Information security awareness initiatives:

Current practice and the measurement of success

July 2007

enisa
European Network and Information Security Agency

Preface

The European Network and Information Security Agency (ENISA) is a European Union Agency created to advance the functioning of the Internal Market. The Agency's mission is to achieve a high and effective level of network and information security within the European Union.

ENISA commissioned PricewaterhouseCoopers LLP (PwC) to develop this report to offer a perspective on what governments and private companies are currently doing for assessing the impact and success of awareness raising activities.

This study is intended to be used by professionals within organisations and public bodies that are tasked with planning, organising, and delivering information security awareness initiatives.

The study has focused on cultural change, the ways in which sets of metrics and key performance indicators (KPIs) can pay off, and how assessing methods (qualitative and quantitative) can contribute to the development of a wider culture of security.

This involved gathering information on the current practices of a number of European government departments and companies, to:

- Provide an outline analysis of recommended security awareness practice and metrics to measure awareness;
- Provide an outline of key metrics that can be used to effectively assess awareness, as well as some high level;
- Convey the results of the survey to assess what entities are doing with regards information security awareness;
- Provide case studies of good practice for awareness and measurement of effectiveness or to highlight information of benefit; and
- Contribute to the development of an information security culture in Member States by encouraging organisations to act responsibly and thus operate more securely.

The research was carried out during May to July 2007 using a structured questionnaire. This was made available on a self-select basis to people responsible for information security in European government departments and companies. In total, 67 organisations headquartered in nine different European countries responded. Many of these had operations in several European countries. The size of the organisations varied from less than 50 staff to more than 10,000 staff. There was a spread of responses across all industry sectors. PwC then interviewed 12 of the 67 respondents in depth and wrote these interviews up as case studies.

This report, therefore, gives an indication of what European organisations are currently doing to measure and improve information security awareness. Because of the self-select nature of this study and limited sample size, the results should not be interpreted as statistically representative of European businesses and government departments as a whole.

About ENISA

ENISA is a European Union Agency created to advance the functioning of the Internal Market by advising and assisting Member States, EU bodies and the business community on how to ensure a high and effective level of network and information security. ENISA also serves as a centre of expertise for Member States and EU institutions that facilitates information exchange and cooperation.

Contact details

Isabella Santa
e-mail: awareness@enisa.europa.eu
Internet http://www.enisa.europa.eu

Research carried out for ENISA by:

PRICEWATERHOUSECOOPERS

The member firms of the PricewaterhouseCoopers network (www.pwc.com/uk) provide industry-focused assurance, tax and advisory services to build public trust and enhance value for its clients and their stakeholders. More than 140,000 people in 149 countries share their thinking, experience and solutions to develop fresh perspectives and practical advice. Unless otherwise indicated, 'PricewaterhouseCoopers' refers to PricewaterhouseCoopers LLP a limited liability partnership incorporated in England. PricewaterhouseCoopers LLP is a member firm of PricewaterhouseCoopers International Limited.

Executive summary

This report analyses how organisations and governments within the European Union (EU) are approaching information security awareness and the measurement of effectiveness. The report covers three main areas.

The first part of the study looks at the importance of information security awareness and specific topics to respondents (see pages 3 to 7). The main findings are:

- Information security is seen as a high or very high priority in four fifths of respondents;
- Much of this is driven by a need to provide assurance to customers that their sensitive data is protected. Identity theft is a significant concern;
- There is also widespread recognition that respondents are now heavily dependent on technology, and the Internet in particular. This leaves companies more exposed to information security threats than ever;
- In addition, there is increased regulatory focus on this area, both inside the EU and beyond;
- The consensus is that the most important topics for staff awareness are email, physical access, passwords and the Internet; and
- Instant messaging and clear desk policies are the least favoured topics.

The second part considers techniques to raise information security awareness (see pages 8 to 13). The main findings are:

- Almost every respondent has defined their security policies, either in their staff handbook or a separate security policy. 85% of respondents have set up an intranet site that provides guidance to staff on information security matters. These techniques are seen as low cost basic disciplines. However, alone they are not effective ways to change staff behaviour;
- Respondents find training to be the most effective technique. 72% include security messages in induction training for new staff. Ongoing training for existing staff is much more patchy; the cost makes many respondents reluctant;
- Half of respondents are using computer-based training (CBT), and two thirds of these have mandated it; benefits cited are cost-effectiveness, consistency of delivery and ability to measure results;
- Despite the high priority given to security, many respondents find it difficult to justify significant spend on awareness programmes. Only a third of respondents build a formal business case to justify this expenditure; of these, only half attempt to quantify the benefits that their awareness programmes will achieve, and very few evaluate return on investment (ROI); and
- Most respondents instead think of security awareness training as something they just have to do, i.e. a compliance requirement. As such, their budget is treated as an overhead rather than an investment.

