspicious email	Common best practices	Report or delete the email
Creating a highly confidential report	Security Policies	Apply the document classification label as specified in the organization's security policies
Storing Customer's PII (Personally Identifiable Information)	Compliance/ Regulations (e.g. PCIDSS)	Store in an encrypted repository
Working from a Cafe	Work Environment	Use a VPN
Creating a new online account	Learning from Incidents	Configure Two-Factor Authentication (based on user-credential breaches of well-known sites)
Installing a new IoT device at home	New technology developments	Use a separate WiFi network for IoT device and keep the WiFi network for work/business isolated
Installing a new application	New security event/ attacks	Apply latest patches/ updates

Table 3 - Inputs, types and RISBs

Refer Appendix 1 for a comprehensive list of RISBs.

4.2 Conducting Baseline Audits

The Baseline Audits, though optional, helps organizations understand the current posture of Information Security Awareness, Competence and Behavior. This helps in establishing an initial benchmark, with which future audit results can be compared with.

Since the approach used for Audits must be the same across each iteration, the practitioner may refer to the following sections of this document for guidance on conducting Baseline Audits.

Section X - Creating the Auditing Framework
Section Y - Mesure

4.3 Defining the Training Ecosystem

Having a robust training ecosystem is essential to ensure the success of the framework. A robust ecosystem will ensure that the training reaches the target audience, is visible through multiple communication channels at a regular frequency and is easily accessible. Hence the training ecosystem must address the following requirements viz.

- Audience
- Format & Visibility
- Coverage
- Frequency

4.3.1 Audience

“Audience” refers to the target **group of people** (employees, contractors, partners and other interested parties) that must be covered under the information security

awareness program. Audience does not mean employees alone. Rather, the term indicates every entity that must be part of the awareness program.

For example;

- Anti-phishing training may be required for partners and suppliers
- Access Control or Two-Factor Authentication training may be required for all entities who access the company's online assets

Hence, the first step in the HIMIS framework is to understand who your audience is and to define them.

4.3.2 Format & Accessibility

"Format" indicates the different types of information security awareness content such as "*Verbal, Paper or Digital*".

"Accessibility" indicates the channel or medium through which the content is accessible. Accessibility channels must be selected to ensure maximum coverage and participation by the audience. An example comparing Format and Accessibility is provided below.

Format	Accessibility (with examples of channels or mediums)
Verbal (Trainer led classroom sessions)	Classrooms or Training Rooms
Paper (Posters, Flyers)	Reception, Cafeteria, Hallways etc.
Digital (Courses, Videos, Mailers, Games, Virtual Reality Training etc)	Learning Management Systems (LMS), Email, Collaboration Channels (Teams, Slack etc.), Intranet Portal

The organization can choose one or more of the channels to ensure maximum coverage. For example, for organizations that have a large workforce, classroom sessions may not be effective as it 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.

4.3.3 Coverage

"Coverage" indicates the percentage of the Audience that must be covered under the training program. The following factors must be considered while defining coverage targets.

4.3.3.1 Efficiency of Delivery Channels and Mediums

The channels (*refer Format & Accessibility*) through which the training content is made accessible must deliver the content efficiently. For example,

- If emails are used to convey the messages, then every member of the audience must have access to emails
- If streaming videos are used to convey the messages, the videos must stream without interruption
- Check compatibility (responsiveness) of the content on Desktop, Laptop, Mobile Devices and Tablets
- If classroom sessions are used to convey the messages, then the trainer must be well versed in the subject and should be able to articulate the subject well

4.3.3.2 Coverage targets and tolerable deviation

Though the aim is to attain 100% coverage, it may not be possible due to various factors. These factors could be technical, procedural, time, audience attitude or poor enforcement, to name a few.

An example of a coverage target is;

"*80% of the audience must complete the training program within the first 90 days. The target will be revised to 90% for the subsequent 90 days*".

Defining tolerable deviations allows the organization to set reasonable goals.

4.3.3.3 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 pertinent factors*

The feedback mechanism is linked to "Step 2 – Deliver", 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.

