

Advanced security methodologies - Awareness raising

Pascal Steichen - M2SSIC-Metz

27/02/2007

Contents

1	Awareness	3
1.1	Why is awareness (raising) important?	3
2	Targets	4
3	How to raise awareness	7
3.1	Plan & Assess	7
3.2	Execute & Manage	13
3.3	Evaluate & Adjust	14
3.4	Obstacles to success	14
4	Beyond awareness raising	17
4.1	If Kuebler-Ross would do security	17
5	Bibliographic references	18

1 Awareness

The OCDE principles for creating a "culture of security" include **awareness** as first point, the second principle (**responsibility**) is however at least as important:

Awareness Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.

Awareness of the risks and available safeguards is the first line of defence for the security of information systems and networks. Information systems and networks can be affected by both internal and external risks. Participants should understand that security failures may significantly harm systems and networks under their control. They should also be aware of the potential harm to others arising from interconnectivity and interdependency. Participants should be aware of the configuration of, and available updates for, their system, its place within networks, good practices that they can implement to enhance security, and the needs of other participants.

Responsibility All participants are responsible for the security of information systems and networks.

Participants depend upon interconnected local and global information systems and networks and should understand their responsibility for the security of those information systems and networks. They should be accountable in a manner appropriate to their individual roles. Participants should review their own policies, practices, measures, and procedures regularly and assess whether these are appropriate to their environment. Those who develop, design and supply products and services should address system and network security and distribute appropriate information including updates in a timely manner so that users are better able to understand the security functionality of products and services and their responsibilities related to security.

1.1 Why is awareness (raising) important?

In the digital age where we now are living and working, individual citizens and businesses alike have found the use of information and communication

technologies (ICT's) to be invaluable in day-to-day tasks.

However, with vulnerabilities in these new environments as well as with the convergence of these technologies, the growing use of "always on" connections and the continuous and exponential number of users, more and more citizens and businesses are at risk of information security breaches. These security breaches may be IT related, for example through the execution of computer viruses, or may be socially motivated, e.g. through physical theft of equipment. At a time ever more reliant on digital information, there are an increasing number of dangers, with a considerable number of citizens still being unaware of the exposure to the risks to their security.

Companies or any other organization cannot protect the *confidentiality*, *integrity*, and *availability* of information in today's highly networked systems environment without ensuring that all people involved in using and managing IT:

- Understand their roles and responsibilities related to the organizational mission;
- Understand the organization's IT security policy, procedures, and practices; and
- Have at least adequate knowledge of the various management, operational, and technical controls required and available to protect the IT resources for which they are responsible.

2 Targets

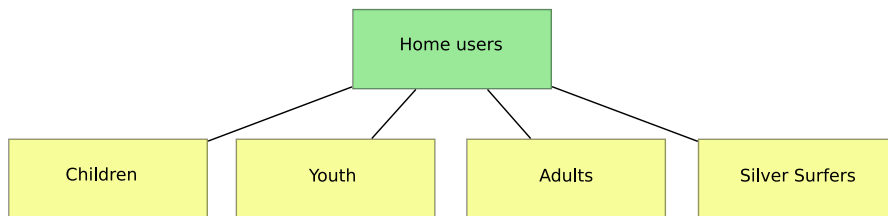
The way awareness initiatives are realised and the content of the communicated information is heavily dependent on the audience. Similar to commercial products or services, security awareness campaigns have to adapt to the specific target groups, to be effective.

Who are the targets ?

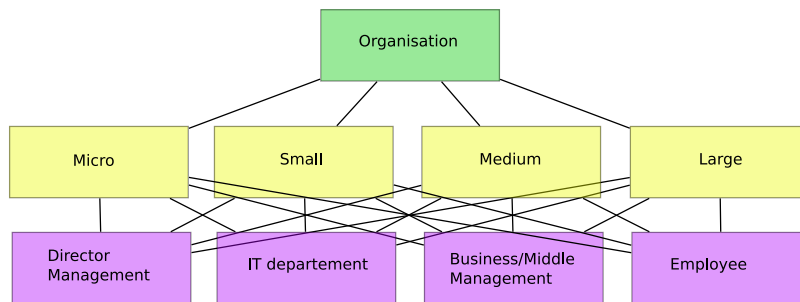
- Citizens / home users / employees
- Managers / directors / decision takers
- IT people / IT market
- Regulators / Legislators / Government
- *Media*

- (Information security sector)

Home users



SMEs



(Local) government

(Local) government is worthy of special attention, it needs to strengthen its own awareness first, then transfer relevant knowledge to their citizens.