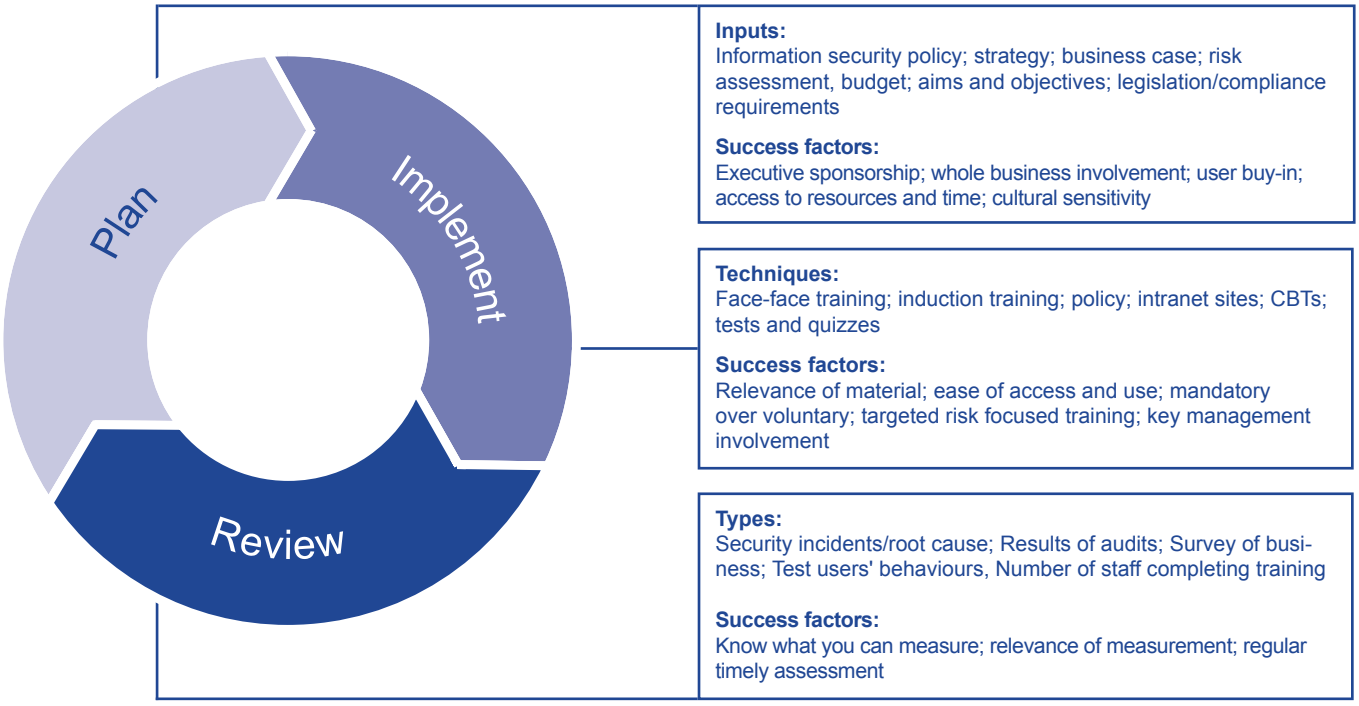
Executive summary

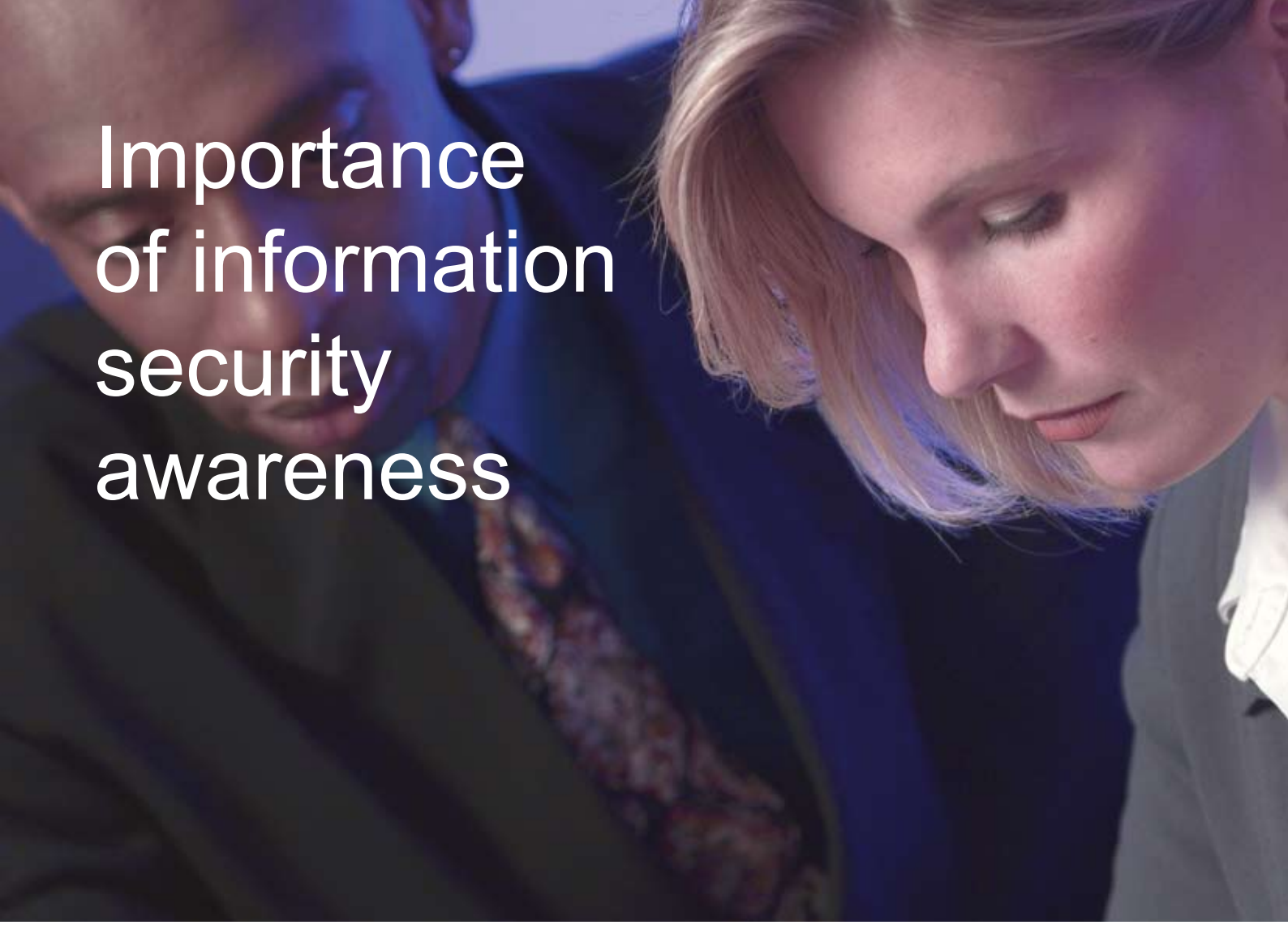
The final part reviews the mechanisms and techniques that are used to measure information security awareness initiatives (see pages 14 to 20). The main findings are:

- A wide variety of different methods are used to measure the effectiveness of information security awareness initiatives. Organisations appear to find it very difficult to put effective quantitative metrics in place;
- There is little consensus on the most effective measures. This is clearly an area where good practice is evolving;
- Ideally, respondents would like to be able to measure actual changes in staff behaviours resulting from the awareness activities. As a consequence, relatively few respondents find input metrics (e.g. number of visitors to intranet site, number of leaflets distributed) helpful;
- The most popular source of information on actual behaviours is audit (internal or external); two thirds of respondents use policy breaches highlighted in audit reports as a measure. The auditors' objective and systematic approach was felt to make these reports reliable sources of information;
- Many respondents use their experience of security incidents as a metric. The most common metrics are the number of incidents caused by human behaviour and root cause analysis of the most serious incidents; more than half of respondents use each of these. Many other respondents, however, have abandoned security incident statistics as a measure of security awareness, since there are many other factors involved;
- A third of respondents include questions on security awareness in staff surveys. They then measure awareness levels before and after initiatives take place. However, some respondents highlight issues with the complexity of collecting and processing this data; and
- Some metrics are used because they provide insight into actual behaviours (e.g. scans or tests). Others are adopted because they resonate with the senior management that sponsor awareness programmes (e.g. cost of incidents).

Each organisation needs to find the right balance for them; there is no "one size fits all" solution. Keeping the approach simple tends to keep it cost-effective. Many currently struggle with quantifying security awareness; however, provided simple mistakes are avoided, a balanced set of key performance indicators (KPIs) and metrics can provide real insight into the effectiveness of awareness programmes. Only with this insight are organisations able to change their programmes from a compliance activity to one that really benefits their operations.

Overall, an iterative approach to security awareness programmes appears most effective, as illustrated below:





Importance of information security awareness

Organisations, whether private or public, are increasingly storing and making more information available electronically. There is a broad increase in reliance on IT systems.

This is coupled with an extraordinary increase in the use of Internet services. This is becoming an increasingly important part of doing business. Lack of an Internet presence can be detrimental to organisations' business objectives.

The increasing use of IT systems to store and process information makes keeping this information secure more important. One of the key undertakings an organisation has is to ensure that staff act in an appropriate manner. This includes staff acting to keep sensitive information secure.

The Information Security Forum (ISF) is one of the world's leading independent authorities on information security. Through surveys and research, the ISF have defined information security awareness as:

> **'an ongoing process of learning that is meaningful to recipients, and delivers measurable benefits to the organisation from lasting behavioural change.'**

This information security awareness is a major component within industry good practice for security. Several international standards refer to this as a prerequisite:

- ISO 27001;
- COBIT;
- Payment Card Industries – Data Security Standard; and
- ISO 9001:2000.

Some of the key drivers increasing the emphasis on information security awareness are:

- Business requirements are changing, as use of technology (such as podcasts) evolves;
- Foreign regulators (e.g. the US and Singapore) are expecting staff to receive awareness training;
- The focus on security from regulatory bodies within EU Member States is increasing. A recent example is the UK information commissioner's comments to UK Chief Executive Officers on "unacceptable privacy breaches";
- The threat from organised crime is on the rise. A recent report on Internet security highlighted high levels of malicious activity across the Internet, with increases in phishing, spam, 'bot' networks, Trojans, and zero-day threats. In the past, these threats were usually distinct and could be addressed separately. Attackers are now refining their methods, so attacks tend to involve multiple attack vectors. They are also consolidating

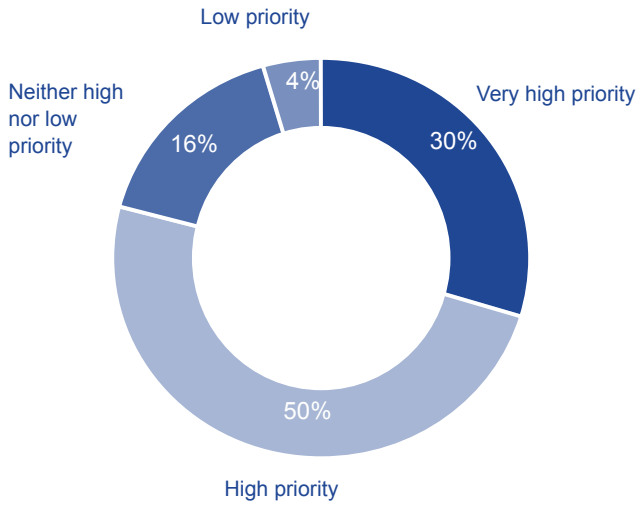
Importance of information security awareness

their assets to create global networks that support co-ordinated criminal activity;

- Customers are more sensitive to security issues than in the past. Adverse press coverage can cause major impact to an organisation's reputation; and
- Identity theft is an increasingly prevalent security issue. Organisations that store and manage personal identification information must take care to ensure the confidentiality and integrity of such data. Any compromise that results in the leakage of personal identity data could cause loss of public confidence, legal liability, and/or costly litigation.

Given these drivers, it is not a surprise that four fifths of respondents rate information security as a high or very high priority to their senior management. This is similar to the proportion noted in other recent security surveys.

Importance of information security



Information security is wide ranging and has many varied topics. Their importance to different organisations depends on the nature of the risks they face. For example, financial services and technology respondents share concerns over passwords; however, phishing is more of a concern in financial services and patching more important to technology companies.

The priority given to information security appears to relate more to the attitude of senior management than the sector in which the organisation operates (hence the risks to which it is exposed). For example, most government departments responding say security is a very high priority to their senior management; one, however, rated it as a low priority and seems to be carrying out the bare minimum necessary to comply with mandatory guidance.

Investment bank – to change behaviours, training needs to be interactive

An investment bank explained that its primary objective is to achieve regulatory compliance in a cost-effective way.