4.3.3.4 Confirmation of receipt

An important component that makes coverage to be termed successful is confirmation of receipt of the training content. Examples are;

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)
3. A click-tracking software that records how many people clicked a digital content

4. A quiz or survey at the end of a content that records how many people completed the content and attempted the quiz/ survey

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

4.3.4 Frequency

"Frequency" indicates the gap between any two deliveries of training content. Frequency is critical because it influences "retention". If the frequency is low (i.e. the gap between two deliveries is high), the program loses momentum and the workforce remembers less about 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.

An example is provided below.

Format	Accessibility (with examples of channels or mediums)	Frequency (Suggested)
Verbal (Trainer led classroom sessions)	Classrooms or Training Rooms	Once every 6 months or yearly
Paper (Posters, Flyers)	Reception, Cafeteria, Hallways etc.	Posters to be changed every 60 days
Digital (Courses, Videos, Mailers, Games, Virtual Reality Training etc)	Learning Management Systems (LMS), Email, Collaboration Channels (Teams, Slack etc.), Intranet Portal	Fortnightly or monthly

4.4 Developing Training Content

The training content should consider both “awareness” and “competence” development. This section addresses both these factors independently.

4.4.1 Information Security Awareness (Knowledge) Training

Information security awareness training is the first component of the training process. Please note that both “awareness” and “competence” training can be part of the same training interaction/ module.

The security awareness training must address the following factors viz.

- Topics and Business relevance
- Impact visualization
- Clarity
- Cultural factors

4.4.1.1 Topics and 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 and client expectations about information security and more.

4.4.1.2 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 visualizes the same to the learner. Usually information security professionals

can visualize the impact of poor security awareness and practices, due to their knowledge of the domain. But, the workforce may not be able to visualize the impact. Hence, training managers must endeavour to incorporate “impact visualization” as much as possible in the information security awareness content.

4.4.1.3 Clarity

Style must not be sacrificed for substance. 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.

4.4.1.4 Cultural factors

In order for the training content to be absorbed effectively, cultural nuances must be incorporated in the content. This could be;

- Using the native language of the Audience in the training content
- Integrating brand elements such as logo, color scheme, fonts etc
- If human characters are used, they should resemble the workforce of the geographical region in appearance

Consideration of cultural factors has a significant impact on the way the workforce understands the content.

4.4.1.5 Retention measurement

“Retention measurement” indicates a method to measure how much the workforce has “**understood and remembers**” after the information security awareness delivery. The retention measurement methods that can be used are,

a. Personal interviews
b. Surveys, and,
c. Quizzes

4.4.2 Information Security Competence (Skills) Training

Cyber Security Competence can be defined as the ability of an individual to implement the correct Cyber Security practices while handling valuable information. Examples of such competencies are;

- *Using password managers to create extremely strong passwords,*
- *Adding Two-Factor Authentication over and above using strong passwords,*
- *Giving only the most necessary permissions to apps,*
- *Disabling location tracking and configuring other privacy settings on computing devices,*
- *Correctly identifying and reporting phishing emails to the help desk etc.*

4.4.2.1 Developing Cyber Security Competencies

Cyber Security Competence is acquired or influenced by three factors – Knowledge, Skills and Natural Abilities.

