9 Awareness raising

This chapter covers the various justifications for, and approaches to, improving awareness of information security, as well as mistakes to avoid. It forms part of Stage 2 – Planning, assessment and evaluation and Stage 3 – Implementation, support and operation in the Toolkit Route map.

Key topics

- **The different ways to target awareness communications to members of an organisation and to specific groups, as well as related challenges**
- **The qualities that awareness material should have in order to get attention and support individuals in developing the necessary security skills**
- **How to align awareness activities with the rest of the organisation, in terms of managing risk and measuring effectiveness**

9.1 Introduction

Information security is a collective responsibility for all members of an organisation. Members of the organisation must be appropriately aware of the risks to information within their role, and how they should use processes and technologies – as provided or sanctioned by the organisation – to manage those risks. Skills must be developed through engagement with individuals and teams working with information, coupled with delivery of targeted knowledge to those who can apply the expertise in practice. Evidence should be available to external parties to show due diligence in making staff aware of their responsibilities, for example after a data protection incident.

9.2 Awareness, education and training

Awareness activities help individuals in an organisation to recognise information security concerns that relate to their role, preparing them for education and training. Here we refer to security awareness, security education and security training, three distinct stages in changing a person's behaviour. The following is a user-focused view demonstrating where each may be applied:

Table 5 - Choosing awareness approaches

Reason for not doing the "right thing"	Targeted intervention
Don't know what it is Don't know how to do it	Training
Don't think it makes sense	Education
Never think of doing it	Awareness
Have no reason to do it	Motivation

For further information see Security Awareness, Education and Training in the reading list.

Security awareness encourages people to be interested in security, by attracting attention and conveying the effect security has within their roles.

With increased awareness, people respond better to security education – materials or courses that provide information about threats and vulnerabilities, and the actions individuals should take to protect themselves and the organisation. This can effect a change in perceptions and attitudes towards security.

Realising change in behaviour – the breaking of old habits and establishing of new habits – requires security training. Through a programme of training new behaviours are presented, but also tested and corrected to develop competencies and skills. Security training must be based in the work context and address specific security needs, and needs to be repeated enough to form the right habits. Monitoring capabilities and user feedback channels should be provided to determine the effectiveness of the programme. In the remainder of this chapter awareness, education, and training will be collectively referred to as awareness activities.

9.3 Triggers for awareness activities

There are various triggers for awareness, education and training activities within an organisation. Numerous external and internal factors can require awareness activities, beyond response to breach events and ongoing management of risks. These can include new laws or government initiatives which directly affect the organisation, updated or new technologies, or changes to organisation strategy or management. Trigger events, such as a revision to the Data Protection Act for example, should be identified and responses formulated at a strategic level through dialogue with decision-makers across the organisation (see Who does information security? within Chapter 8).

Communication channels should be maintained to support response to trigger events (rather than being developed in response to an event). A coordinated response also limits awareness content to that which is necessary for members of the organisation - this is important, as security is an enabling task supporting people in doing their job. Referring to the previous section, members may require awareness, education or training, depending on how the trigger event affects their work.

Members may also look to the organisation to provide guidance to address concerns or a desire to work more securely. Factors can include the vicarious experience of information security threats and visible enforcement of policies, but also social elements such as wishing to avoid embarrassment, demonstrating allegiance to the organisation and respect for others, and maintaining the reputation of the organisation. Factors should be identified through user engagement activities such as targeted surveys, regular involvement in team talks, or dedicated feedback channels within the organisation. (see Who does information security? within Chapter 8).

9.4 Foundations of an awareness programme

The training that individuals receive should align with the information risks that they need to manage as part of their role. The management of risks should then drive decisions within an awareness programme, including how to prioritise messaging to both address top risks for specific groups and limit the draw on members' attention.

Whilst general awareness raising is extremely important, the organisation should start with the clear message that compliance is required, both to encourage appropriate behaviour and to demonstrate to third parties, such as the ICO, that it takes information security seriously.

See Chapter 5, Risk assessment, for a discussion of risk management – a risk-driven awareness programme tempers the amount and relevance of training, through regular review of risks as the operating environment and threat landscape change. Messaging should also align with the values of the organisation, and the shared sense of professional responsibility for upholding those values.