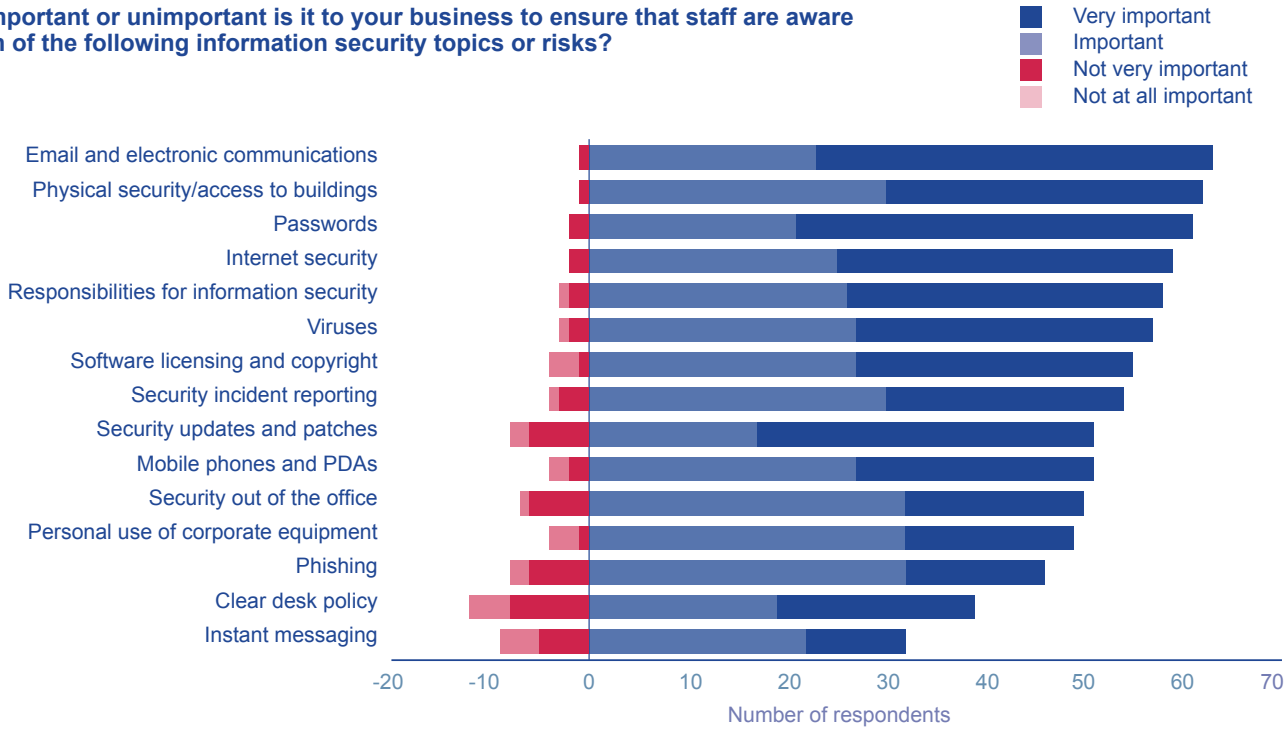
This is not possible without the creation of clear policies that set out what individuals should and should not do. Without this foundation, enforcement and discipline become hard if things break down. The bank has, as far as possible, included information security points in existing policies and training, rather than creating new ones.

Policies themselves are not effective unless staff understand them. The bank's security team gives induction presentations to all new joiners that explain the bank's security policies. This face-to-face contact gives staff an opportunity to discuss possible issues with the security team. Feedback from the training shows that interaction is critical to challenging people's attitudes and helping them learn. If people are asking questions, they are thinking and considering the information. A room full of silent people is unlikely to be learning much. Sharing war stories and relevant experiences helps staff see how security threats might affect them.

The bank has found that induction training alone is not enough. It is important that staff receive frequent reminders that reinforce key messages in a coherent way. Critical to this reinforcement has been getting senior management to lead by example; they, rather than the security team, are the best people to promote the importance of the messages.

The security team uses a variety of techniques to reinforce awareness messages on an ongoing basis. Quizzes and prizes get a good response level from staff; they get people thinking, and are well received within the business. Again, interaction with staff is vital. For example, posters that are passive reminders and ultimately require no individual action are often ignored in practice. Intranet articles and sites are good ways to promote messages to those that already actively use them. However, for people who do not visit them (the majority of staff), they are not an effective mechanism.

How important or unimportant is it to your business to ensure that staff are aware of each of the following information security topics or risks?



Traditionally, financial services companies have been leaders in security practice. Our respondents confirm that security remains a high priority to most financial services boards; however, in some security still seems to be driven bottom-up rather than top-down.

One company rating security as a low priority sums up the attitude of their senior management as taking the view that nothing bad has happened yet and so why spend money.

In contrast, those at the other end of the spectrum are principally motivated by customer perception and the damage to their reputation that a breach might cause.

Overall, most respondents agree that four topics are very important for staff to understand:

- Email and electronic communications;
- Physical security/access to buildings;
- Passwords; and
- Internet security.

For each of these, more than half of respondents rate them as very important; roughly nine tenths rate them as very important or important.

Passwords remain the primary authentication method to IT systems. Given concerns about potential privacy breaches, the need for staff to adopt good password disciplines is high. There have been many recent press stories involving inappropriate emails or Internet usage. The reputations of many companies and government departments have suffered as a result. Making sure that staff are aware of what the organisation considers to be acceptable usage is critical here.

Avoiding easily guessable passwords, keeping passwords secure and not sharing them are all important elements of awareness training.

In the light of the rise in terrorist activity over the last decade, it is perhaps unsurprising that physical security is so high up the list. Particular issues here include tail-gating, escorting visitors and granting/rescinding access to temporary staff.

Interestingly, the respondents that rate email and physical security as not very important are from the public sector. Attitudes to these specific areas may be more relaxed here.

For most of the other topics, roughly four fifths of respondents rate them as either very important or important.

Some of these topics (responsibilities for information security within the organisation and security incident reporting) are seen as basic information that staff needed to know.

Viruses and patching are a particular concern in the technology sector. The days of indiscriminate Internet worms are past. Businesses today are subject to sophisticated targeted attacks by programs that hide from detection and gather confidential information. Staff need to be aware of the changing nature of this threat.

Importance of information security awareness

Mobile Phones and PDAs (Personal Digital Assistants e.g. Blackberries) are a particular issue for financial services respondents. Organisations in this sector can make and lose money in short timeframes. Information tends to be more time critical to them and their staff. They, therefore, tend to be leaders in adopting technologies that provide information to staff right now.

There are two clear topics that are of perceived least importance to organisations. These are promotion of a clear desk policy and instant messaging.

The low priority given to awareness of clear desk policies is, perhaps, understandable. Many companies simply do not adopt or enforce such policies. They feel their physical access controls mitigate the risks sufficiently.

The low priority given to the use of instant messaging is more of a paradox given the high importance attributed to email. Both provide a mechanism for people to connect directly with external parties and to transfer information to them. They would appear to be very similar in nature and risk.

There is a clear risk of uncontrolled distribution of confidential information through both media. Indeed, it could be argued that instant messaging poses a higher risk than the use of email, since email filters are often more sophisticated. It may simply be that some respondents have blocked instant messaging technology from working in their organisation, so do not feel they have to make staff aware of the risks.

International insurer – senior management commitment makes a big difference

An insurance company explained why information security is important to their business. They collect, store, and process significant amounts of financial, medical, and personal information. This information is their number one asset; confidentiality breaches could put their reputation at risk, as well as exposing them to harmful litigation. Unfortunately, the threats (such as identity theft and scams) are rising; this makes staff awareness vital.

The main challenge has been to develop an approach that is suitable for over 10,000 employees speaking many different languages. To counteract this, the company engaged an external provider to help them build suitable training plans and materials. To create the greatest impact with staff, training materials were translated into the local mother tongues of the countries concerned.

There is a continual programme to adjust and promote the key messages. The objectives of this are to try to change people's behaviour and perception of risk. Numerous techniques are used to reach the audience, since different people learn by different mechanisms.

The most effective technique has been face-to-face time with staff through workshops and training sessions. Being able to put a face to a name or function is more personable and people are more receptive to messages being face-to-face. The training is mandatory. Senior management actively support the awareness schemes, making sure training events are at convenient times for the business and promoting them to staff. There is good attendance at sessions since missing the events results in escalation to the employee's manager. This senior management support across the business has proved to be critical to the success of the awareness programme.

Other non-interactive mechanisms, such as intranet articles, emails, posters and publications, are used to reinforce important messages. However, it has proved difficult to gauge how many people have read or understood the messages and people can easily ignore them. So, they are used as a complement to, rather than a substitute for, classroom training.

The main measure of the impact of the awareness training is feedback and questionnaires completed on or shortly after training sessions. This feedback gives a good insight into the impact of the training on the individual. Generally this has been positive, with the vast majority saying that they have learned something new and will try to change their behaviours.

Other ways to test awareness, such as checking the strength of passwords or mocking up social engineering type situations to gauge responses, have been considered. However, these are not used, due to concerns about dependence on other variables (such as the mood of the person), privacy and entrapment.