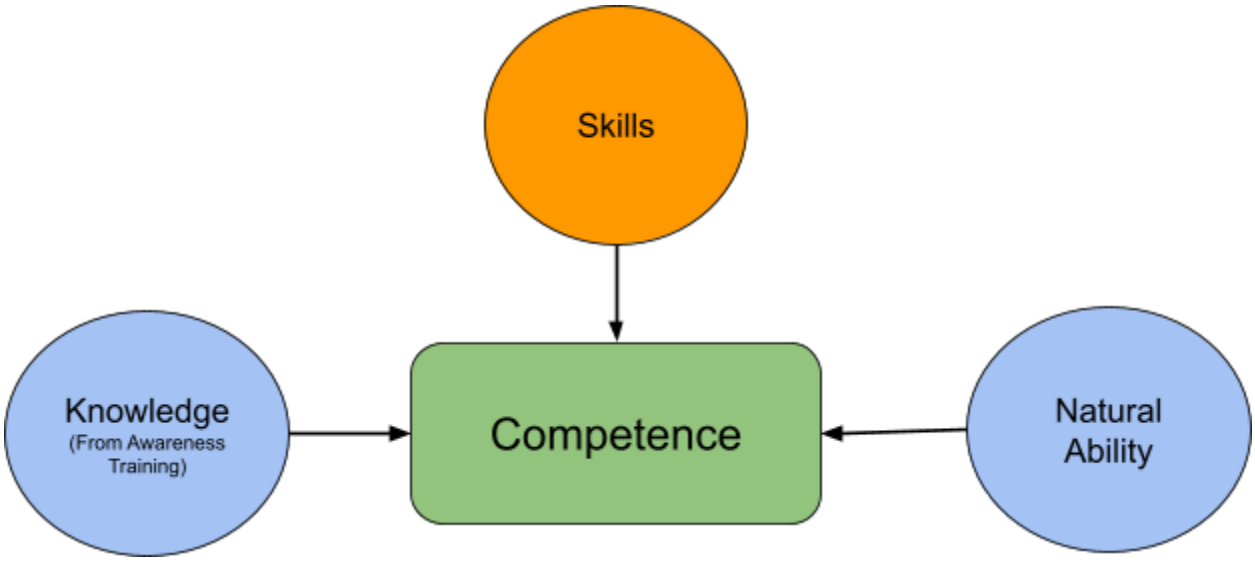

Fig 2. Developing Cyber Security Competencies

Knowledge

Cyber Security Knowledge is acquired through high quality awareness training. The training conveys important background information, cyber security facts, organizational policies, case studies based on security incidents and best practices.

Skills

Cyber Security skills are developed using specialized training that uses the time-tested principle of Learning by Doing. The principle of Learning by Doing is highly effective as it uses the concept of Immersion, Analysis, Decision and Outcome. An example of the application of this principle is awareness training using Cyber-Risk Simulations. These simulations recreate real security incidents or events that enable the learner to experience them in an almost real environment. Further, it simulates the learner to make decisions and learn from the outcomes of these decisions.

Natural Ability

Natural abilities are inborn. Examples are innate traits, personal qualities and attributes. In the context of Cyber Security, natural abilities may not hold warrant as Cyber Security skills have to be learned. But, qualities such as diligence and observation skills aid tremendously in enhancing these skills.

4.4.2.2 The 'Learning by Doing' Method

The 'Learning by Doing' method is a time-tested method for skills training.

Learning is best when it is hands-on. Performing an activity and analyzing the outcomes is a powerful way to learn. Every outcome leads to experience. By acquiring experiences over time, one builds a knowledge base. To drive secure Cyber Security behavior, the learning must follow four principles – Immersion, Analysis, Decision and Outcome.