An awareness programme cannot necessarily achieve its goals through fixed-period computer-based training alone; embedded training develops skills to address risks as they arise within the production task i.e. the person's job.

Good training requires appropriate resources and expertise. Trainers must be prepared to help individuals repeat awareness activities sufficiently often to form secure habits. Monitoring of the internalisation of awareness material, and the effects of awareness campaigns upon the operating environment, should be implemented, as well as a capacity for corrective feedback while skills are being developed (rather than as an isolated, static, one-off exercise). The organisation (specifically those managing the application of the awareness programme) should be prepared to dedicate extra resources to those who may fail to develop skills despite training and feedback – these individuals or groups may benefit from alternative solutions such as supporting processes or technologies rather than the application of more training.

9.5 Identifying channels for an awareness programme

There are many ways to communicate an information security message to target audiences. There is a right place for every format, with advantages and disadvantages to each approach. Approaches include:

- physical hand-outs such as leaflets, fact sheets, and comics
- on the job person-to-person guided work
- electronic communications (email, enewsletter)
- fixed-place messaging (posters and banners, fairs and seminars)
- persistent messaging such as screensavers
- videos/podcasts/webinars
- dedicated websites
- online intranet tools (wikis, forums, blogs) and training materials.

The US National Institute of Standards and Technology (see the NIST handbook in the reading list) separates activities by teaching method:

- media may act to improve recognition;
- practical instruction improves skills;
- theoretical instruction e.g. seminars improves understanding.

When designing awareness materials and approaches, the organisation should consider how long these will be valid for. For example, posters will "fade into the background" after a while, and people will forget what they learned in a course.

The ENISA publication The new users guide: how to raise information security awareness notes the advantages and disadvantages of various approaches. Note that there should be a recognition of general communications intended for all members of the organisation (supporting the values and intended image of the organisation); targeted communications for specific groups requiring particular competencies based on the risks they must manage (see Chapter 8, Roles and competencies), and targeted behaviour change activities that address specific scenarios (which especially can involve interactive or embedded training). Note that individuals learn mostly from doing, then less so from others around them, with formal training having the smallest impact.

The Raising user awareness of information security - Cardiff University case study demonstrates an awareness programme which uses a range of approaches together - doing so can serve to reach a wider audience within the organisation.

9.6 Identifying content for an awareness activity

Organisations can target behaviour change further by developing content around key risks or assets (see Chapter 5, Risk assessment). Engagement with individuals and local decision-makers may take time and resources, but can identify how vulnerable assets factor in the working day – awareness activities must support individuals to manage risks themselves. Awareness activities must be targeted so as to identify the right content for the right task, for the right audience. This may not necessarily be targeted at a departmental level, but otherwise scoped by profession or role (see Chapter 8, Roles and competencies). Regulate the scalability of the awareness programme with the level of targeted training for specific groups, applying a best-effort approach. Ideally education materials will empower users, avoiding "don't" mandates wherever possible.

Carefully-designed survey exercises or user quizzes can identify the needs of technology users and those handling information. This includes capturing how groups use IT facilities and sensitive information. The ENISA publication The new users guide: how to raise information security awareness includes template user questionnaires. Surveys and questionnaires provide the user perspective, and engagement with decision-makers and implementers identifies the system-level and strategic measures for monitoring the effectiveness of awareness activities.

The organisation should also consider how messaging around security relates to promoted values. Content should be able to change the way people think about security and make it fun and interesting (through cartoons or games). Role models – ideally organisational leadership – must be seen to follow the rules. Training should then be supported with strategic buy-in and tailored to those with authority and influence. Materials should be of appropriate technical level, as technology-related information can fall on deaf ears. Certain buzz-phrases can also cause a negative reaction (e.g. "information security", ironically).

For the design of security messaging, the organisation should be realistic in the demands made on user time and attention. Some principles from advertising may be useful: try to make material informative, brief, visual, attractive, unexpected, or funny. The posters appended to Cardiff University's case study on raising user awareness of information security, in the resources section at the end of this document, demonstrate some of these qualities in practice.