- Local government bodies are critical infrastructures
- They manage critical infrastructures that depend on information systems (transportation, water supply, local tax etc.)
- They constitute a front line to citizens
- They must guarantee transparency and accountability
- They don't usually have the skills required to manage information security
- They can act as awareness agents for citizens and schools

(Local) government needs an extra high level of security awareness.

National governments have to customise the security strategies they implement/recommend at the local government level, in particular due to the large difference that exists in degrees of autonomy.

In particular they should:

- define and implement an ICT security concept adapted to their organizational needs
- implement ICT baseline protection (BSI-Standard 100-1, BS7799, ISO27001, EBIOS(FEROCE))
- protect critical infrastructures that play an important role in citizens' lives
- sensitize employees in order to foster an "information-security culture"

Media

Media requires special attention in security awareness because until now ICT-security has been a neglected topic in mass media (exception: extreme virus attacks):

- journalists have to be persuaded that ICT-security is a useful and important issue in our information society and that their task is to report about this important issue
- media plays an important role in awareness raising and in educating the broader public
- journalists need support and incentive to report much more about ICT Security, so that the broad public can be more easily reached
- media lobbies on public issues and legislation

Objectives:

- Educate media on ICT-security
- Make media aware of the need for ICT-security due to society's increasing dependency on ICT
- Ensure that media assumes social responsibility and enforces its "Public service" commitments as the "4th state power"

3 How to raise awareness

An awareness programme/campaign has to be seen as a long term investment in the culture of security, be it on a company, national or international level. To be effective it should have a life-cycle (design, develop, implement, evaluation) and be **specific**, **realistic** and **mesurable**.

It should, further, be considered a full project and as such the classical project management tools and practices, like setting the scope and objectifs, defining a budget, a planning and determining ressources, should be used. So the overall strategy could look as follows:

- Plan & Assess
- Execute & Manage
- Evaluate & Adjust

3.1 Plan & Assess

- Establish the context
 - National, organisation or unit level ?
 - Is it the first campaign ?
 - Obtain management support **and** funding
 - Establish a (motivated) team (centralised / distributed)
- Evaluate the needs
 - via interviews / questionnaires
 - based on prior experiences / metrics / results
 - risk analysis
 - audit reports
 - structural changes (organisation / infrastructure)
 - new technologies / threats (wireless, social engineering, ...)
- Define goals and objectives
 - run as cost benefit analysis
 - identify programme benefits

Target groups and message

- Establish Message for a Specific Target Group
 - Necessary to target a specific group that has similar interests and priorities as the public in general has diverse interests, expertise and experiences. Because different audiences place different emphasis on different risks (often stemming from personal experiences), message needs to be targeted to a specific group.
 - Ask questions such as what will they notice or grab their attention, why should they care (tailored to audience's needs and concerns) and what will they do.
- Detail Message
 - Need to understand the audience such as their level of awareness for the issue, their needs, and the issues they are concerned about, where they get the information and what information they like to receive.
 - Actual message content needs to do three things: catch audience's attention, alert them to risk and provide them with information or a reference from where to get it.
 - Need to make sure the message is as inclusive as possible, for example, it should not discriminate against minorities.
- Test Message
 - Launch the campaign and evaluate results or responses. Evaluation (quantitative and qualitative) can be done through methods such as focus groups, Interviews, questionnaires or omnibus surveys.

Communication strategy

1. Define communication objectives
2. Perform target group analysis & identify suitable media
3. Identify key communication messages
4. Assign roles and responsibilities
5. Develop detailed communication plan

Channels of Communication

- Brochure or Magazine

- Advantages:**
- Easier to define message content and format.
 - Allows for careful study of content by Target Group.
 - Established audiences can be reached.