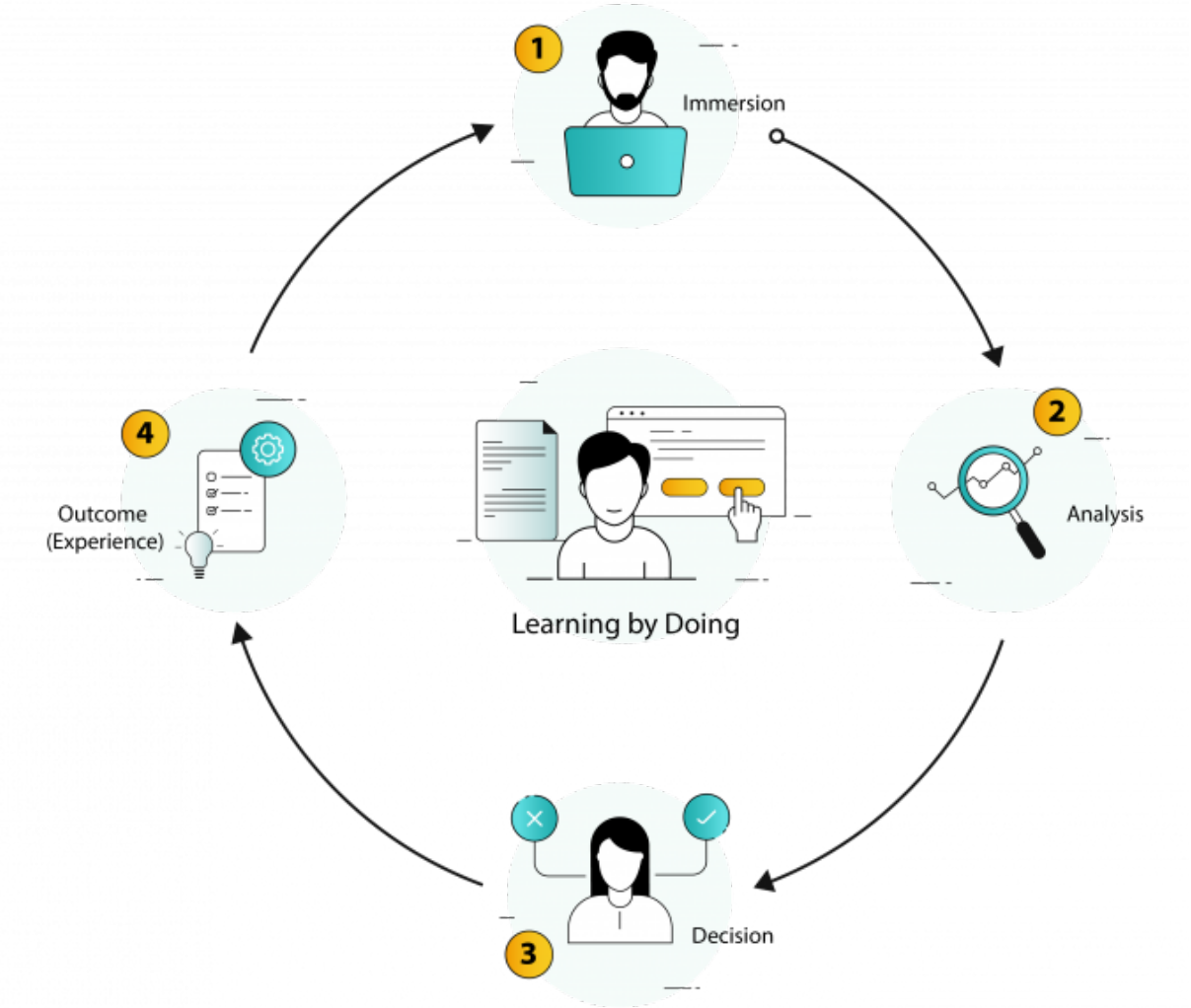

Fig 3. The Learning by Doing method

Immersion

The learning experience must include risk simulations that re-create Cyber-risk scenarios. This enables the learner to immerse themselves and feel the risk.

Analysis

Every risk presents an opportunity for analysis. The learner must take a choice to mitigate the risk and make a decision.

Decision

Decisions influence the outcome, resulting in a positive or negative Cyber Security event. Decisions may be right or wrong. Nevertheless, they lead to an outcome (experience), either good or bad.

Outcome (Experience)

If the experience is good, the risk is mitigated, the learner undergoes a positive experience and their confidence is built. As a result the behavior is repeated. If the outcome is bad, the behavior is avoided or substituted with the right behavior.

For more information on the method, please refer to;

https://en.wikipedia.org/wiki/Learning-by-doing

https://en.wikipedia.org/wiki/Experiential_learning

4.5 Defining a conducive and supportive environment

The ultimate goal of a Cyber Security Training program is to foster responsible Cyber Security Behavior. As discussed earlier in this document, a conducive and supportive environment is critical to develop positive behavior.

