Information security awareness in financial organisations

November 08

enisa

European Network and Information Security Agency

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

Contact details:

For contacting ENISA or for general enquiries on information security awareness matters, please use the following details:

Email: Isabella Santa, Senior Expert Awareness Raising — awareness@enisa.europa.eu
Internet: http://www.enisa.europa.eu/

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004. This publication does not necessarily represent state-of the-art and it might be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

enisa
European Network
and Information
Security Agency

Information security awareness in financial organisations

November 2008

Acknowledgments

Several parties supported and contributed directly or indirectly to this work in a number of ways. The information includes contributions from members of the ENISA Virtual Working Group (VWG) on "How to organise awareness raising programmes in financial organisations". This VWG and its members are part of the ENISA Awareness Raising Community.

ENISA wishes to acknowledge and thank Mr. Thomas Schlienger, whose initial support and co-operation have influenced some prevailing aspects of this project, the member of the VWG and their organisations, Ms. Kate Dodds of Sai Global, Mr. Mathieu Gorge of VigiTrust, Mr. Jorge Pinto of Banco Credibom, Mr. Thomas Schlienger of TreeSolution Consulting GmbH, Ms. Paula Davis of Sai Global, Ms. Sissel Thomassen of InfoSecure, Mr. Stefan K. Burau of Clariden Leu for prompt support, valuable input and material provided for the compilation of this paper.

Finally, the author would also like to acknowledge Ms. Kate Dodds of Sai Global, Ms. Colette Hanley of Betfair, Ms. Isabel Milu of Banco Credibom, Mr. Luke O'Connor of Zurich Financial Services, Ms. Tone Thingbø of Norges Bank who contributed to this document with reviews, valuable insights, observations and suggestions. The content would be incomplete and incorrect without their help.

Contents

Executive summary

This report targets decision-makers and staff involved in developing information security awareness programmes in financial organisations, a sector which is increasingly threatened by information security breaches. The average loss caused by theft of customer information is on the rise, as is the cost of responding to security incidents. Security breaches in financial organisations not only damage reputation but also cause heavy financial losses, which can be difficult to recover from.

According to the 2008 report of the UK Financial Services Authority (FSA), financial services firms could significantly improve their controls to prevent data loss or theft. Moreover, employees are now considered the single most likely cause of security incidents as confirmed by many international surveys including the 2007 Global State of Security and the 2008 BERR survey. Technical solutions are no longer the panacea that they might have been in the past. The effort to mitigate the security risks evolving around the human element is growing, and constitutes an important financial commitment for any organisation.

The objectives of this publication are to explain the importance of information security awareness in financial organisations, to analyse the environment and the business drivers which may impact such programmes, and to provide a communication framework to better organise an awareness initiative. Case studies and recommendations are given to help as a starting point for the awareness raising professionals and teams.

The first part of the report is an assessment of the environment of financial organisations and their main business drivers. In these environments, information security awareness must integrate with the ongoing information security and compliance requirements set by legal and industry mandates. It is extremely challenging to run information security awareness training initiatives and at the same time ensure business continuity and disaster recovery in such a demanding operational environment. This is because the flow of data, apart from requiring high levels of protection, cannot be stopped or reduced even for short periods of time in this type of business.

The paper then focuses on the landscape of international standards, fundamental legislation in place and certification objectives together with major risks, threats and end-user behaviour with regard to information security. Several parameters define the awareness strategy to be followed in addition to those mentioned above, such as audience segmentation, roles and job functions, geographical location, multiculturalism and so forth.

The second part covers the different phases of implementation of awareness raising programmes in financial organisations and the assessment of results. To ensure that information security awareness corresponds to the objectives of a financial institution, it should be a continuing and ever-evolving process. Factors to be taken into account in the planning, designing, implementation phases are presented in this chapter together with tools for measuring the success of awareness raising initiatives.

The third part includes practical advice, recommendations and case studies provided by a number of private organisations.

ENISA hopes that this paper will provide financial organisations with a valuable tool to improve understanding of the importance of data loss and prepare and implement awareness raising and training programmes. Providing information security awareness is a huge challenge in itself for any company; awareness raising in this targeted industry sector is an important first step towards meeting that challenge.

PART 1: Business environment and main drivers

Introduction

Governments and regulators have attempted to address information security threats through the implementation of a range of legislation and regulation such as the Data Privacy laws, Computer Misuse laws, Sarbanes Oxley and so forth.

Failure to ensure the appropriate use and adequate protection of an organisation's information assets may well result in a breach of one or more of these requirements and may also result in adverse publicity relating to the misuse of information or resources - with an associated potential loss of consumer and shareholder confidence. Penalties are increasingly draconian and varied in form; for example SOX fines can be up to $15m with accompanying actions against company officers and Basel II has the potential to result in increased capital adequacy requirements with costly implications for profitability.

Most security risks are driven in practice by the lack of a well-defined and managed information security culture, with errors and breaches frequently caused by human error and a failure to follow procedure. The UK Department for Business, Enterprise and Regulatory Reform (BERR) reported in their 2008 Information Security Breaches Survey that 47% of UK large businesses suffered from staff misuse of information systems ([1]).

Metrics in themselves are compelling - the average loss from theft of proprietary information is on the increase as is the cost of responding to security incidents. The 2008 BERR survey reported that 77% of UK businesses spent their information security budget on protecting customer information and 72% on maintaining information integrity. The average total cost of a UK company's worst incident is between £ 10,000 and £ 20,000, with direct financial loss (such as loss of assets, fines etc.) between £ 500 and £ 1,000.