- Disadvantages:**
- Not a static source of information as material could be lost.
 - May only appeal to a select Target Group.

- Comic

- Advantages:**
- Instant appeal to certain Target Groups like the young
 - Message content can be more abstract in nature.

- Disadvantages:**
- Difficult to incorporate messages with more detail.
 - May only appeal to a select Target Group.

- Distant learning (Computer Based Training (CBT), online training)

- Advantages:**
- Enables training over geographically dispersed areas.
 - Message content can be more detailed.

- Disadvantages:**
- Can be expensive to create training programmes.
 - Implies trainee has some technical knowledge already.

- Education

- Advantages:**
- Good way to reach large numbers of children.
 - Often established channels exist to distribute materials.

- Disadvantages:**
- Time in school is already at a premium and curricula are often crowded.
 - Teachers may not have expertise to deliver message.
 - Computing facilities may not allow some activities e.g. practice in installing antivirus software.

- Email

- Advantages:**
- Relatively cheap channel to target mass audience.
 - Allows Target Group to digest information in own time.

- Disadvantages:** – Message may be undermined due to volume of emails and spam.

 - Email addresses must be known.
- Event (fair, meeting, seminar, conference)
 - Advantages:** – Can reach a very wide range of audiences by careful selection of venues and topics.

 - Has more chance of interesting the audience due to the interactive element of the channel.
 - Disadvantages:** – Your intended audience may not attend.

 - Not a proactive channel with the Target Group expected to participate.
- Leaflet or fact sheet
 - Advantages:** – Can provide a lot of information.

 - Cost effective to produce.
 - Disadvantages:** – Need to organise distribution channels so your leaflets get the right audience.

 - Not a static source of information as material could be lost.
- eNewsletter
 - Advantages:** – Similar advantages as the email channel.
 - Disadvantages:** – Not a proactive channel as typically requires users to register.

 - Implies trainee has some technical knowledge already.
- Newspaper
 - Advantages:** – Mass circulation with deep market penetration. On a cost-per-thousand basis, newspapers are generally an inexpensive, cost-efficient means of delivering a message to a wide audience.

 - A newspaper ad can give as much detailed information as is needed and even display images or logos.
 - Disadvantages:** – The clutter factor. There is a lot of competition for the reader's attention in a newspaper. Newspapers are usually filled with many ads, in various sizes and styles, promoting many products and services.

 - If wishing to reach only a specific population segment may find that newspapers waste too much circulation.

- Newspapers have a short life. They are frequently read in a rush, with little opportunity for careful study.

- Phone

Advantages: – Allows direct Target Group contact.

- Has more chance of interesting the audience due to the interactive element of the channel.

Disadvantages: – Can be relatively expensive.

- Target Group contact details need to be available.

- Poster

Advantages: – Can be attention grabbing due to size and format.

- Information can be universally available when put up on walls.

Disadvantages: – With abundance of information material, message may be overlooked.

- Radio

Advantages: – Radio's biggest advantage is high frequency (reaching the same audience numerous times) at a reasonable cost.

- Station music formatting helps define interest groups and some demographic categories. So you can choose the specific type of audience you'd like to reach.

Disadvantages: – Radio has heavy commercialisation.

- You can't show your subject and cannot demonstrate it.
- A radio spot lacks the permanence of a printed message.
- Because of formatting and audience specialisation, a single station can seldom offer broad market reach.

- Screensavers

Advantages: – Places information on the computer so users are likely to see it.

Disadvantages: – Requires development.

- Inexperienced users may be unable to install it.
- Does not reach those without Computers.

- SMS

Advantages: – Message content can be delivered straight to the Target Group ensuring visibility.

Disadvantages: – Need to work with Telecoms provider.
– Effective channel to alert the Target Group of dangers but not raise awareness due to limited content.

- Training

Advantages: – Has more chance of interesting the audience due to the interactive element of the channel.

– Content of message can be more detailed and customised.

Disadvantages: – Not a proactive channel with the Target Group expected to participate.

– Can't really reach mass audience due to resources and logistics involved.