4.5.1 Cyber Security Behavior

Cyber Security Behavior is the way in which a person reacts when confronted with a cyber security situation such as an attack or incident. It is also the security controls they practice while performing everyday activities such as sending emails, working with sensitive documents or working with computing devices.

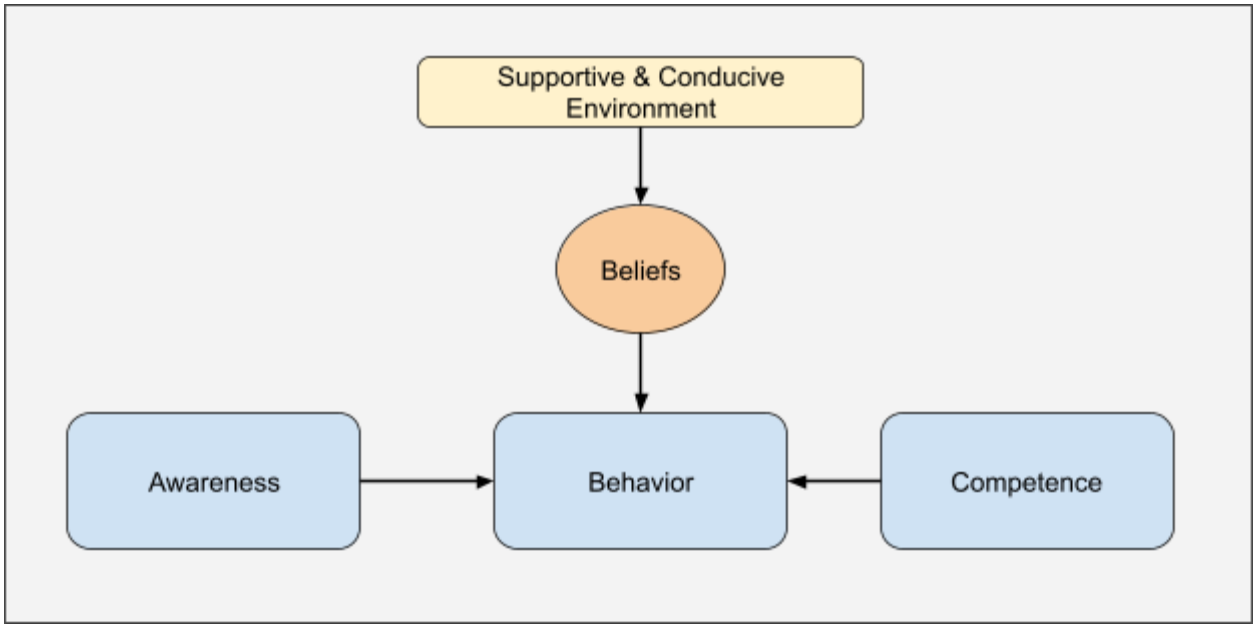

Fig 4. Behavior is influenced by Awareness, Competence and Beliefs. Beliefs are influenced by the surrounding environment.

Awareness and Competence training is fundamental to developing positive Cyber Security Behavior. But, that in itself is not enough. **Positive behavior is developed in a conducive environment where the behavior is rewarded (or, in case of poor**

Cyber Security behavior, it is penalised). To create such a positive environment, Cyber Security training frameworks must evolve to influence three factors – **Beliefs, Attitude** and **Action**.

4.5.1.1 Beliefs

Beliefs are often personal and must have evolved outside the controls of the organization. But, organizations can influence and create a positive belief in Cyber Security by showing a larger picture. The larger picture must demonstrate;

– The influence of Cyber Security on customer trust and subsequently the growth and success of the organization

– The positive impact of Cyber Security for each employee in terms of enabling them to perform their jobs securely

– Finally, the indirect and positive influence of Cyber Security in their career growth

Organizations must take the effort to showcase the reward of positive Cyber Security behavior. The rewards are – **growth for the organization and indirectly, growth for the employee.**

4.5.1.2 Attitudes

Attitude is a preconceived opinion or approach. Often Cyber Security suffers because employees perceive security practices as obstacles that slow down work. Cyber Security practices increase the quantum of time and effort to everyday tasks. Therefore, the challenge is to remove this negative attitude around Cyber Security as an additional burden.