The company is now focused on ensuring that training continues to engage people; e-learning modules are being developed to add variety. A continual process is underway to enhance the relevance of the material to staff, so they can see the benefits and understand the risks more clearly.

International financial services group – changing times drive changing needs

A large international financial services group explained why a new approach to information security awareness has been implemented. The firm's objective is for customers and staff to view the firm as the safest place to do business. The firm believes good security is good business.

Given its size and the diversity of its operations, the firm and its customers are subject to continually changing threats. Fraudsters have always targeted banks, but the increasing use of the Internet has changed the nature of these fraud risks; keeping losses to customers and the firm under control is a strong driver for security.

There also appears to be a shift in the regulatory and cultural environment. Countries outside the EU (such as the US and Singapore) already have more prescriptive requirements for information security training. The climate within the EU appears to be changing. Information security and privacy are becoming more important on people's agendas. In this changing environment, the bank wants to make sure it is ahead of the curve.

This has driven some changes to their global awareness strategy over the last year. Corporate information security policy has been altered and awareness and training are now mandatory. Job descriptions and individuals' objectives are being tailored to include information security responsibilities.

A challenge is the size and scope of the different divisions of the company. A centralised team is now in place to co-ordinate the awareness and training strategy and set training standards for information security awareness across the firm. Individual business units are then responsible for implementing the policy and standards in their local operations.

The firm has found that the most important thing is to have a structured approach, and not just do things in an ad-hoc fashion. In this vein, the firm uses a variety of techniques to keep the messages and media channels fresh, including a security web portal. Keeping the material relevant and up-to-date has helped the effectiveness of the message. Currently, there is not much face-to-face training, although there are plans to include more of this later in the programme. This will be initially targeted at the key influencers and managers, so that it has the biggest impact on the culture. If management buy into the importance of security awareness, they will drive and promote it within their business units.

While some business units use computer-based training (CBT), they are not as widespread as was initially planned. There were plans for a centralised global CBT system. However, due to the diversity of the business and the cost of updating material, this was not implemented. Other techniques they have found to be ineffective are "free stationery"; pens, pencils, etc.

Despite the very structured and clearly defined approach adopted, quantitative assessment of the impact and effectiveness has proved problematic. An information security specific self assessment used to be carried out regularly to gauge the level of awareness with staff. However, this was discontinued since it required a large amount of resources to co-ordinate and analyse, and it was found that some of the results were misleading. People will answer surveys with the answers that they think you want to hear and not what is actually going on. The survey suggested staff knew procedures well; however, the results of internal and external audits showed that this was not always correct.

The firm is now focusing on measuring and reporting on training, as well as watching the results of internal and external audits closely. Now that information security awareness and training requirements are set in policy, the central team can review audits and compliance measures to monitor the levels of awareness and the effectiveness of training.

Approaches to raise awareness

The foundation for any framework for information security awareness is a formal security policy. Without an outline 'law' covering the use of systems and information, enforcing good behaviour is very hard.

Good practice standards place a strong emphasis on having an organisation-wide security policy. For example, ISO 27001 suggests that organisations implement training and awareness programmes. There is a requirement of management to ensure that people working for them apply security according to polices. To accomplish this they are required to provide appropriate awareness training and regular updates in organisational policies and procedures, as relevant for the job function of all employees of the organisation and, where relevant, contractors and third party users.

Incidentally, many standards also suggest or require that a company's security policy should also include user awareness training.

Recent surveys suggest that the number of companies with a formal security policy in place has never been higher. Among our respondents, 88% have a specific security policy, and a further 76% refer to security requirements in their staff handbook.

A key component of any information security policy and awareness training is to analyse the threats and risks that the business faces. This analysis should drive the areas that the policy and training need to cover.

Every organisation faces changing environments, threats and risks. To be effective, any awareness initiatives should be supported by senior management. Ideally, it should have board or executive level endorsement, to enhance the importance of the topic with staff. If senior management do not treat awareness as important, it is unlikely that training will be successful.

Most standards recommend that a formalised approach is adopted to information security awareness. A virtuous circle involves three reinforcing elements:

1. Requirements analysis: Management need to identify what topics staff need to understand. Users should be made aware of the sections of the security policy that are relevant (to their job function). Many standards suggest topics to consider, such as spyware, virus outbreaks and strong passwords.
2. Training tailored to role: Both contractors and employees should receive training, appropriately geared towards their role. They should also be regularly updated with any relevant changes to the security policies or procedures. Training needs to address how staff can implement security in their day-to-day procedures.

3. Ongoing review: The awareness programme's content should be revisited and revised periodically. The effectiveness of the awareness programme on the intended participants should be reviewed regularly. Any appropriate changes to the original security policy should be reflected in the corresponding information security awareness training programmes.

Recent security surveys (such as the UK DTI information security breaches survey) indicate that:

- The vast majority of businesses take some steps to make their staff aware of their security responsibilities. Companies are doing more to educate their staff than in the past. Most large businesses include security responsibilities in their staff handbook and train new employees in security;
- Almost every company with a security policy takes steps to educate its employees about their security responsibilities; and
- The higher the priority that information security is to senior management, the more likely the company is to educate its staff. For example, only half of those for whom security is not a priority at all have taken any steps to raise awareness.

This study shows a consistent pattern. All the respondents use some techniques to make their staff aware of their security responsibilities.

As with much else in business, having an approved budget is vital to achieving an effective awareness programme. It takes both time from staff and money to create appropriate materials. This is an investment in the future of the business; it should be approved by senior management.

Despite the high priority given to security, many respondents find it difficult to justify significant spend on awareness programmes. Only a third of respondents build a formal business case to justify this expenditure;

International airline – engaging with the right people is critical

An airline explained why information security is a very high priority to their senior management. The terrorist threat continues to be severe. This makes it particularly important that staff pay attention to physical security. In addition, the airline captures and stores large quantities of personal and financial information (such as immigration data and credit card details). This data is frequently transferred between countries, so data protection and privacy are big concerns.

One big challenge is the number and diversity of staff employed – over ten thousand people spread across many countries, both within the EU and worldwide. A wide range of different techniques are used to reach different types of end user. For each department, risk assessment is used to understand the type of information at risk, the nature of past incidents and the best way to communicate with staff. This then drives a tailored training approach. Giving the same training to cabin crew and to a database administrator, for example, just does not work.

Face-to-face sessions with staff have been by far the most effective technique, producing the greatest impact on awareness and behaviour. Both workshops and training sessions have been used. Having a person to talk to and an interactive forum for discussion can help to make people realise what they can and should be doing.

The downside of face-to-face training is that it can be time intensive and costly to deliver. Targeting face-to-face training on the areas at greatest risk, coupled with the provision of computer-based training for lower risk areas, helps address this. Making the training as relevant and interesting to the target individuals as possible (e.g. including sessions on home computer security) can help overcome the perennial challenge of getting time in people's diaries.

Posters and email messages have been the least effective at raising awareness. With both of these, there is a tendency to overburden people with information, which they do not fully take in. Also, these media are not interactive and tend not to provoke much thought in the reader.

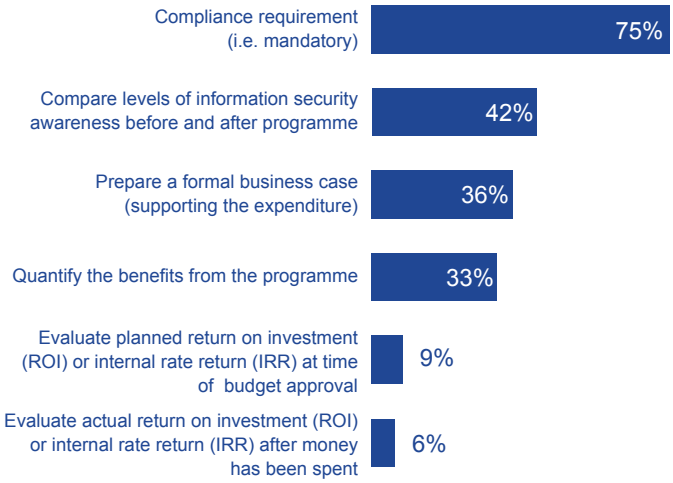
When it comes to measuring the effectiveness of the awareness programme, quizzes and surveys have proved to be the most effective techniques. Comparing the results before and after training gives a true reflection of people's understanding and helps gauge the effectiveness of the training. Quiz responses also often highlight weaknesses in specific areas. This has enabled management to fine-tune training messages or produce targeted sessions to address any weaknesses.

The number of security incidents reported has turned out to be an unreliable metric. People tend to think that, as people become more aware, there will be fewer incidents (i.e. awareness prevents breaches). However, the airline's actual experience was that greater awareness resulted in a rise in reported incidents. In other words, the first benefit awareness brings is an improvement in the reporting of breaches.

Recently, the airline has started to create formal annual business cases for their security awareness programme. At this time, the benefits are not quantified and there is no formal tracking of return on investment.