- TV

Advantages: – High impact, combining sight, sound and motion - can be attention-getting and memorable.

– TV comes as close as any medium can to face-to-face communication.

– The personal message delivered by an authority can be very convincing.

– You can demonstrate message.

– TV offers audience selectivity by programming. It offers scheduling flexibility in different programs and day parts, and the opportunity to stress reach or frequency.

Disadvantages: – Cost - Budget requirements are relatively high.

– Although you can pick your programmes, you run the risk of the most popular shows being sold out.

- Video

Advantages: – Allows for creative freedom with awareness message.

– Professionalism of channel if implemented correctly could help enforce message.

Disadvantages: – May not reach a technologically naive audience.

- Website

Advantages: – Can be updated to reflect changes.

- Can present content for multiple audiences.
- Can easily link to other information.

Disadvantages:

- May not reach a technologically naive audience.
- Implies trainee has some technical knowledge already.
- Not a proactive channel and with wealth of websites and information on the Internet available, message may get overlooked.

Plan & Assess (continued)

- Take a change management approach
 - Identify and involve key stakeholders in decision-making, planning, implementation and evaluation.
 - Establish a clear goal for the change endpoint, in consultation with key stakeholders.
 - Clearly define roles, responsibilities and accountabilities.
 - Link and integrate key elements of change.
 - Manage risks and address barriers to change.
 - Provide leadership at all levels for the change process.
 - Communicate in an open, honest, clear and timely manner.
 - Allow for flexibility in approaches to suit different stakeholder needs.
 - Resource, support and manage the change.
 - Support with training and development to ensure a change in behaviour and culture.
 - Learn from previous and ongoing experiences, build capability for change and celebrate achievements.
- Define indicators to measure the success of the programme
- Establish baseline for evaluation
- Document lessons learned

3.2 Execute & Manage

- Confirm programme/content
 - 3 concept approach : *risks, counter-measures, responsibilities*
- Launch and implement the programme
- Document lessons learned

3.3 Evaluate & Adjust

- Measure/evaluate the results
 - Conduct evaluations
 - Review programme objectives
- Update and improve the programme
- (Re-launch the programme)

3.4 Obstacles to success

1. Implementation of new technology

When new technology is implemented, it often requires a behaviour change or new level of user understanding. This alone is not an issue, however, sometimes technology moves faster than or independently from the awareness programme. It could happen that the awareness team is not up-to-date nor adequately informed of these types of educational opportunities until it is too late. This is why it is important for a security awareness programme to emphasise internal communications, as well as ensure that an emergency or crisis communication strategy is in place.

2. One-size-fits-all

Some security awareness programmes fail to segment their audience adequately and appropriate messages are not delivered. This results in messages being ignored. Information technology users receive hundreds of messages every day from a multitude of sources. It is critical to segment audiences and ensure that people only receive the messages they need. A one-size-fits-all strategy might be easier to develop and implement, but it will not be effective.

3. Too much information

Over-education is quite a common mistake. The public tends to have a threshold of how much information they are willing to accept from any one source. If individuals are inundated with a constant barrage of messages, it is likely to turn their attention away. Even after having taken the necessary steps to segment the audiences and only sending appropriate messages, too much information is simply too much. An awareness programme does not have to be built over a very short period of time. Take the time to be open to the audiences' needs and find the right balance.

4. Lack of organisation

Many awareness programmes fail to develop consistent processes and strategies for delivering messages to users. Without a consistent style, theme and delivery, it is difficult for the user to engage in the programme or even know what to expect. It is key to develop consistency in communications. This will also help establish an identity for the programme and build a relationship with the audiences.

5. Failure to follow-up

It is quite common for security awareness programmes to be launched with great enthusiasm only to fizzle out with little success. Many programmes fail to establish and maintain a regular cycle of communications. It is important to establish regular communications so that users receive regular reminders of the key messages. In addition, many programmes fail to follow-up with their audiences and solicit feedback. It is critical to listen to the audiences and adjust the programme based on their needs.