Again, the solution is in showing the larger picture as to how small steps by every employee helps in strengthening the Cyber Security posture of the organization. By consistently repeating and supporting this message, negative attitudes around Cyber Security can be removed.

4.5.1.3 Action

Cyber Security actions are observable Cyber Security practices. By repeating these actions, the behavior becomes inculcated or second nature.

4.5.2 Creating a conducive environment

To create a conducive environment to foster positive Cyber Security Behavior, organizations may consider the following strategies.

4.5.2.1 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.

4.5.2.2 Enforcement or disciplinary strategies

This approach focuses on specifying the penalties for non-compliance. Non-compliance here means a deviation from the positive Cyber Security Behavior. Often, enforcement or disciplinary strategies have a “tone of repercussion”, but it is necessary.

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.

4.6 Defining the Auditing Framework

While the actual audit is executed in the 3rd phase (Measure), it is essential to define the essential elements and the strategies of the audit at the beginning of the program.

4.6.1 Audit Strategy

The audit strategy must consider the following elements;

4.6.1.1 Selection of RISBs

Select the RISBs the organization has prioritised and prepare the audit strategies to audit conformance. For each RISB;

- The awareness component of the RISB must be checked
- The corresponding competence component of the RISB must be checked
- Finally, the behavior component of the RISB must be checked

4.6.1.2 Audit Methods

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

- Interviews
- Surveys
- Quizzes
- Observations
- Log review
- Data analysis
- Incident report review

4.6.1.3 Efficiency of the ecosystems

Audits must evaluate the efficiency of the training ecosystem. This is accomplished by checking factors such as Delivery Speed, Attendance, Learner Feedback etc. Further, the audits must evaluate the influence of the organizational environment in terms of changing employee Cyber Security Behavior.

5.6.1.3 Audit Teams

A team of independent auditors, either external or internal (cross-functional) must be identified and trained on the audit methods before the audits.

For more information on Auditing, please refer to Section X - Measure

5. The Deliver Phase

While the "Define" phase was concerned with strategy and planning, it is the "Deliver" phase where the work or action begins. It is in this phase that the training program is rolled out across the organization. Hence, this phase is about ensuring that training reaches the target audience and is easy to access, understand and complete.

The key activities in this phase are - Efficiency monitoring, Attendance (Participation) monitoring and Feedback collection.

5.1 Efficiency monitoring

Efficiency tracking is linked to the "Efficiency of the delivery channels and mediums" mentioned in the "Define" phase. The objective is to ensure that the training content is received and consumed in a timely manner without interruptions. The objective can be tracked by sampling. Examples are;

- Check if videos are streaming smoothly even at peak load
- Check if videos are viewable on all types of devices - Desktops, laptops, mobile devices and tablets
- Check the quality of the trainer by attending classroom sessions

5.2 Attendance/ Participation Monitoring

Attendance targets are linked to the Coverage targets mentioned in the "Define" phase. The objective is to ensure that the targets are met. For monitoring attendance, the following strategies are recommended;

- Click tracking if the content is delivered online

- Completion tracking if the content is delivered via a Learning Management System (LMS) using SCORM or AICC or xAPI trackers
- Manual registers if the training is done via classroom sessions with an expert trainer

5.3 Retention Measurement

"Retention measurement" indicates a method to measure how much the learner has understood and remembers at the completion of the training. These targets are linked to the retention measurement targets mentioned in the Define phase. Retention measurement methods must be determined beforehand. Some examples are;

a. Personal interviews
b. Surveys
c. Quizzes

5.4 Feedback Collection

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*

6. The Measure Phase

The “Measure” phase concerns itself with checking the effectiveness of the program. Since, the HIMIS model addresses Awareness, Competence and Behavior independently, the measurements must cover each of these components independently to the maximum extent possible.

6.1 The Audit Approach

The approach is centred around selection of RISBs that are identified during the Define phase.