Approaches to raise awareness

How do you justify the ongoing cost of your awareness programme?



of these, only half attempt to quantify the benefits that their awareness programmes will achieve, and very few evaluate ROI. 15% of respondents quantify the benefits from their programme even though they do not prepare a formal business case.

Most respondents instead think of security awareness training as something they just have to do, i.e. a compliance requirement. As such, their budget is treated as an overhead rather than an investment. This is interesting, since regulations in most EU Member States do not require specific information security training. It seems that EU data protection laws are driving an increase in awareness training.

Approximately two fifths of respondents justify their programme by comparing levels of information security awareness before and after the programme.

Most respondents conclude that the benefits of improved security awareness are often not tangible and quantifiable. People find it difficult to define good metrics for behaviours. Without reliable metrics to measure change, the effort in working out return on investment outweighs the benefits. Conversely, though, as metrics improve, more organisations should prepare formal business cases.

Once the scope of an information security awareness programme has been defined, the next step is to draw up a communication plan. This entails analysing the audience and deciding which techniques are most appropriate to use.

Just under half of our respondents do this in a formal way; most simply get on with the task at hand.

There is a wide range of awareness raising techniques available. Most respondents use multiple techniques. Companies that give a low priority to information security take the fewest steps to make staff aware of security topics. Their desire to keep costs to a minimum is strong.

Telecommunications provider – the role of risk assessment

A telecommunications provider's IT systems are vital to servicing its customers. Any problems with information security could quickly damage the company's reputation. Having a security awareness training programme in place is, therefore, an Executive level concern.

In this international organisation, the first stage was to get local management to endorse the main messages. Ultimately, it is them engaging with their staff face-to-face that makes the most difference to behaviours. Getting the support of the right people is essential to the programme's success.

The company has a diverse range of people, with different levels of understanding and training needs. A central team provides baseline mandatory policies and training that provides a uniform and consistent set of messages. This includes e-learning modules and quizzes. Additional information and optional training materials are also available. These enable local entities to tailor group security policy and training to the local environment and their staff's needs. The extra material includes posters, screensavers and quizzes.

A global security portal provides all this information. It has proved to be the most effective way to distribute messages across the whole world. For users, the portal is easy to access and quick. For the central team, it is simple to keep up to date with relevant content.

At a country level, getting staff actively discussing issues face-to-face has been the best way to improve awareness. Both induction and ongoing training are used to achieve this.

Regular security risk assessments and gap analyses are carried out for each significant operation. These take place before new major initiatives; the results are used to hone the training, target messages, and help to measure the effectiveness.

Staff surveys measure the level of awareness on an ongoing basis. Once a year, the results are analysed to identify any changes to behaviours. This analysis is then compared with the risk assessments and gap analyses, to judge the impact and effectiveness of the programme.

There appear to be certain basic disciplines that every organisation should adopt. Almost every respondent has defined their security policies, either in their staff handbook or a separate security policy. 85% of respondents have set up an intranet site that provides guidance to staff on information security matters. These techniques are low cost and so there is no reason not to use them.

However, many respondents believe policies, handbooks and guidance alone are not an effective way to improve awareness. It is simply unrealistic to expect most staff to read and absorb all the information they are bombarded with. These techniques serve a useful role in underpinning and reinforcing other awareness raising activities. However, alone they are not effective ways to change staff behaviour.

Respondents find classroom training to be the most effective technique to change the way people behave. 72% include security messages in induction training for new staff. This reaches the highest risk people (new joiners) and is relatively low cost, since security aspects can be incorporated into existing events.

While classroom training is considered highly effective, relatively few respondents carry out ongoing training for existing staff. This could be due to the perceived cost of arranging and running these courses. Time is a precious commodity to busy business people. Getting sufficient time to cover training needs may be very difficult. The most effective awareness programmes appear to be those that target their limited classroom training budget at the highest risk populations. Blanket classroom training appears unlikely to be cost-effective.

Instead, half of respondents are using CBT, and two thirds of these have mandated it to all staff. While there is an investment cost in setting up CBT, once it is running, the delivery costs are very low. It, therefore, lends itself well to ongoing training to a large population of existing users. Consistency of delivery is usually better than with large classroom training programmes. Building tests into the CBT also allows some measurement of how well recipients have absorbed the training.

What techniques have you used to make staff aware of information security issues and their obligations?

Approaches to raise awareness

Retailer – fitting in with the culture

A large retailer explained why being flexible in the approach to information security awareness is important. They handle large volumes of information about customers, such as their financial and credit card details. However, the retail sector does not have as strong a compliance culture as many other industry sectors although Data Protection and PCI compliance are key.

The diverse nature of the work force makes delivering an effective awareness programme challenging. The level of computer literacy varies widely and the age of staff ranges from school leavers to retirement age. Messages need to be tailored accordingly. Staff broadly comprise of three different groups. Firstly, in shops and outlets, staff deal with customers and use tills and stock systems and have generally less IT experience. Secondly, most back office staff and Head Office staff are ordinary users of computer equipment. Finally, the technical teams within IT that have powerful access rights.

A risk-based approach is used to define messages. The key risks that are present for each group of users are analysed. Based on this, key messages for each year are identified and communication plans put in place. Each group faces different risks, so the messages for each group are different.

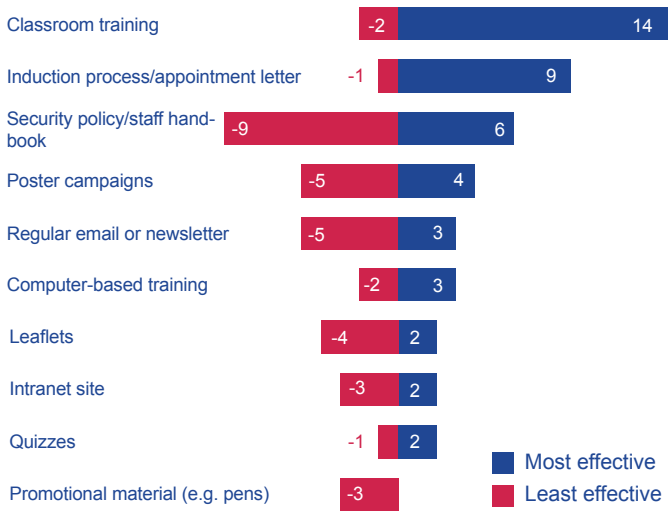
A wide range of techniques are used due to the diversity of the staff. Information security is built into staff induction training; this ensures that people are informed of their responsibilities as they join. In store outlets posters have been particularly effective with good feedback from staff. In the last campaign, security messages were tied into another campaign running at the time and this approach was effective. Using similar presentation of the information for both campaigns helped get a consistent message across to staff. Security needs to be part of, not separate from, the rest of the business.

Face-to-face methods to promote awareness are not widely used to raise security awareness within the organisation especially within the store outlets. Given the large number of staff who use computers relatively little in these locations, classroom training tends not to be cost-effective.

Cultural issues also have a big impact on the techniques used to raise awareness. People do not expect to read long policies or complex handbooks. What works instead is delivering the key messages in a short snappy style for example via leaflets or posters or computer-based training (CBT). Being sensitive and aware of what is appropriate for the organisation has improved delivery of the messages.

Baseline awareness is reinforced by mandatory CBT within the Head Offices. The CBT includes tests; the test scores are monitored. Surveys have been used to measure the success of campaigns; the number of staff knowing key messages is measured before and after the campaign. This information is then used to refine the programme.

What techniques have proved effective at raising information security awareness?



Part of running an effective programme is targeting the right messages to the right people. This involves understanding each group's current information security issues and the extent to which they are aware of them. Surprisingly, only 36% of respondents have any formal mechanism for doing this. This happens more often within financial services than other sectors. Many financial services providers have learned the hard way that it is possible to spend large sums of money on indiscriminate awareness activities without having much impact on the overall risk profile. They now use a combination of blanket coverage basic disciplines and target extra activity on the areas of greatest risk.

Poster campaigns, promotional materials (such as pens) and blanket emails are each used by a significant number of respondents. Many respondents had used these techniques in the past but have now abandoned or scaled back their use. They have a relatively short shelf-life and can be expensive to distribute across the organisation.

There is also a limit to how much information they can convey to the reader, and many people simply ignore them completely.

One in five respondents use surveys and quizzes to drum up interest and raise awareness. Of those that have tried them in the past, more respondents found them effective than not. The proper use of incentives can achieve high take-up and can really get people thinking about their behaviours.

Implementing a successful security awareness programme can be a difficult task. There may be some large or

seemingly insurmountable barriers along the way. What is most effective in the long term is being able to recognise any particular limitations in your efforts, such as a lack of senior management buy-in or a cultural resistance within the organisation. Recognising potential hurdles beforehand will enable plans to be put in place to overcome these obstacles.

Law enforcement agency – ISO standards can help

A law enforcement agency explained why putting in place information security controls in line with ISO 27001 has helped with awareness.

They store and process information that could result in people's lives being put at risk if compromised. As use of IT systems has increased over the years, the need for information security has risen.

