Over recent decades organisations have spent countless millions on information security awareness activities. The rationale behind this approach was to take their biggest asset – people – and change their behaviours, thus reducing risk by providing them with knowledge of their responsibilities and what they need to do.

But have these activities succeeded? Information gathered from ISF Members would tend to indicate not...or at least not fully.

It is true that organisations continue to heavily invest in ‘developing human capital’. No CEO’s speech or annual report would be complete without stating its value. The implicit idea is that awareness and training always deliver some kind of value with no need to prove it – employee satisfaction was considered enough. This is no longer the case. Leaders now more often demand return on investment forecasts for the projects that they have to choose between, and awareness and training are no exception. Evaluating and demonstrating their value is becoming a business imperative.

Analysis of the data supplied by Members at workshops around the world identified six fundamental reasons why information security awareness activities are failing:

1. Solutions are not aligned to business risks
2. Neither progress nor value are measured
3. Incorrect assumptions are made about people and their motivations
4. Unrealistic expectations are set
5. The correct skills are not deployed
6. Awareness is just background noise.

Conclusion? A new approach is needed. The time has come to move away from mere knowledge to the embedding of behaviours that reduce information security risk. The ISF report From Promoting Awareness to Embedding Behaviours offers Members an Approach to do that. The key messages from the Report and Approach are shown overleaf.
The ISF Approach

The ISF recognises that there is no single process or method for introducing information security behaviour change, as organisations vary so widely in their demographics, previous experiences and achievements, and goals. The ISF Approach – depicted on the opposite page – provides a structure, based on the key principles from the research, that can be adapted by organisations to meet their individual needs.

The ISF Approach is offered to spur Members on to introduce a behaviour change programme and thus reduce their information security risk. This Approach should be used as a guide with its content adapted by security professionals and others to individual circumstances, selecting and modifying the Stages, Phases and Steps to best fit their unique requirements.

The ISF research for From Promoting Awareness to Embedding Behaviours identified ten principles which should form the basis of Members’ programmes:

1. Let risk drive solutions
2. Continue to look for alternatives
3. Embed positive behaviours
4. Empower people
5. Set a realistic timescale
6. Aim for ‘stop and think’
7. Move from ‘self’ to ‘self’
8. Tap into the right skills
9. Identify and integrate champions into efforts
10. Hold people accountable

Key actions to embed positive information security behaviours

- Ensure each solution has a direct link to business requirements and addresses site or meta risks.
- Form a strong baseline and measurement criteria based on risk as a starting point.
- Challenge complex systems or cumbersome processes rather than forcing behaviour change to accommodate them.
- Strive to ensure that new systems and processes are as simple and user-friendly as possible.
- Promote and value behaviours that facilitate people playing an essential role in strengthening organisational resilience.
- Enable people to recognise key moments and make the right decisions.
- Win hearts and minds through trust, motivation, and empowerment.
- Position people to make information security a critical element of “how things are done around here.”
- Plan in detail, but think in terms of three to five years for lasting change.
- Stop looking for a silver bullet – behaviours across an organisation don’t change overnight.
- Prepare people to make the right decisions – or to know when to consult: if everyone stops and thinks at key moments, the battle is won.
- Do not attempt to train people for all occasions – it’s impossible in today’s business environment.
- Design persuasive solutions which are tailored to the risk profile of segmented audiences.
- Recognise that “one size fits all” solutions typically fail to engage everyone on a personal level.
- Identity and deploy expert skills to define and implement solutions which are distinctive.
- Ensure the longevity of the programme through a strong brand and identity.
- Identify a network of information security champions from the business to help introduce and sustain positive information security behaviours.
- Ensure the champions are trained and prepared to undertake their role with confidence.
- Reward good behaviours.
- Address untenable behaviours constructively – in the same way as any other sub-standard performance.
Where next?

From Promoting Awareness to Embedding Behaviours helps organisations understand what Members are doing about security awareness and behavioural change. This includes presenting what ‘good practice’ looks like, and proposing new and creative ideas that will improve or augment what leading ISF Member organisations already have in place. The research identified four requirements for future success:

1. Develop a risk-driven programme
2. Target behaviour change
3. Set realistic expectations
4. Engage people on a personal level.

Input was gathered from discussions and one-on-one interviews with security practitioners, directors, and CISOs; thought leadership provided by the ISF Global Team and the ISF Advisory Board; workshops and online meetings with ISF Members around the world; ISF Member case studies; and research carried out for other ISF projects.

The report is supported by an implementation space on the ISF Member website, ISF Live, which contains a facilitated forum for Members to discuss related issues and solutions, along with additional resources including a webcast and presentations.

The From Promoting Awareness to Embedding Behaviours report is available free of charge to ISF Members, and can be downloaded from the ISF Member website www.isfflive.org. Non-Members can purchase the report by contacting Steve Durbin at steve.durbin@securityforum.org.

Contact
For more information, please contact:
Steve Durbin, Managing Director
US Tel: +1 (347) 767 6772
UK Tel: +44 (0)20 3289 5884
UK Mobile: +44 (0)7785 953 800
Email: steve.durbin@securityforum.org
Web: www.securityforum.org

About the ISF
Founded in 1989, the Information Security Forum (ISF) is an independent, not-for-profit association of leading organisations from around the world. It is dedicated to investigating, clarifying and resolving key issues in cyber, information security and risk management by developing best practice methodologies, processes and solutions that meet the business needs of its Members.

ISF Members benefit from harnessing and sharing in-depth knowledge and practical experience drawn from within their organisations and developed through an extensive research and work programme. The ISF provides a confidential forum and framework, which ensures that Members adopt leading-edge information security strategies and solutions. And by working together, Members avoid the major expenditure required to reach the same goals on their own.

Disclaimer
This document has been published to provide general information only. It is not intended to provide advice of any kind. Neither the Information Security Forum nor the Information Security Forum Limited accept any responsibility for the consequences of any use you make of the information contained in this document.

Reference: ISF 14 02 03 Copyright © 2014 Information Security Forum Limited. All rights reserved. Classification: Public, no restrictions

From Promoting Awareness to Embedding Behaviours
Secure by choice, not by chance

Over recent decades organisations have spent countless millions on information security awareness activities. The rationale behind this approach was to take their biggest asset – people – and change their behaviours, thus reducing risk by providing them with knowledge of their responsibilities and what they need to do.

But have these activities succeeded? Information gathered from ISF Members would tend to indicate not...or at least not fully.

It is true that organisations continue to heavily invest in ‘developing human capital’. No CEO’s speech or annual report would be complete without stating its value. The implicit idea is that awareness and training always deliver some kind of value with no need to prove it – employee satisfaction was considered enough. This is no longer the case. Leaders now more often demand return on investment forecasts for the projects that they have to choose between, and awareness and training are no exception. Evaluating and demonstrating their value is becoming a business imperative.

Analysis of the data supplied by Members at workshops around the world identified six fundamental reasons why information security awareness activities are failing:

1. Solutions are not aligned to business risks
2. Neither progress nor value are measured
3. Incorrect assumptions are made about people and their motivations
4. Unrealistic expectations are set
5. The correct skills are not deployed
6. Awareness is just background noise.

Conclusion? A new approach is needed. The time has come to move away from mere knowledge to the embedding of behaviours that reduce information security risk. The ISF report From Promoting Awareness to Embedding Behaviours offers Members an Approach to do that. The key messages from the Report and Approach are shown overleaf.