1. Select the RISBs to be audited
2. Each components of the RISB must be audited independently;
   2.1. The Awareness Component
   2.2. The Competence Component
   2.3. The Behavior Component
3. The reports are created based on the audit findings and submitted to interested parties
4. Decisions based on the audit reports are taken and implemented

A sample audit check-list is provided below.

RISB	Awareness (I know)	Competence (I can)	Behavior (I do)
Two-Factor Authentication	Knows what 2-FA is	Can configure 2-FA	Applies 2-FA in a real-life scenario
Phishing	Knows what phishing is	Can identify phishing emails	Correctly deletes or identified phishing emails in a real-life scenario

For a comprehensive audit-checklist, please refer Appendix Y

6.2 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".

6.3 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 RISB the following may be considered:
    - Interviews
    - Assessments/ Quizzes

- For auditing the competence components of the RISB the following may be considered:
    - Observations
    - Practical assessments
    - Virtual Reality based assessments

- For auditing the behaviour component of the RISB the following may be considered:

- 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 pattern can be observed through log reviews of corresponding systems*
- Data Analysis : *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).*

6.4 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 RISB's like "mobile computing security". The behaviour component of this RISB 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.

6.5 Behaviour may not be always visible

The reason why audit methods include "data analysis, 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.

6.6 Quantification and presentation of audit reports

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

6.6.1 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,

- What is the current awareness, competence and behaviour score?
- How much has awareness, competence and behaviour increased (or decreased)?

HIMIS does not aim to be prescriptive in its 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.

- 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
- Quantifying competence and behaviour may not be possible directly and indirect methods may have to be used. For example,
    - Number of violations found for an RISB
    - Impact of the violation
    - *A score derived by consideration of “a” and “b” above*

6.6.2 Content of the audit report

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

- Introduction with reasons for the information security awareness, competence and behaviour management program
- List of RISB's and the reasons for the selection of each RISB
- Strategy for the program
- Delivery models
- Average Awareness score (from averages of each RISB awareness score)
- Average Competence score
- 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.*
- Root cause analysis for poor awareness, competence and behaviour
- Recommended corrective actions

7. The Optimise Phase

This phase concerns itself with acting upon the findings of the audit apart from analysing others events to make improvements in the Cyber Security Behavior management program. Since this phase is about making decisions, which is specific to each organization, the following recommendations may be useful in the process.

7.1 Reassess RISBs and associated goals

The audit findings will usually trigger an assessment of the RISBs and whether there is an improvement in the Cyber Security behavior of employees. This could lead to important decisions regarding;

- Changes in the organizational environment (Refer - Defining a Supportive and Conducive Environment)
- Addition, deletion or modification of RISBs
- Improving the training ecosystem
- Making changes in the audit approach

7.2 Analysis of incidents and external events

During the period of the program there might have been internal security incidents that may trigger analysis. These analyses may lead to addition/ modification of RISBs. Further, there might be external events such as new cyber attacks or the emergence of new technologies that may trigger the need for new Awareness, Competence and Behavioral requirements.

7.3 Alignment with Compliance/ Regulatory Programs

It makes sense that the program be aligned with Compliance or Regulatory programs (e.g. ISO 27001, PCI DSS, NIST etc.) The HIMIS model helps to satisfy the training controls mandated by the compliance/ regulatory guidelines. The audit reports from the Measure phase can act as an input to analyse human-related risks in the journey towards compliance.

8. Summary

Behavior is influenced by Awareness (Knowledge), Competence (Skills) and ultimately Beliefs (the expectation of rewards or aversion of punishments). In the context of Cyber Security, HIMIS is an implementable model for fostering responsible Cyber Security behaviour amongst the workforce of an organization.

HIMIS provides a detailed, stepwise approach that organizations can adopt and enhance in order to Define, Deliver, Measure and Optimise continuously. The model is measurable in order to ensure continuous improvement.

Appendix 1 - Responsible Information Security Behavior List

Appendix 2 - Sample HIMIS Audit Checklist