How To Make Information Security Awareness Training Truly Effective

Iain McLeod is Managing Director at SAI Global Compliance EMEA, an international business that helps organizations implement effective information security awareness solutions. In this white paper, he reflects on recent experiences in the information security field and considers some best practices to consider when planning, developing and implementing an enterprise-wide employee awareness program.

Summary

• Information security awareness training – an essential part of an effective security strategy
• Some common misconceptions about security awareness training
• 11 key principles for making information security awareness training truly effective

“\textit{I can have all the gadgets in the world, but if people don’t understand the basics – like don’t send things over the internet, and make sure your files are put away – well, I can spend millions on security, and it won’t do any good.}”


Information Security Awareness Training - An Essential Part of an Effective Security Strategy

Large companies around the world spend millions of dollars on technology to manage their information security problems, but many are failing to address the human element of information security – their employees. Employees are one of the biggest threats to information security – and a threat that can only in part be protected by technology. Recent surveys in the USA and the UK have addressed this issue and have concluded that information security awareness and education programs should form an essential part of a security strategy – and be a top priority for the Board of Directors.
Organizations that are really serious about information security need to ensure that effective employee awareness training is used alongside technology – forming a stronger and more robust level of protection. Those who are failing to recognize the importance of end-user awareness training could be exposing themselves to serious risk.

**Some Common Misconceptions About Security Awareness Training**

SAI Global has worked with organizations worldwide helping to plan, develop and implement security awareness programs. In delivering these projects, we have learned that there are several common misconceptions that exist:

**The publication of IS policies/procedures is the answer to awareness**

Unfortunately, the mindset of many organizations is that effective security awareness training simply requires creating information security policies and publishing them in either paper or digital form. Their failure has been to recognize that employees need to be ‘sold to’ and convinced that information security is good for the organization and good for them. Effective security awareness training is about getting ‘buy-in’ from employees. This involves changing behaviors to create a more responsible and vigilant security culture within the organization as a whole. This requires a much more focused, imaginative and proactive training approach.

**The ISO should be responsible for the planning, development and implementation of an awareness program**

Organizations tend to forget that ISOs are not training and communication experts; they are information security experts. They may be capable of writing information security policies, but it is unlikely that they will be able to develop an effective training and awareness program that will be successful at training general employees. It should be recognized that ISOs would need additional help – either internally via training experts, or externally using a consultant or vendor that specializes in security awareness solutions or employee communication. Annual or one-off training will work. In the short-term, these solutions will certainly help, but awareness training is an ongoing process – not a once a year, or one-off initiative. Just like with any successful marketing campaign, it is important to raise and maintain awareness levels consistently to sell the concept to the audience. The effectiveness of a security awareness program will be greatly enhanced if complimentary refresher-training initiatives and reinforcement techniques are used. This can be done using a variety of delivery methods, from an enterprise-wide poster campaign, to an intranet-based security awareness survey. As new security threats arise, such as social engineering or identity theft, it is also important to ensure that awareness training content is updated to reflect these issues – otherwise training will be ineffective in protecting against new and most likely virulent threats. To summarize: a short-term boost in awareness levels will only help protect your organization for a limited amount of time, whereas an ongoing approach will benefit your organization for the long term.

So – how does an organization go about developing and implementing an effective information security awareness and education program? And in a time of budget squeezes and tough competitive environments, what is the best way to get the security message to stick?
Eleven Key Principles for Making Information Security Awareness Training Truly Effective

Despite all these issues, many organizations have produced very effective and elegant solutions. The best examples have combined online and offline techniques, have been positioned and managed within an overall internal communication context and have been skillfully managed to handle the needs of different audiences, business lines and jurisdictions. Below we have also set out what we believe are the key principles for making information security awareness training truly effective:

1. **Clarity of ownership, executive buy-in.** Clear and visible executive buy-in lends credibility and avoids gaps between words and actions. Within the organization, there should be clear and unequivocal ownership of the project to ensure that it meets organizational objectives, but can accommodate the needs of different business lines.

2. **Avoid dealing with the problem in pieces.** Many programs are mostly subject driven (password management, social engineering, virus control, and so on) based on a perceived business risk. For employees, when subjects are dealt with case by case, this can create internal confusion with lack of clarity about relative priorities.

3. **Measurement of awareness and understanding is vital.** Even before embarking on the development of a training program, carrying out an awareness audit can provide important indicators on the knowledge gaps that exist. More importantly, it is crucial to test awareness and understanding, post-training, to ensure that knowledge gaps have been filled effectively.

Most online training solutions provide an audit/tracking system, or a Learning Management System (LMS) that will automatically track participation and understanding. These records can help to pin-point risk areas, and could also help mitigate any potential fines or penalties imposed if charges are fined against your organization for non-compliance with external regulations. A word of caution though – look beyond the glossy vendor brochures. Many Learning Management Systems fail the test of utility and have limited ability to manage different types of courseware.

4. **Integrated compliance.** Getting each department to create its own solution may be a way forward but for the most consistent, cost effective and comprehensive solution, an enterprise-wide approach generally yields the optimum outcome.

5. **It is about understanding, not information; less is always more.** We do not all have to be experts in information security. Information Security and Legal departments generate substantive policies and procedures, as they must, but for the majority of employees the issue is simple: they need the answer to three basic questions – what is it, why is it important and how does it apply to me? Sensible, relevant and clear information to deliver clarity of understanding is what is required. Reference material is fine – but keep it to be used only when needed. If any training is much more than an hour long, you should be asking some very hard questions about its effectiveness. Studies show user retention and commitment plummets after more than 60 minutes on screen.
6. **Value rather than cost.** A canned solution may be the answer; a swift PowerPoint may be cheaper, but bear in mind that costs relate to scale (generally the more users there are, the cheaper the cost per user) and that the real measure is the effectiveness of the outcome, not the initial recorded cost per head. The cost of security breaches are many, many times greater than the cost of effective training and awareness, to say nothing of the real cost of an impaired business reputation. There tends to be excessive focus on cost rather than benefit or applicability.

7. **The right combination of spirit and structure.** Don’t bore users into submission. Keep it light; a touch of humor will not go unnoticed. At the same time, reinforce personal responsibility and the corporate commitment to making this happen and getting it right.

8. **Relevant context setting.** Nothing turns employees off more quickly than irrelevant, inappropriate or unrealistic case studies and contexts. Actual examples from the archives or real situations are best. Training needs to be “sold” and delivered to employees, so they can understand where this fits into their daily routines.

9. **Consistency.** Make sure messages are consistent and that the way training and awareness is delivered runs with the grain of organizational culture and style.

10. **Technology should enable and no more.** Streaming video may be a great idea, but training should work within the context of what is possible, not what is desired. It is the content that makes the difference. IT needs to be involved but always consider the art of the possible. A good vendor will always have plenty of solutions and fixes for working around technology glitches.

11. **Project management, project management, project management.** Above all else the key ingredient and the real reason why most implementations fail. Ensure both you and your chosen partner have good project management capabilities, ensure all parties are on board and before starting anything that there is clear internal ownership and accountability. At a minimum, insist on a detailed training needs analysis, a comprehensive technical specification and allow a good deal of time for testing, feedback and fine-tuning.
SAI Global
SAI Global is one of the world’s leading business publishing, compliance, training and assurance organizations with operations in North America, Europe and Asia Pacific. The Compliance Division of SAI Global works with organizations worldwide helping to build a culture of compliance. Using our international experience, we deliver effective solutions to help manage risk, achieve compliance and promote ethical behaviour. We offer a flexible range of risk and compliance solutions and services, which engage staff at all levels of an organization.