In 2007 the Financial Crime and Intelligence Division (FCID) of the Financial Services Authority in the UK handled 187 financial crime cases, of which 56 involved data loss. Due to the nature of their business, mismanagement of data security could constitute a significant risk to financial organisations They generally hold large volumes of personal and financial data about their customers, such as names, addresses, dates of birth, bank account details, transaction records, PINs, national insurance numbers and so on ([2]). Safeguarding this personal and financial data is a key responsibility of the financial services industry.

Additional technology alone will not solve these issues; a more holistic approach is needed that incorporates behaviour and culture, as well as technology. While policies and technical controls are certainly a critical part of any information security (IS) programme, these measures alone cannot deliver sufficient assurance that information is protected in practice. In order to be effective, information security awareness programmes are reliant on the actions of individuals within the organisation. Employees are, of course, the real perimeter of the organisation's network and their behaviour is a vital aspect of the total security picture.

([1]) BERR, *2008 Information Security Breaches Survey*, 2008, available at http://www.security-survey.gov.uk (last visited on 22 July 2008).

([2]) Financial Services Authority, *Data Security in Financial Services*, United Kingdom, April 2008.

Research and analysis conducted by ENISA suggest that effective employee awareness, where employees not only understand their obligations but routinely act upon them, is one of the most effective ways of managing the information security risk faced by any large organisation today.

Purpose

ENISA considers the poor state of data security as a serious and widespread issue. It recognises that effective employee awareness for managing information security risks is crucial, especially within financial organisations. This white paper aims to provide an introduction to the importance of information security in this specific industry sector. It also aims to provide valuable tips on preparing and implementing information security awareness initiative.

The document is structured in three parts covering the following issues:

- ✓ Assessment of the financial organisations environment and main business drivers.
- ✓ Awareness raising programme in financial organisations.
- ✓ Practical advice in the form of recommendations and case studies provided by a number of private organisations and models.

Objectives

The objectives of this publication are for ENISA to:

- ✓ Explain the importance of information security awareness in financial organisations.
- ✓ Analyse the environment and the business drivers which may impact such programmes.
- ✓ Present case studies and recommendations to be used as starting points by the awareness raising team.
- ✓ Contribute to the development of an information security culture and promote knowledge sharing between Member States.

Audiences

This white paper is for use by staff and decision-makers in financial organisations, when undertaking information security awareness raising programmes. It also seeks to raise awareness of the importance and criticality of endorsing information security awareness within their organisation.

Background

The Awareness Raising (AR) Community is a subscription-free community open to experts who have an interest in raising information security awareness within their organisations. The AR Community was launched in February 2008 and is designed to engage with the Awareness Raising Section of ENISA in its mission to foster a culture of information security — with the aim of supporting the Section in its activities.

Contributors to this paper offer a diverse range of skills, and knowledge, as well as differing interests, a range of areas of expertise and a variety of business priorities. Their combined analysis allows the AR Community to play a key role in the exchange of information security good practice across Europe.

Being a point of contact for matters related to information security awareness, the AR Community invited members to take part in Virtual Working Groups (VWG) to explore in further detail relevant topics aiming at producing white papers.

This paper relies on studies and analyses conducted by the ENISA VWG "How to organise awareness raising programmes in financial organisations", ENISA staff and through information that is publicly available or has been supplied to ENISA by appropriate organisations.

Financial organisations: a definition

This paper targets financial organisations, in particular decision-makers and staff involved in developing information security awareness programmes, to ensure the ability to secure data and to assess related risks as well as to plan effective training and awareness initiatives in order to prevent information security breaches and incidents.

We refer to financial organisations in a generic way to indicate retail and wholesale banks, investment firms, insurance companies (life and general), financial advisers, credit unions and payment service providers of any size.

Assessment of environment and main drivers

An introduction

There has been much talk of information security incidents and data breaches in financial organisations in the last year. Of course, most of us will have focused our discussion on the banks as they are the centrepiece of the financial world. However it is worth noting that due to the current regulatory climate, all financial organisations are currently reviewing their approach towards information security and especially towards security education for staff at all levels of seniority. This phenomenon includes credit card associations, merchants from the retail industry, payment service providers as well as insurance organisations.

These actors of the financial world are subject to multiple legal and industry frameworks regulating how they should educate staff on dealing with information and how to protect sensitive information. Whilst some frameworks offer clear guidelines as to why, how and how often information security education must take place, others remain vague. Financial organisations must all consider the following important questions:

- ✓ What legal and industry frameworks apply to my financial organisation and to our way of doing business?
- ✓ Does our current information security strategy allow the organisation to take a pro-active approach towards security in order to meet compliance requirements as well as industry security mandates?
- ✓ How do our information security awareness programmes and staff education initiatives compare with the demands of financial industry best practices?
- ✓ Is information security awareness approved and fully endorsed by senior management?
- ✓ Has information security awareness been positioned as a business enabler and, if not, how can my organisation turn information security awareness initiatives from a cost centre to a return on investment and productivity enhancement tool?

The challenge for financial organisations, however, is firstly to plan for IS awareness raising activities and to then deliver awareness programmes. This is due to the nature of their business. Staff are continuously engaged in guaranteeing data flows all the time as downtime cannot be afforded. The recent example of the London Stock Exchange being unable to function for an unprecedented period of time shows just how IT system failures can affect daily work. A way of dealing with this challenge is to extend existing generic induction and training programmes to include information security awareness. Information security awareness must, nevertheless, be part of an ongoing security and compliance process: education first, then remediation and, where applicable, official accreditation/compliance and, finally, accreditation maintenance through ongoing information security awareness initiatives. Maintaining this iterative process is very important for financial markets as they are fundamental to the world's critical infrastructure (CI) and therefore much scrutinised by consumers, businesses and Governments.