6. Getting the message where it will have an effect

Often it is a real challenge to deliver the right message to the right audience. This is especially true in large communities. For example, even if a local council has already developed a thorough communication strategy with a well-maintained process for targeted communications, delivering the right messages to right audience can still be very difficult. Email groups based on individual criteria can be helpful, but do not fully solve the problem. In some cases, although a particular audience has been identified, it might be a challenge to figure out specifically who belongs in the audience. For example, there may be a message that needs to be delivered to one particular segment. For example, parents may have been identified based on school registration, but it is likely that the list is not complete due to reasons such as children living full-time with another parent. The challenge is how best to identify and maintain a list that ensures all pertinent messages get to all of the parents every time. This is a difficult task.

7. Lack of resources

This usually stems from the lack of management support. Without management support, it is difficult to secure adequate resources; without adequate resources, a security awareness programme is limited in what it is able to achieve.

8. No explanation of why

Many security awareness programmes fail to educate users on why security is important. All other aspects are covered, but unfortunately

the information that is most likely to motivate users to change behaviour is omitted. Users who understand why certain behaviours are risky are most likely to take ownership of the issue and change their behaviour. For example, if guidelines on a new password process with more stringent complexity rules are communicated, users will most likely view the new process as nothing more than an inconvenience. However, if it is also communicated how passwords are cracked and misused and the potential impact this could have, and then users are much more likely to take ownership and follow the new guidelines.

9. Changing long-established behaviours

In many organisations, security is often implemented as an afterthought. Because security is not always integrated from the very beginning, users have months, weeks and even years to develop bad habits. This makes the challenge of implementing a security awareness programme even more difficult. Not only is there a need to educate users on security, but also users need help to "unlearn" any bad habits that they may have acquired. In addition, such users tend to have more difficulty buying into the value of security. As far as they are concerned, the organisation has operated just fine for many years without security. New security requirements are viewed as unnecessary changes that make their lives more difficult.

10. "Security is an information technology department problem, not mine..."

Many users share the perception that security is the sole responsibility of the IT department. They tend to limit their role to the bare minimum of compliance to maintain their jobs rather than the big picture of how to be a part of the solution. While adhering to policy is a good start, there is much more that can be done. It is important that users understand that IT staff cannot tackle information security alone.

11. Lack of management support

Obtaining management support is one of the most essential aspects of a security awareness programme. It is also one of the most challenging. For security messages to be effective, they must be supported from the top down. Even though many managers express their desire to support security initiatives, putting it into action is another story. This is because managers have their own roles and responsibilities. Their primary goal is to meet their business objectives and it is often difficult to find room for security issues, no matter how much they believe security is important.

4 Beyond awareness raising

The learning continuum:

1. Awareness (*I know it exists*)
2. Understanding (*I know what it is*)
3. Value (*I know why it's important*)
4. Ownership (*I like it*)
5. Commitment (*I'll do it*)
6. Communication (*I'll tell others*)
7. Development (*I'll help enhance it*)

4.1 If Kuebler-Ross would do security

1. Denial
 - *"I didn't open that e-mail (containing a virus)!"*
 - *"I never surf on such sites!"*
2. Anger
 - *"Why do you block 'skype'!"*
 - *"I can't work this way!"*
3. Bargaining
 - *"I'll follow all the procedures, if you just let me use 'MSN'!"*
4. Depression
 - *"My email is totally useless with all this SPAM!"*
 - *"I won't never use the Internet again!"*
5. Acceptance
 - *"You're right this security policy is indeed useful!"*

5 Bibliographic references

- ENISA ENISA - A Users' Guide: How to Raise Information Security Awareness
- ENISA awareness raising working group
- NIST 800-50 Building an Information Technology Security Awareness and Training Program
- Kuebler-Ross model
- www.protegetonordi.com
- klicksafe.de
- www.passe-ton-permis-web.com
- CASES Luxembourg
 - Permis Web - Webschein
 - eLearning
- mySecureIT
- LuSI (Luxembourg SaferInternet)
- GOVCERT.NL - waarschuwingdienst
 - BotnetFilm (en,mpg)
 - HackDemo (en,mov)
- Computer Security Awareness Video Contest 2006
 - Bob you've been phished
- pecephobie (Ginette)