Putting in place a structured approach from the start was very important. Government guidelines and industry good practice was combined to create new policies. A dedicated information security function was created.

The initial adoption of new policies and procedures brought into focus areas where staff were not aware of the security risks. People started asking questions: Why change? Were the new procedures necessary? This showed that the existing training in these areas was not sufficient. Based on this, the training and awareness programmes with HR were reviewed. More rigorous risk focused inductions and training were put in place.

Changes since the initial rollout are creating new challenges. Public sector organisations are increasingly networked. Information is being shared with other departments. This makes security even more important. The agency's primary focus is to comply with government legislation and guidelines. The agency also reports on compliance with the ISO 27001 standard to their regulatory body.

Formal face-to-face training sessions have proved to be the most effective way to raise awareness. They allow staff to get to know people within the information security function; they also enable the material to be put across in a more relevant way. Discussion gets people to think about risks and different situations; this has been very useful in challenging and ultimately changing behaviours.

Recently, computer-based training has been commissioned. This will be mandatory - all people within the agency will have to complete it. Tests built into the training will check users' understanding and the delivery of key messages. Results will be analysed; awareness training strategies and materials will then be tailored to address any knowledge gaps identified.

Financial services group – reducing the training burden on staff

A large financial services company explained that information security awareness has a high priority. It is on the board's agenda; they see it as important to retaining the trust of customers.

One challenge is the high percentage of part time staff and contractors. Another is the existing mandatory training burden on staff (anti-money laundering, data protection, anti-fraud, etc.). Linking information security awareness training into other on-the-job training activities has proved vital. The company has recently restructured its security function to bring together physical security, information security and fraud prevention. The key awareness issues from each of these aspects are combined and distilled into a single set of training messages.

Staff show good understanding of some security issues, such as email and mobile devices (phones and lap top computers etc.). Getting messages across in other areas (such as Internet-related threats and instant messaging) has proved harder. The awareness training clearly explains each individual's personal responsibilities for information security. It then provides guidance on good practices the individual can adopt to discharge those responsibilities.

The business demands training to be available as required and in a cost-effective way. To meet these demands, there is a drive to deliver security awareness through on-line systems and self training. Completion of computer-based training (CBT) is now mandatory. Quizzes in the CBT provide statistics that measure the levels of awareness; the CBT itself records the extent to which staff have been trained. The speed, ease of use and consistency of the on-line training programme are seen as key benefits. While the set-up has involved some investment, the efficiency of training delivery achieved has maximised the return on this investment.

Other measures that have proved helpful in tracking staff awareness include the number of mobile devices lost, and the number of concerns and security-related incidents reported.

The content of CBT training is continually reviewed, so that it reflects emerging risks and staff continue to see the benefits. The next stage will be to target high risk groups for additional face-to-face security awareness training.

Measuring the effectiveness of awareness programmes

Many business leaders have observed that “what gets measured gets done”. Ultimately, information security awareness is about people’s behaviours. These are always hard to measure, so this is a challenging area for most organisations.

Different organisations adopt different methods of assessing the effectiveness of information security awareness activities. These include both quantitative and qualitative approaches. In general, there are four main approaches, each with different performance indicators:

1. Process improvement

This approach assesses the effectiveness of the programme by looking at its activities. In other words, these measures are around the effort put into the programme; they do not directly measure whether the end result has improved security.

Possible performance indicators include:

- The extent of development of security guidelines. For example, people can assess how well security guidelines address the main security risks or technology platforms;
- The extent to which the guidance is disseminated. Typical metrics are the number of leaflets distributed, visitors to the intranet site, or staff receiving awareness training;
- The efficiency of the awareness process. The normal measure is the cost of delivery, e.g. cost (in time and expenses) per person trained;
- The relevance of the awareness material. A simple measure here is the frequency with which it is updated; and
- The effectiveness of the deployment of the security guidelines. Surveys that ask staff whether they are aware of guidelines and know what procedures to follow are one way to measure this.

The advantage of process improvement measures is that they are easy to define and to gather.

The disadvantage is that they provide only indirect comfort as to whether the programme is making the organisation any more secure.

2. Attack resistance

This approach focuses on measuring how resistant staff are to a potential attack. Possible performance indicators include:

- The extent to which staff recognise attacks. This normally involves asking specific questions in a staff survey, quiz or computer-based test; and
- The extent to which staff fall prey to attacks. Simulated attacks, such as emails containing executables or people phoning up to ask staff for their passwords, are helpful here.

The advantage of attack resistance measures is that they provide some direct evidence of the actual state of staff awareness. They tend to be good for impressing senior management on the need for investment in security awareness.

The main disadvantage is that there are potentially many attack scenarios; any individual measure will be quite specific to the scenario it is testing. Simulated tests can also be relatively expensive to set up. A risk-based approach can help overcome these issues.

3. Efficiency and effectiveness

This approach focuses on the actual experience of security incidents within the organisation. Possible performance indicators include:

- The extent of security incidents arising from human behaviour. Typical metrics include the number and cost of those incidents. Some organisations also consider the proportion of security incidents arising from human behaviour;
- The extent of downtime arising from human behaviour. This is a particular concern in sectors where availability of systems is critical; and
- The extent to which human behaviour caused the organisation's most severe incidents. Root cause analysis into serious incidents provides this data; the measure is normally then expressed as a proportion of the total number of serious incidents.

Airport operator – the role of metrics and audit

The operator of an airport is subject to an increasing threat from terrorists and other malicious attacks. They regularly transfer large volumes of information between their systems and third parties. Their key control systems are networked. All of this means information security is of critical importance to their business.

They employ a large number of staff from diverse backgrounds, including lots of temporary and contracting staff. As a result, they choose to use a wide range of techniques to raise security awareness. Since some of the staff are not very computer literate, regular topical emails and communications have proved very effective. Monitoring incidents within and outside the organisation allows staff to provide up-to-date guidance.

They have implemented polices and procedures in line with ISO standards. This has not, on its own, improved awareness. Policy is a necessary component of the framework for control, but is simply not very exciting to staff.

Where practical, requirements from the policies have been built into electronic or automated processes. These help staff comply with policy, and produce better activity logs than equivalent manual processes. Reviewing these logs is a quick way to check people's behaviours against policy.

Internal and external audits have played a major role in examining behaviour and checking adherence to process and policy. The audits have successfully highlighted areas where awareness of good practice or policy has been lacking. Since audit reports go to senior management deficiencies are taken seriously. This makes the approval of new security initiatives and awareness training go more smoothly.

Tracking incidents also sheds light on awareness levels. Investigating the root causes of incidents and downtime has highlighted trends in behaviours. These are then analysed to identify any particular gaps in awareness or training and then addressed in the planning of future awareness initiatives.

Measuring the effectiveness of awareness programmes

Government – get safe online

A government department explained how on-line systems are increasingly used to deliver public services. Security is essential to maintaining citizens' trust in the continued use of these and future technologies. The government wants to ensure that the country is a 'secure' place to be online and so is keen that people are aware of the associated security threats. Good information security is viewed as being increasingly important to the success and stability of the country as a whole.

The threats are growing rapidly, with e-crime doubling roughly every 18 months. A recent survey showed that one in ten people had suffered Internet fraud losing 1,200 euros each on average. While often banks rather than citizens take these losses, individuals affected by identity theft suffer a great deal of disruption to their personal life. To reduce this, the government aims to make people more aware of the risks to their electronic information, be it their credit card or social security details.

Within the general public, there is a diverse range of people to reach. Different techniques work well on different audience groups. The level of prior knowledge and age are useful ways of categorising the audience. Overall, many different techniques are used to increase awareness. Some of the most successful campaign elements have been websites, phone-ins, conducting online and offline quizzes and email newsletters. These have been very good at grabbing people's attention and getting across key messages.

Measurement is critical to ensuring the campaigns are delivering the right messages and working as intended. Surveys measure behaviours and perceptions before and after the campaigns. These immediately highlight differences and shed light on the effectiveness and impact of the campaign.

A big challenge is retaining the right balance in the content. The purpose of awareness is not to scare people, but to educate them and change their behaviour. The content and distribution methods also need to remain relevant in the face of a rapidly changing environment.

It is important that there is a joint government and industry approach to promoting Internet safety. Government is not solely responsible for keeping people safe online – industry must also accept responsibility for the safety of their customers to assure the continuing growth of e-commerce.

The advantage of these metrics is twofold: firstly, the data can be gathered through the overall security incident monitoring that most information security groups do anyway; secondly, these statistics are usually of great interest to senior management.

The disadvantage is that they do not necessarily give a true reflection of security awareness. It is not just security awareness that determines whether incidents occur; the extent to which attacks actually occur is the main factor. In the long term, the trend can be a good indicator of awareness. In practice, however, people often take action based on individual incidents; this may not be the most effective approach.