The financial industry is typically governed by two types of mandates: legal mandates and industry frameworks. Whilst there is some level of convergence between both elements, such that compliance with industry guidelines may become a legal requirement, most financial legal frameworks are independent of industry frameworks that regulate the design, development and implementation of information security awareness initiatives in financial institutions. Notwithstanding this aspect, one should however note that in the last five years, the industry has clearly seen common objectives between legal and industry frameworks emerge with regard to information security for financial institutions. This is due to the fact that the number of identity theft incidents has soared and major breaches have occurred primarily in the UK and in the US. This is relevant as these two countries are the key global financial centres and have, as a consequence, been leading the way in developing legislation and regulation to tackle these problems. In addition, the requirement to notify security breaches has been imposed in many jurisdictions worldwide and is becoming the norm across the globe. For instance, the concept of Senate Bill 1386 in California (SB 1386), which details when and how consumers, authorities and the media need to be notified of data breaches, was used as a model for similar state legislation in the US where over 40 states now have notification laws. A number of countries in the EU, including the UK and Ireland, are exploring similar avenues. This is important to note because if notification of security breaches becomes a legal requirement, then more efforts are likely to be accorded to preventing breaches in the first place. This also means that all staff within financial institutions will need to become all the more aware of information security threats and will require formal education in the risks associated with processing financial data.

Review of business drivers

The main driver for compliance with legislation and industry mandate is the fear of penalties and prosecution for failure to comply (which may involve civil or criminal law suits). Whilst there is rarely any direct financial or legal ("safe harbour" type) rewards for compliance, it can result in reduced insurance costs in some cases.

Fundamentally, with regard to awareness requirements, financial organisations should be familiar with compliance and governance mandates and security frameworks in order to understand which apply to them globally or nationally and which impact the whole financial industry. The main business drivers revolve around demonstrating good governance and compliance whilst actually increasing information security both for the financial institution itself and for its customers and suppliers. In other words, the financial organisations' ecosystem makes all of its actors interdependent and there are clear links between those responsible for promoting standards and those who must implement the standards down the chain, for example with Payment Card Industry Data Security Standard (PCI DSS) requirements. By complying with legal and industry mandates, we are making use of industry frameworks to protect sensitive data and ensure continuity of operations within this ecosystem. Technically, this is achieved by focusing on reducing legal exposure, protecting public relations and the reputation of the brand by protecting consumer financial assets and the identity of each individual customer.

The Payment Card Industry Data Security Standard (PCI DSS) is probably one of very few security standards which actually dedicate a full control objective to information security awareness training (requirement 12.6). It includes requirements for information security awareness programmes and touches on multiple layers of the financial organisations industry from the card associations to other entities such as the acquiring banks, payment service providers, merchants and any third party in this chain which might store, process and transmit credit card information. As such, compliance to the requirements of PCI DSS will be expected from most high street retailers as well as any corner shop able to take credit card payment. The standard applies to all entities worldwide. It consists of 12 high-level requirements each associated with a set of policy, procedure, technical controls and skills transfer requirements. Requirement 12.6 states that an entity "needs to implement a formal security awareness programme, and educate employees upon hire at least once annually on the importance of cardholder data security". It also covers how compliance with the rule is to be checked for the most stringent level of PCI DSS (level 1) which requires an annual on-site audit to be performed by Qualified Security Assessors (QSAs). An entity "needs to be able to demonstrate through training records that all staff in scope have been trained. In addition, you need to be able to produce the security awareness material and show that it has been updated on a regular basis to reflect changes in your own cardholder data environment as well as new requirements within the standard". From a more holistic perspective, all entities are responsible for raising awareness levels of those downstream in the PCI chain, such that acquiring banks are responsible for promoting the standard to all of its merchants which in itself requires a security awareness raising project.

ISO/IEC 27001, the international standard for information security originating from BS7799, and complemented by ISO/IEC 27002 and 27005, is also gaining traction and includes a provision for information security awareness programmes. Although the ISO/IEC 27001 framework can be applied to any organisation, it is not unusual to see financial organisations it as a benchmark for good information security practices with a view to complying with a wide range of legal and regularly frameworks, including PCI DSS (note: the UK Post Office delivered a presentation at a recent PCI DSS seminar stating how they used ISO/IEC 27001 as the basis for PCI DSS Compliance since implementing an information management system (ISMS) will go some way to cover a large number of PCI DSS compliance requirements).

At a more fundamental level, whilst some of the newer members are still refining their data protection and retention regimes, the European Directive on Data Protection of 1995 has been adopted in most EU countries. Whether you consider for example the Irish Data Protection Act, the UK Data Protection Act, the Portuguese Data Protection Law, the German Datenschutzgesetz or the French Act's, Loi n° 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés, most European legal frameworks governing data protection include clauses whereby organisations are required to "take appropriate security measures to safeguard the good name of the company, its employees, affiliates and customers" and insists on protecting "key data including any financial information" it may hold ([3]). The means recommended for achieving that goal is security awareness programmes.

In Ireland, this has been very well communicated by the Office of the Data Protection Commissioner. A number of banks and insurance organisations have registered with the Office and developed security awareness programmes for staff and even for their customers, the end-consumers. Some

[3] *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, OJ L 281 of 23.11.1995. Also in the *Irish Data Protection (Amendment) Act 2003*, Article 2 "(a) "personal data" shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity", available at http://www.dataprotection.ie/documents/legal/act2003.pdf.

banks, such as Ulster Bank, have rolled out basic education programmes for their merchants to help them with PCI compliance whilst others are actively engaging with employees in a bid to raise security awareness levels.