9.7 Arguments for different audiences

Distinct roles within organisations should be considered when planning for effective awareness activities (see Chapter 8, Roles and competencies). Awareness activities are generally concerned with the enabling task of security that supports a person in their job. For different groups there will be different risks to manage, and in turn different situations where individuals need to make the right decisions or know who to contact (where the security outcome can depend on actions taken in the moment). There will also be routine tasks, and novel problems where existing skills must be adapted based on the individual's reasoning of the situation.

Every member of the organisation should have the skills to use the organisation's facilities securely in their role. In using basic organisation facilities such as provisioned email accounts, all members likely need some basic comprehension of the threats posed by phishing, spam, and social engineering. There is also a need to manage regular access to system accounts (through passwords or other authentication technologies), as well as the management of data according to the organisation's policy (see Chapter 7, Information management, for reasons why an information management scheme must be easily understood). Information security extends to all forms of information/records, not just electronic copies (for example exam scripts, paper-based records, etc.). Mobility activities may require instruction on how to work remotely, use teleconferencing facilities, and work at conferences/events in a secure manner (not just with technology, but also in respect to information that is shared during those activities).

Staff and management should appreciate the impact of their actions on organisational reputation, as should students (potentially including recent or not-so-recent alumni). For those involved in securing funding, professional reputation is important, and security events can impact upon this - they will want to know how to protect their standing in the community. Those involved in research must manage intellectual property (unpublished work, research data, sensitive data, personal data), and those managing sensitive data must have the skills to appropriately adhere to data protection regulations. Staff with administrative duties must, amongst other things, consider protection of student coursework records, management of staff payroll details, and on- and off-boarding of staff or students to managed systems. Temporary or irregular visitors and collaborators may need a highly-targeted crib sheet that outlines their responsibilities even when they may only be working with organisation representatives for a brief time in limited ways. Hosts must know where to find this information and where it fits in the on-boarding process (whether shared upon arrival or made available beforehand).

There may also be third parties such as cleaning staff and contractors to consider, as they will at the very least have physical access to campus facilities – departmental representatives may have to understand procedure for overseeing access, and the third parties themselves should be aware of practices that relate to their activities on-campus.

Internet2 describes further considerations for various user groups in their Information Security Guide (see the reading list for this chapter).

9.8 Challenges

An individual's perception of security may make changing habits difficult. This may be seen as a failure to appreciate or understand threats – "I know how to do my job", "Nobody would target me"); frequently-made excuses (such as futility in the face of a determined attacker); or that security-conscious behaviour is not seen as an attractive or socially-accepted trait (e.g. challenging people when they try to follow an employee through a secure door without authenticating). Issues such as these should be identified in user engagement activities, such as surveys and team talks, and may require dedicated effort to change, or alternative solutions to manage related risks. Different cultures may have very different attitudes to acceptable behaviour, and this should be taken into account when designing awareness materials.

Individual capacity to engage with awareness material is limited, and competition for user attention is fierce. Individuals grow used to messaging that is targeted at them – even the most well-designed security posters can blend into the environment. Awareness techniques should then be creative and frequently changed. Care should also be taken not to overburden individuals with unneeded details, especially as they will be the target of multiple (other) training programmes within the organisation.

Pitching material can be difficult. Awareness activities should act to improve basic security practices, not to make individuals security experts in their own right – security-specific terminology may further confuse non-experts in security. At the other end of the scale, awareness activities can fail if they provide no explanation as to why a behaviour should be adopted. User engagement activities can help to find a balance.

9.9 Evaluating the response

Monitoring capabilities and user feedback channels should be provided to determine the effectiveness of the programme, particularly to identify any individuals who are not responding to training and may require dedicated attention. There may be persistent behaviours which cannot be changed, and these may not necessarily indicate a negative result but nonetheless inform awareness of security behaviours within the organisation.

In addition, records should be kept to verify that training is actually taking place as planned, and to record employees' performance in training courses, if relevant.

Referring to Chapter 11, When things go wrong: nonconformities and incidents, it may be that policies are not being followed, or that training to support policies is not effective. If training is not effective - and not relevant to the role - by drawing time away from the productive task it can also frustrate individuals. Feedback on the quality of training then contributes to the management of risks.