4. Internal Protections

This category is concerned with how well an individual is protected against potential threats. In other words, has the individual's awareness resulted in secure behaviour? Possible performance indicators include:

- The extent to which individuals incorporate security into the development and acquisition of systems. This can be measured by reviewing a sample of business cases and requirements specifications;
- The extent to which individuals protect their data files. Scanning tools can be used to build up a picture of this;
- The extent to which individuals have allowed their systems to be infected by viruses or other malicious software. Normally anti-virus activities can provide statistics on this; and
- The extent to which individuals have allowed their systems to harbour inappropriate (e.g. pornographic) material or unauthorised (e.g. pirated) software. There are specific scanning tools that can quickly measure this.

The advantage of these measures is that they provide direct evidence of staff behaviours. They assess whether awareness is making the organisation more secure and avoid hypotheses or extrapolation. In addition, existing audits (by internal or external auditors) may provide feedback here, effectively for free.

The disadvantage is that any individual measure is quite specific to the behaviour it is measuring. Often, an awareness programme aims to change many behaviours. This can result in many potential metrics. Each, in turn, may require investment in scanning tools or audits. A risk-based or rotational approach can help reduce the ongoing cost.

Most organisations use a combination of several of the

four approaches. Blending different metrics enables them to build up a balanced scorecard for their awareness programme. Decisions are based on the overall picture, rather than on any single measure.

The respondents in this study use a wide variety of different methods to measure the effectiveness of their information security awareness initiatives. All of the measures prompted in our questionnaire have some advocates.

Measures of internal protection are the most popular overall. Two thirds of respondents use policy breaches highlighted in (external or internal) audit reports as a measure. The audits can be undertaken by members of internal teams or may be as a result of external or third party audits. The auditors' objective and systematic approach is felt to make these reports reliable sources of information. In addition, nearly a third of respondents use the results of software scans as a metric for the effectiveness of their awareness programme. Some possible metrics (such as the proportion of systems that are made with security in mind) are hardly used.

Efficiency and effectiveness measures are the next most popular. Many respondents use their experience of security incidents. The most common metrics are the number of incidents caused by human behaviour and root cause analysis of the most serious incidents; more than half of respondents use each of these. A third also consider the proportion of incidents caused by human behaviour. Fewer respondents track cost of incidents, but many of those that do believe this is one of their most important metrics.

A significant minority of respondents use some form of attack resistance metrics. A third include questions on security awareness in staff surveys. They then measure awareness levels before and after initiatives take place. However, some respondents highlight issues with the complexity of collecting and processing this data. A quarter of all respondents carry out tests to check whether staff behave in the right way when presented with a possible threat.

International commercial bank – measuring is critical to targeting efforts

A large commercial bank has a central information security function. This team is responsible for driving awareness training across the world. They aim to get basic messages about security across to a large, geographically dispersed audience. They also need to send specific messages to smaller groups of staff with key roles in systems or security.

A big challenge faced by the bank has been how to measure awareness levels and the effectiveness of its awareness programme. Ideally, the bank wants to measure the change in people's behaviours. This is difficult to assess quantitatively. However, measurement is critical to targeting training efforts at weak areas, so the bank has invested in identifying practical metrics and key performance indicators.

A particularly successful technique has been the use of computer-based training (CBT). A centralised CBT library includes training courses and captures test results from the automated testing of staff. All new employees must complete the training as part of their induction. The training is updated regularly, and all staff must complete the updated training. Reports analyse the extent of completion of CBT training and the scores in tests; the central team monitor these and act on any significant trends.

Password scans provide a useful direct quantitative measure of the attitude and behaviour of staff. The bank periodically runs software that scans password files on key systems and analyses the strength of individual passwords. The number of staff using easily guessable passwords is a key indicator of security awareness.

Other techniques that have proved effective include simulated phishing emails and competitions. These have made the targeted staff think carefully about why they are asked to be secure. They have also provided helpful statistics for trend analysis.

There are plans to introduce a new survey to gauge the level of security awareness and behaviours within the bank. An independent third party will gather responses from a random sample of staff (rather than self-select). This will enable the bank to use the survey results to draw statistically valid conclusions across the business.

Initially, the bank monitored incidents to assess security awareness. However, root cause analysis has shown there are many different factors behind each incident, so the number of incidents is not a true reflection of security awareness. In addition, the frequency of incidents is so low that trend analysis is not meaningful. For these reasons, incident statistics are no longer used to measure awareness.

Measuring the effectiveness of awareness programmes

Public department – blocking and monitoring

A government department explained why enforcing policy and measuring people's behaviours are critical to good security awareness. Security of the personal data they store and process is vital to maintaining the public trust. The time sensitivity of this information is higher than in most private companies. Threats to it, from foreign governments, criminals, and journalists, are numerous. To maintain security, the department needs a rigorous, comprehensive control and awareness framework.

One challenge they face is a high turnover of staff, 30-40% per year. With so many transient staff, maintaining effective awareness is difficult. A key technique to do this is the use of comprehensive induction training. This covers important topics including data privacy and information security. Staff have to sign to confirm they understand and will abide by the department's policies.

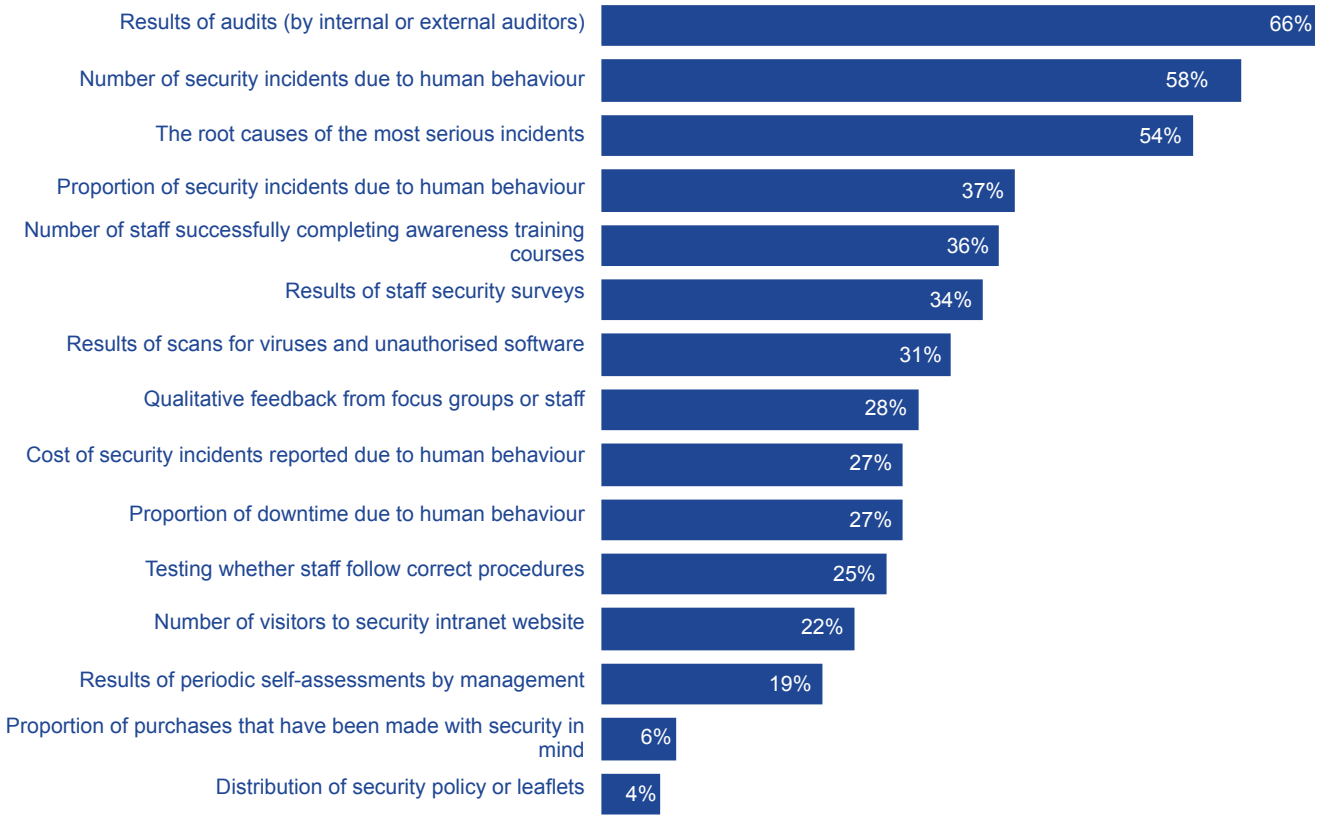
Cost effectiveness drives the approach adopted to raise awareness. The use of intranet sites and emails have been effective. These are instantly available to staff; they can convey important messages quickly and to a wide audience. Surveys were used in the past to gauge awareness; however, response was low and the results did not always provide the required information.

Where possible, information security requirements are automated, i.e. built into systems. Manual spot checks are also used, targeted at high risk systems and areas.

Penetration testing and social engineering are used to assess people's actual behaviours. In addition, to ensure staff are following policy, a random sample of users' emails are audited. Based on these, a 'security league table' report is sent to management. This encourages people to improve their areas. Where specific weaknesses are found, they are addressed with targeted training.