Traditionally, financial institutions have always tended to be ahead of the game with regard to information security awareness programmes, along with some government institutions, the IT and pharmaceutical sectors. However, initiatives have remained focused around ad hoc training seminars dealing with fraud and identity theft or on social engineering. This type of effort is no longer sufficient (if it ever was) to meet legal and industry mandates or to reassure consumers. Consumers expect that their financial information is kept safe as a matter of fact and that their financial assets are protected even in the event of a network information security breach suffered by the bank. In other words, whilst consumers may not fully understand the ramifications and demands of putting in place security strategies, controls and safeguards, they still expect financial institutions to protect the money they have entrusted to them. This is called trust.

Financial institutions have to provide a controlled and secure environment for consumers. However there are noticeable regional and industry variations in the way legal and industry frameworks mandating information security awareness training are applied to the target "markets" of a given financial institution. This is often a major challenge for large international financial organisations who must understand the local regional legal mandates in order to incorporate them into a wider corporate information security awareness strategy which will allow them to ensure that internal corporate security standards are met whilst compliant with national and country-specific legal requirements.

Best practice to develop such an awareness strategy within financial organisations usually involves several steps:

- ✓ Step1 – Categorise the business into country/zones subject to similar legislations and industry frameworks in order to make the project more manageable.
- ✓ Step 2 – Identify data protection and data retention frameworks applying to each category.
- ✓ Step 3 – Define a full specification for information security awareness mandates for each category.
- ✓ Step 4 – Perform a gap analysis against existing awareness programmes and update programmes to address legal/industry mandates.
- ✓ Step 5 – Deliver updated programme to all categories.
- ✓ Step 6 – Make steps 1 to 5 an ongoing process subject to annual reviews (at least).

The development of such strategies and programmes take it as given that an Acceptable Usage Policy for corporate communications tools is in place and that a data classification schema has also been approved by the board governing what constitutes confidential, sensitive and public data for the financial organisation.

Most financial institutions will include key topics in their programmes: protection of personal data, details of monitoring techniques used by the organisation (which is a requirement under the EU Data Protection Directive), and guidelines for data transfer (such as from EU to US). Attention may also be given to notification mechanisms whereby notification for incidents taking place in the US will be mandatory and notification in the EU will be internal to the security team first. The team will then work with the local data protection enforcers to ensure they notify when required.

Financial organisations are also typically good at measuring success rates of information security awareness programmes. They tend to use matrix-based measurements which include reach (has the organisation reached out to all its staff across all territories?), understanding (has the target audience fully understood what is required of them, why and how to improve security?) as well as behavioural change (ensuring that bad security habits are no longer in use and that all staff are fully security aware).

It is also worth considering the fact that most large financial organisations are in a position to take a holistic approach towards information security awareness. Senior decision makers who must become involved in this process remain the prime point of contact/target for government and industry frameworks enforcers and as such will want to foster a culture of information security using the measurable and long term vision for information security awareness described above. This means that they will be looking to ensure that the programmes are sustainable (i.e. a long term programme that will evolve as the financial organisation's business model may change and reflect on emerging threats as well as new legal and industry mandates), consistent (always and fairly applied to all staff regardless of seniority or rank), efficient (measured for effectiveness and improved on an ongoing basis) and transparent (fully communicated to all staff including penalties for non compliance with information security requirements as detailed in the awareness programme).

Focus on the US – Latest news in Awareness Raising Requirements: ID Theft Red Flags Rules

This new requirement for US financial institutions is coming into effect on 1 November 2008. It is worth noting that it demands that banking institutions strengthen, document and implement new awareness programmes for employees and customers alike. Training, including that of board members, is a major part of achieving this compliance.

The Red Flags Rule is part of the Fair and Accurate Credit Transactions (FACT) Act of 2003. Under this rule, financial institutions and creditors with covered accounts must have identified theft prevention programmes in place by 1 November 2008, in order to identify, detect, and respond to patterns, practices, or specific activities that could indicate identity theft ([4]).
Banking regulatory agencies are working with their institutions to ensure compliance. Meanwhile, the Federal Trade Commission oversees compliance by the rest of the covered entities identified as creditors.

The State of Banking Information Security 2008 - Survey executive overview

According to the 2008 State of Banking Information Security survey, customer education remains insufficient ([5]). The survey argues that "To secure this trust, they must demonstrate proactive

([4]) See McGlasson, Linda, 'ID Theft Red Flags Rule: How to Help Your Business Customers Comply', *BankInfoSecurity.com*, 8 September, 2008
http://www.bankinfosecurity.com/articles.php?art_id=960andrf=090908eb

efforts to educate customers about online banking safety and the risks of identity theft – including phishing, which occurs via email and telephones outside of the institutions, but still can cause untold damage and erode customer confidence".

This shows that education and awareness raising for financial organisations needs to be carried out internally as well as externally to foster a platform of trust and allow for compliance and governance mandates to be adhered to on a pro-active basis.

Financial organisations' concerns

Following the research and analysis conducted by ENISA it was possible to identify some of the major corporate concerns relating to data security.