Embedded exercises such as self-phishing (as in Raising user awareness of information security - Cardiff University, case study) can serve as a leading indicator that something is happening or likely to happen, where incidents (see Chapter 11, When things go wrong: nonconformities and incidents) are a lagging indicator that something has happened. In line with organisation values and the management of risks, be careful in considering ways to reward good behaviour and punish bad behaviour beyond the awareness campaign.

The organisation should be in a position to identify security champions – there may be individuals who represent good security habits and are able to discuss security well with others in their team or the larger organisation. These role models should be supported in being seen in the organisation, and ideally would include top executives in their number.

9.10 Evaluating the awareness programme

The quality of the awareness programme should itself be monitored. Obstacles to an effective awareness programme can include lack of resources, the adaptive nature of social engineering attacks, and cost considerations – these include preparation and refreshing of materials (including the time of the preparer), the costs of providing instruction, and the employee time dedicated to attending courses and watching videos. Oversight is necessary when obtaining support for adjustments or additions to training material.

When deciding which training is mandatory, the suggestion of punishment for not following instructions should not be promoted if it is known that the instructions will be disobeyed ("we tell them not to, but we know they do it anyway") – this would impact the visibility of policy enforcement. It should be determined upfront whether there are the monitoring capabilities to detect an infringement, and the resources and buy-in to take action.

On a related note, training records are a valuable source of evidence that people have at least undergone training. This is helpful when attempting to demonstrate that due diligence has been followed, especially when working with an external body (such as the ICO) to determine the cause(s) of an incident, and possibly assign liability. Records should include the names of people trained, dates, and any scores or training measurements (see Chapter 10, Measurement).

If technologies or processes are consistently not working or being ignored, no amount of training may persuade users to use them; consider alternative solutions beyond awareness.

There are a number of indirect indicators that training is not working or will not work: security education is static, one-way and saturates attention (such as one-way "briefings", lectures, and posters); efforts are fragmented; the programme is the same for everyone regardless of responsibilities or where the message is best targeted; and education activities remain the same across consecutive years (regardless of any new technologies or feedback gathered in that time). These points should be addressed in the dialogue with decision-makers (see Who does information security? within Chapter 8, Roles and competencies). It is necessary to set a realistic timeline for achieving change in security habits.

Summary

- For greatest impact, target content to match identified risks and roles within the organisation, in response to changes in the organisation environment and threat landscape
- Target learning through media, practical instruction, or theoretical instruction, using physical handouts such as flyers, electronic communications, fixed-place messaging like posters, and persistent messaging (such as screensavers and online training)
- Consider that security is supporting the individual to do their job well, and that there is competition for their attention – security needs to be there to help develop skills that will be applied in targeted roles

Resources

Raising user awareness of information security - Cardiff University, case study

Development and use of a phishing exercise to raise awareness of phishing as an issue - Cardiff University, case study

Reading list

ENISA, The new user's guide: how to raise information security awareness, 2010
www.ucisa.ac.uk/ismt34
www.enisa.europa.eu/publications/archive/copy_of_new-users-guide/at_download/fullReport

C. Herley, More is not the Answer, Security and Privacy, Volume 12, Issue 1, Pg.14-19, IEEE, 2014
www.ucisa.ac.uk/ismt35
http://ieeexplore.ieee.org/xpl/tocresult.jsp?isnumber=6756734

Information Security Guide: Effective Practices and Solutions for Higher Education, Internet2,
www.ucisa.ac.uk/ismt36
https://spaces.internet2.edu/display/2014infosecurityguide/Home

Special Publication 800-12: An Introduction to Computer Security - The NIST Handbook: Chapter 13 - Awareness, Training, and Education
www.ucisa.ac.uk/ismt37
http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

Training materials from the Information Commissioner's Office:
www.ucisa.ac.uk/ismt38
https://ico.org.uk/for-organisations/training-materials/

Roper, Grau and Fischer, Security Awareness, Education and Training, 2006

Sasse et al, Human Factors Working Group White Paper: Human Vulnerabilities in Security Systems, Cyber Security KTN, 2007

Information Security Forum, From Promoting Awareness to Embedding Behaviours, Version 2, 2014