Incidents are also tracked. Due to the relatively low numbers of events, slight increases can be easily seen and analysed. The results are used to target further awareness training if any trends are found. Previous analysis showed that new joiners had lower awareness and changes were made to induction training to address this. Further monitoring of the awareness is accomplished through yearly audits for compliance with ISO 27001.

How do you measure the level of information security awareness in your organisation?



Given the ease with which process improvement measures can be captured, the number of respondents using them is low. Ideally, respondents would like to be able to measure actual changes in staff behaviours resulting from the awareness activities. As a consequence, relatively few respondents find input metrics (e.g. number of visitors to intranet site, number of leaflets distributed) helpful. The most used measures of this type are the number of staff receiving training and qualitative feedback from staff on the programme; roughly a third of respondents used each of these metrics.

There is little consensus among respondents on the most effective measures. This is clearly an area where good practice is evolving.

Even the most popular metrics had been found wanting in some organisations. For example, many respondents have abandoned security incident statistics as a measure of security awareness. One reason is that there are many other factors driving the number of security incidents. Another is that the volume is (mercifully) low and hence spiky in nature; this makes trend analysis difficult.

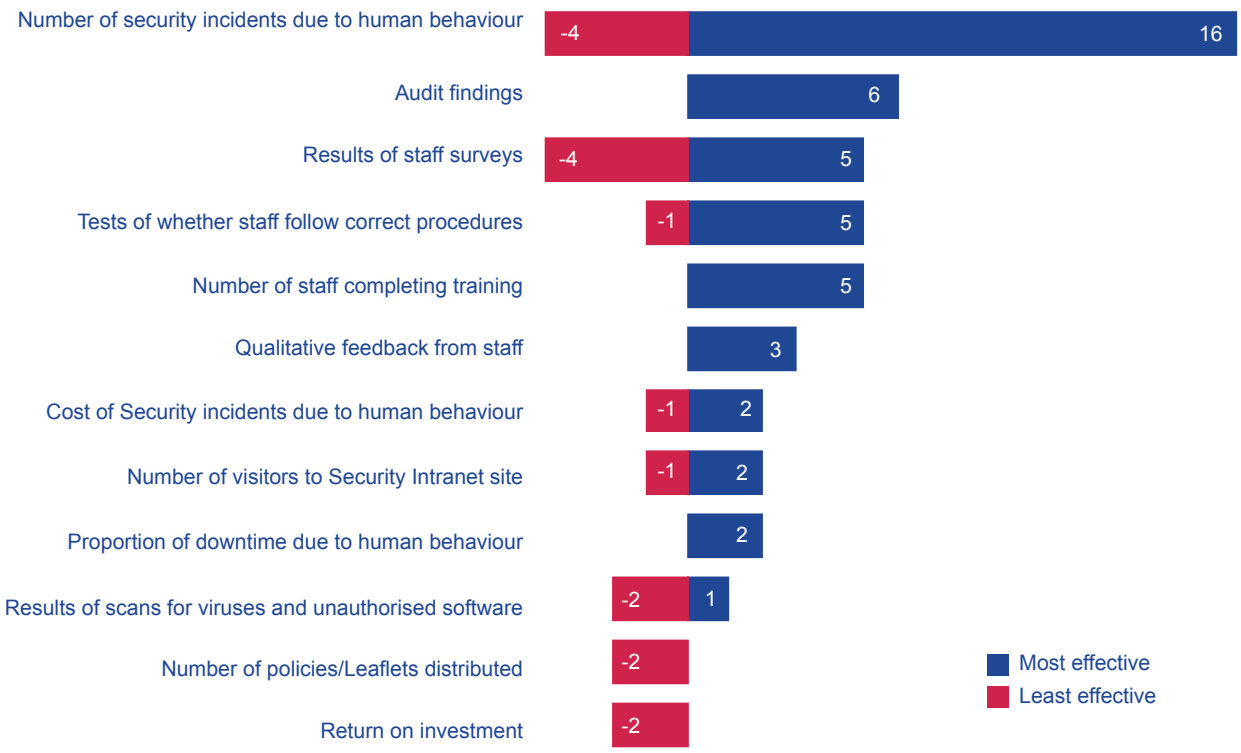
Overall, there was a good correlation between the metrics that were highlighted as most effective and the most popular metrics in actual use across all respondents. As a group, they seem to have learned a lot over the years; their past experience of what works well has shaped what they do today. Most respondents acknowledge that they are continuing to improve their approach, but there is much to learn from what they do today.

Generally the results did not show significant differences between the sectors of respondents. This indicates that what people have found to be effective across industries is broadly similar. Although one particular item of note was that financial services organisations were less likely to use metrics related to the costs of incidents than government, retail, telecommunication and utilities.

Many respondents have encountered problems in the past, putting effective quantitative measures in place. It is important that the method any organisation uses to produce and collect awareness indicators addresses these common issues. The main concerns raised by respondents in this study include:

- **Quality and comparability issues**. A particular issue here is with staff surveys, where the exacting wording and the placement of the question in the survey can affect the answers given. Often staff tell surveys what they think management want to hear, not necessarily what they really think. Compliance returns from senior management (e.g. self assessments) can also be misleading; the people signing the returns are often divorced from the detail of their operations and so report what they are told by their teams;
- **Relevance**. It is important not to take the wrong inference from measures. For example, an increase in virus infection rates may indicate a problem with staff awareness, but it could equally be an issue with the anti-virus software. A rise in security incidents could indicate a problem with awareness (more actual breaches),

What metrics have proved effective at measuring the success of information security awareness activities?



Measuring the effectiveness of awareness programmes

or improved awareness (more reporting of the same breaches). The number of leaflets or emails sent out does not mean anyone has necessarily read them. Using a portfolio of measures enables sense to be made out of what can be a confusing picture;

- **Availability of specific indicators**. Some measures are simply too hard to gather for the payback they give. While in principle, many respondents think return on investment is a sensible approach, most find it hard to quantify the benefits of better staff awareness. In a non-sales environment, estimating the cost of security breaches can be hard; and
- **Processing**. Once data has been collected, it is important to process this and turn it into meaningful information. The information may need to be edited to remove suspect results (for example, if there is a problem with a particular training course). Data may need to be weighted to reflect better the overall staff profile of the organisation. A general rule of thumb is that the less processing the better. Some respondents, for example, have abandoned using before and after comparisons of survey data because of the complexity of the processing required.

In conclusion, there appear to be many reasons why individual metrics might be helpful. Some metrics are used because they provide insight into actual behaviours (e.g. scans or tests). Others are adopted because they resonate with the senior management that sponsor awareness programmes (e.g. cost of incidents). Others are simply easily to hand and require little effort (e.g. results of audits).

Each organisation needs to find the right balance for them; there is no "one size fits all" solution. Keeping the approach simple tends to keep it cost-effective. Many currently struggle with quantifying security awareness; however, provided simple mistakes are avoided, a balanced set of metrics can provide real insight into the effectiveness of awareness programmes. Only with this insight are organisations able to change their programmes from a compliance activity to one that really benefits their operations.

An example of a balanced set of key performance indicators is provided in the following table. This combines the five most popular measures used by respondents into an overall security awareness dashboard. Also listed are case studies in the report where these particular metrics are being used; these include more information about how to use them effectively to assess the level of awareness.

Metric	Points to consider	Case studies
Number of security incidents due to human behaviour	Can quickly show trends and deviations in behaviour. Can help understand root causes and estimate costs to the business. May not be enough incidents to draw meaningful results. May be other factors that affect the incidents.	Financial services group – page 13 Airport operator – page 15 Public department – page 18
Audit findings	Generally conducted by independent and knowledgeable people who can provide third party assurance on behaviours. May be significant areas of awareness not reviewed.	International finance services group – page 7 Airport operator – page 15
Results of staff surveys	If used before and after specific training, can be used to gauge the effectiveness of campaigns. If sufficiently large, can provide statistical conclusions on staff behaviours. Need to be targeted at verifying key messages. Have to be carefully designed since staff may respond with 'expected' answers and not true behaviours.	International insurer – page 6 International airline – page 9 Telecommunications provider – page 10 Retailer – page 12 Government – page 16
Tests of whether staff follow correct procedures	Very good way of actually measuring behaviours and highlighting changes after training. Have to be carefully planned and carried out since could be breaches of employment and data protection laws. Need a big enough sample if results are to be meaningful.	International commercial bank – page 17 Public department – page 18
Number of staff completing training	Need to decide what combination of classroom and computer-based training to use. Have to consider what training to make mandatory. May need to be tailored for different areas or regions. May need regular and potentially costly updates.	International finance services group – page 7 Retailer – page 12 Law enforcement agency – page 13 International commercial bank – page 17

European Network and Information Security Agency
P.O. Box 1309
71001 Heraklion
Greece
Tel: +30 2810 39 1280
http://www.enisa.europa.eu