- ✓ Market confidence: maintaining confidence in the financial system [6].
- ✓ Consumer protection and awareness: data loss could have a significant impact on individuals.
- ✓ Data leakage: to limit data leakage, organisations could, for example, establish information security policies and regulate the use of mobile devices.
- ✓ Lost data and support costs: an information security policy could help financial organisations recuperate stolen or lost data, which can occur even when security measures are in place, decreasing the costs of ownership and support.
- ✓ Challenges of complying with regulatory and security standards: having enterprises take care of data security will help in complying with the three aspects of information security (confidentiality, availability and integrity) and some security standards and/or compliance framework (such as ISO/IEC 27001, PCI DDS and so forth).
- ✓ Reduction of financial crime.

Risks and threats

Given the structure of financial organisations, the procedures they are required to follow, the frequent use of third parties to provide specialised services (for sending bulk mailings, providing IT services and so forth) and the ability to access, store and transmit sensitive information quickly, easily and efficiently, the number of possible risks and threats is almost infinite. The following can be identified.

- ✓ Data leakage [7]: it is not possible to estimate the effects of valuable data leaking out of an organisation, but the problem is growing.
- ✓ Information loss: it is most likely when sensitive information (for instance customer and/or employee data) falls into the wrong hands, it is kept and eventually re-used for personal use, even when marked as confidential. This can possibly result in legal liability.
- ✓ Information confidentiality: when information falls into the wrong hands, the financial institution suffers a much greater loss than simply the replacement of the cost of, for

[5] See 'The State of Banking Information Security 2008 - Survey Executive Overview', *BankInfoSecurity.com*, available at http://www.bankinfosecurity.com/whitepapers.php?wp_id=143 (last visited 20 November 2008).

[6] Financial Services Authority, *Data Security in Financial Services*, United Kingdom, April 2008.

[7] Heiser, Jay, *Understanding data leakage*, Gartner, 21 August 2007; 'Data-leak security proves to be too hard to use', *Infoworld.com*, available at http://www.infoworld.com/article/08/03/06/10NF-data-loss-prevention-problem_1.html (last visited on 2 June 2008).

example, the drive the information was stored on.

- ✓ Information integrity: when content is modified.
- ✓ Corruption of data: when unintentional changes are made to data
- ✓ Data security: smuggling information out of the business. There is a risk that the data will be used or sold for criminal purposes.
- ✓ Damage to company business/reputation/image: when data is stolen the resulting publicity can be extremely damaging to the reputation of the company and therefore negatively impact business.

- ✓ Market leadership loss.
- ✓ Malware: when malicious software code is introduced to the network, being a virus, worms, spyware or trojans.
- ✓ Fraud/deception:
  - Extortion.
  - Identity theft: for example in the UK, a laptop with data of some 2,000 people with individual savings accounts (ISAs) was stolen from a HM Revenue & Customs employee; HM Revenue & Customs lost personal details of 6,500 private pension holders; nine NHS trusts lost patient records kept on disk ([8]).
  - Theft of intellectual property, trade secrets, proprietary information.
- ✓ Money laundering.
- ✓ Market abuse.

Audience segmentation: a definition

A large part of the planning of a training and awareness campaign in an organisation is to ensure that the programme is delivered efficiently and effectively and that the content is easily understood. It must be in a format everybody can understand.

A corporate programme may be difficult to apply across an organisation where the message may have to be changed to fit the country's culture, laws and regulations. Local customisations are often required for any corporate message however the programme must be delivered in the recognised company style to have the same look and feel.

- ✓ What is already in place across the corporation/locally?
- ✓ What other initiatives are in place (link in with current initiative)?

Job functions

Staff need to be divided into target groups depending on job function. Each target group will have different requirements for training and awareness. Applicable content needs to be arranged in modules and delivered efficiently. Their availability and place of work (i.e. mobile workers, home workers and so on) must be considered when defining the content.

[8] ENISA, *Secure USB Flash Drives*, 2008, available at http://www.enisa.europa.eu/doc/pdf/publications/Secure%20USB%20drives_180608.pdf

To allow a targeted training programme, it is necessary to group people into different job functions/target groups and define the business risks for the different target groups to enable appropriate training.

To prevent wasted time and frustration, it is important that an awareness initiative is targeted and only applicable training should be provided. By delivering applicable training in the correct format, an organisation will have motivated their staff by providing them with a relevant message and will prevent unnecessary use of time and funds by avoiding hours of inappropriate training.

Because information security is a pervasive issue, different groups of employees have different needs of education. Besides regular awareness for employees in general which should include, among other topics, proper usage of organisation resources, alert procedures, business continuity responsibilities, compliance and ethics issues, the following specific groups are a small example of the different types of training that can exist:

- ✓ Employees with access to internal client information in direct or indirect contact with the public, such as call centre employees and tellers, should have access to information regarding issues like social engineering and privacy regulations due to the fact these employees have access to client information and could unwillingly provide it to unauthorised parties.
- ✓ Employees with access to internal business information in contact with the public like salespeople and account managers should be made aware of the need for information confidentiality regarding internal business processes, partnerships and control mechanisms within the company that directly or indirectly affect the strategy of the organisation.
- ✓ IT staff should have training that include the regulations the company is subjected to, internal control and auditing mechanisms in place as well as the organisation strategy regarding best practices for computer and network security management.
- ✓ C-Level staff (CEO, CFO and so forth) are in charge of the organisation and are, ultimately, responsible for it, so a specific training/awareness programme should be developed in order to identify and maintain awareness in respect to existing regulations and how they can affect the organisation (in both a positive or negative way).

When designing an awareness programme, it is imperative that all the roles are clearly defined and match them to information security topics. The tables below provide a list of roles and related description and a sample of a model with the roles down the left-hand side and across the top the information security topics that they may need to be aware of:

Role	Description
Senior Executives	Need to be aware of information governance issues as well as the legal frameworks, risks and liabilities (including personal liabilities). They are typically time-poor and unwilling to undertake the same awareness activities as the general population. Short and much focussed awareness activities are best with clear links between information security and the protection of the organisation's reputation.
Clerical and administrative staff in back office and support functions	These employees often work to strict transaction processing schedules and targets. Careful consideration may need to be given to the organisation and scheduling of training in these areas. It is be important to liaise with managers regarding the scheduling of training and facilitated group training sessions may not be appropriate as there would be too big an impact on 'business as usual'. Most staff in these areas do not work outside of the office and do not make extensive use of portable

Role	Description
	devices. This narrows the range of information security topics that need to be covered and, therefore, reduces the duration of the overall training requirement.
Call centre staff	As with clerical and administrative staff, the scheduling of training is likely to be critical in a call centre environment where prompt response to customer calls is of prime importance. Again, liaison with call centre management will be important. Again, most staff in these areas don't work outside of the office and do not make extensive use of portable devices thus reducing the scope of the training requirement. Data protection and confidentiality, as well as awareness of social engineering is, however, likely to be vital.
Branch staff for retail financial services	Many employees in branches do not have access to their own dedicated workstation and in some retail banks tellers do not even have intranet access. Access to technology-based training is often via shared PCs or managers' PCs and, therefore, requires careful scheduling in order to maintain service levels whilst achieving training objectives. In retail banking, it is also common for more geographically remote branches to have limited bandwidth and challenges accessing the corporate intranet – consideration may, therefore need to be given to optimising delivery of web-based training for this environment.
Sales staff and remote workers	These employees are likely to access the corporate intranet remotely from portable computing devices. They have some particular training needs over and above those in the general population including: ✓ Information security out of the office (security of mobile devices and so on) ✓ Remote access procedures ✓ Travel Security.
Investment banking	Investment banks tend to have performance and compensation-orientated cultures. Presenting the rationale for the training is critical in this group. It is also important to ensure that the training is of the minimum duration possible, that it can be studied in manageable chunks and that the training can be bookmarked so that learners can return to the point where they left the training without needing to repeat any content. Senior management sponsorship from within the business unit is typically critical for the success of an information security training programme within this audience group.
Marketing	Marketing personnel are in charge of public relationships as well as the institution image. They need to know what types of information they can and cannot use whether it's preparing a campaign or interfacing with media in case of an incident.
IT Staff	IT staff should be made aware of the organisation security strategy and what types of controls are mandatory as well as what type of evidences need to be generated in order to insure compliance.

Figure 1: List of roles and related description. Illustrative only.

Some of the information security topics mentioned below may vary for each role depending on the policies of the financial organisation. A bank may permit home working for certain clerical staff, for example. Thus there could be variations in policy that would change the awareness required by that role.

Also, certain topics may be broken down into subsections ("handling customer data" is an important subset of handling sensitive information and may be worthy of its own section) or topics may intersect with other topics ("equipment security" would be present in "mobile working" awareness, for instance).

	Senior Executives	Clerical & administrative staff in back office and support functions	Call centre staff	Branch staff for retail financial services	Sales staff & remote workers	Investment banking	Marketing	IT Staff
Physical security	✓	✓	✓				✓	✓
Workplace security (for example office, branch and so forth)	✓	✓	✓	✓		✓	✓	✓
Equipment security	✓				✓	✓	✓	✓
Internal controls	✓	✓	✓	✓	✓	✓	✓	✓
Recognising & reporting security breaches	✓	✓	✓	✓	✓	✓	✓	✓
Privacy							✓	
Business continuity	✓	✓	✓	✓	✓	✓	✓	✓
Mandatory regulations						✓		
Data protection & privacy	✓							
Retention, storage & disposal of sensitive information	✓	✓	✓	✓	✓	✓	✓	✓
Handling customer data		✓	✓	✓	✓	✓	✓	✓
Portal devices	✓				✓	✓	✓	✓
Removable media	✓			✓	✓	✓	✓	✓
Software (licensing)	✓	✓		✓	✓	✓	✓	
Passwords	✓	✓	✓	✓	✓	✓	✓	✓
Back ups	✓	✓		✓	✓	✓	✓	✓
Malicious code	✓	✓			✓	✓	✓	✓
Mobile & home working	✓				✓	✓	✓	✓
Use of Internet & Email	✓	✓		✓	✓	✓	✓	✓
Third parties (i.e. vendors & visitors)	✓					✓		
Social engineering	✓	✓	✓	✓	✓	✓	✓	✓

Figure 2: Roles match to security topics. Illustrative only.

Geographical location

Implementing an information security awareness programme for staff in different geographical locations is challenging with regard to both the content and the method of delivery. The key challenge is to deliver the training across the organisation and ensure that it is in a format that is recognised and accepted by the different audiences consistently. The following should be taken into consideration:

- ✓ IT Systems/methods for delivering awareness training: in organisations that are spread over a wide geographical area where a common approach is not possible, various alternatives for delivering awareness training are considered. Different parts of the world have limitations due to the available infrastructure. Where e-learning or computer-based training (CBT) training is the preferred method, it is important to identify existing limitations before planning the design of a central or distributed solution. Undertaking a pilot implementation often will ensure that the programme can support the different system requirements and will prevent delays in the implementation process. Key system tests need to be included for:
  - Network bandwidth.
  - Web server limitations.
  - End user systems limitations (audio/video etc).
  - Different Intranet styles.
- ✓ Laws and regulations/legislations vary in each country: data protections/privacy laws vary between different jurisdictions and the following must be considered ahead of producing content in an awareness programme:
  - Ensure that content complies with local laws and regulations.
  - Use local partners and specialists for content where may be insufficient internal knowledge.
  - Customise parts of the programme to cater for local laws and regulations and legislation.
- ✓ Organisational structure
  - Complicated reporting lines: each part of the organisation may have different or unclear reporting lines. Therefore, senior management support is an absolute necessity in every implementation of information security awareness initiatives. In this regard, the project needs to consider:
    - Who to engage with.
    - Management support.
    - Funding.
    - Planning.
    - Development/customisations.
    - Delivery/roll-out.
    - Evaluation.
- ✓ Head Office initiating the awareness campaign: most implementations of awareness programmes have been initiated by the organisation's Head Office with varying degrees of global acceptance. It's important to gain senior management acceptance in each country/region thus ensuring a successful adoption of the programme throughout the organisation. Equally, this approach will ensure that, local requirements are identified at an early stage and programmes customised accordingly.

Mergers and acquisitions

The awareness programme must be constructed to meet the challenges associated with acquisitions and mergers. Programme design must be modular to prevent having to change large portions of content while exploiting opportunities to improve the programme overall. The following should be taken into consideration:

- ✓ Different company cultures: the company may have a variety of cultures and the content may have to be adapted slightly to cater for new requirements.

- ✓ New companies/other processes/other business risks: the risk profile may change because of business merger, and parts of the awareness content may need to be changed or amended.
- ✓ Company profile: intranet style and logos may change. The awareness programme must be sufficiently flexible to adapt content to the new company profile.
- ✓ Management: the awareness programme must be acceptable to new senior and line management. It is, therefore, important that a message from the board accompanies the programme showing senior management commitment and stakeholder commitment to it.

Multicultural environment

Implementation of an information security training and awareness programme in a multicultural environment is a major challenge both between organisations and also internally within each organisation. The differences are on more than one level and the fundamental issue is to recognise them and deal sympathetically with each one, while retaining the integrity of the whole.

Cultural differences within an organisation must also be taken into account during the planning phase. Parts of the organisation may have different organisational cultures, especially where companies have inherited processes and systems as a part of a merger. The following should be taken into consideration:

- ✓ Cultural issues.
- ✓ Gender issues.
- ✓ Religious issues.
- ✓ Racial issues.
- ✓ Attitude to humour (verbal and non-verbal).

Media channels/Method of delivery

The media channels and method of delivery, as well as the message and its sender, must be influential and credible. Otherwise the target group may be less inclined to listen. To engage the audience successfully, more than one communication channel must be used.

The following section details some of the main media channels and method of delivery available to help raise users' awareness as part of an information security related initiative. Moreover, it suggests using a blend of approaches:

- ✓ Targeted modular training: see Audience segmentation above. It is important that the awareness programme is built up using individual modules. This will allow appropriate training to different target groups, at the same time as some of the content can be re-used in different programmes.
- ✓ Use of workshop/e-learning: experiences with implementations show that the best approach for encouraging discussion, and subsequent adoption of the learning in the operational environment, is to run departmental workshops so that the content of the awareness programme can, under the line managers' control, form part of a departmental work plan developed during workshop. This way the employees will have the opportunity to discuss the local business risks and related awareness content with one another and the line manager at their work place.

  Use of e-learning has proven to be more effective where staff are physically located in different areas and where e-learning is already in use within the organisation. The e-learning version should support the workshop awareness programme using the same content to ensure all employees throughout the organisation have a consistent level of information security awareness training. E-learning has also proven to be effective where specific training is required for defined target groups.

- ✓ Use of different content: using a combination of film clips, right/wrong scenarios, learning material, games and self-test questions, has proven to be successful in delivering information security awareness training. Showing film clips of incidents helps people to associate rules with the more practical elements of their jobs. Where a lighter approach and format is offered, people feel more relaxed and will not need a lot of additional learning material in order to understand business risks, how to deal with incidents that happen and, more importantly, how incidents can be prevented from happening in the first place.
- ✓ Awareness vs. Training: Awareness is defined in NIST Special Publication 800-16 as follows: "Awareness is not training. The purpose of awareness presentations is simply to focus attention on security and understand why security is important. Awareness presentations are intended to allow individuals to recognise IT security concerns and respond accordingly. In awareness activities, the learner is the recipient of information, whereas the learner in a training environment has a more active role. Awareness relies on reaching broad audiences with attractive packaging techniques. Training is more formal, having a goal of building knowledge and skills to facilitate the job performance" ([9]).

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.

[9] NIST, *Information technology security training requirements: A role- and performance-based model,* NIST — SP 800-16, USA, 1998, available at http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf (last visited on 21 July 2008).

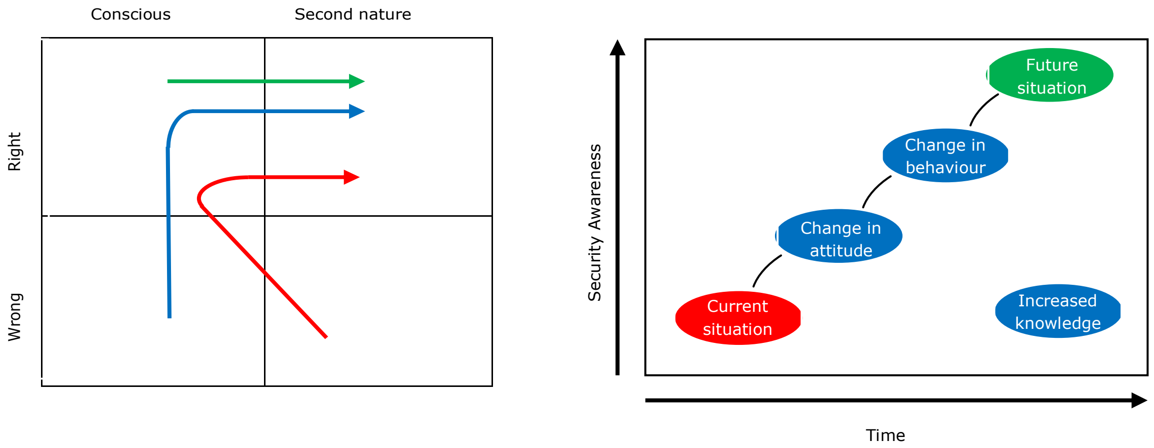

Figure 3: – Information security as second nature.

Training is one of the "how" components to implement information security. A training programme should be designed and developed according to the learning objectives set by the organisation. Thus the training seeks to teach skills which allow a person to perform a specific function, while awareness seeks to focus an individual's attention on an issue or set of issues. The skills acquired during training are built upon the awareness foundation, in particular upon the information security basics and literacy material ([10]).

Awareness programmes start with awareness, build eventually to training, and evolve into education. They should be customised for the specific audience they are targeting. Thus it will be very important to define the users who will attend both programmes. Different methods could be used to define the target audience. ENISA developed a simple tool to identify better a target group and capture the related data, as described in the section "Define target group" ([11]).

([10]) NIST, *Information technology security training requirements: A role- and performance-based model,* NIST — SP 800-16, USA, 1998, available at http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf (last visited on 21 July 2008).

([11]) Herold*,* Rebecca, *Information security and privacy awareness program,* Auerbach Publications, USA, 2005; NIST, *Building an information technology security awareness program*, NIST — SP800-50, NIST, 2003, available at http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf (last visited on 17 July 2008).

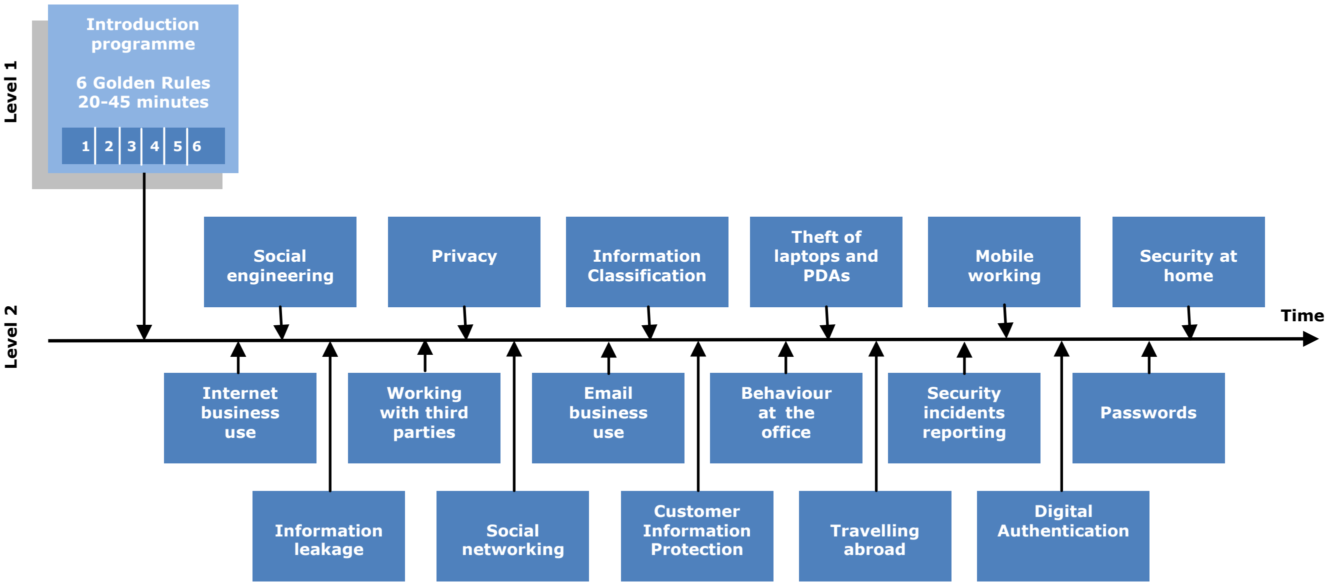

Figure 4: Illustration of continuous awareness programme.

Scalability

The issue of scalability is fundamental to successfully reaching a growing global audience. It might further encourage the modular approach to awareness (segmentation of the audience and the message).

Languages

Getting a message through to people and making sure they understand the message presents another challenge. The formal business language in a company may not be sufficient and understood by all employees and the most effective way of delivering a workshop and e-learning content is to do it in their local languages. Therefore it is very important to consider that in one geographical location there may be several languages. The following should be taken into consideration:

- ✓ Different languages within the same country
  - One country – several languages
- ✓ Different languages between countries
  - International operations
- ✓ Corporate language
- ✓ Different variations of the same language
  - For example business English vs. plain English

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.

PART 2: AWARENESS RAISING PROGRAMMES

INDEX
Oct 24, 2008
1,600.28
-145.39
2-WEEK HIGH: 3,785.75 (Oct 29 '07)
LOW: 1,600.28 (Oct 24 '08)
Feb '08
April
June
Aug
Oct
Points

Awareness raising programmes

Raising information security awareness is not a one-off exercise. In the same manner, an awareness raising programme cannot then be relied on indefinitely in an organisation without further action or modification. To ensure that the programme continues to correspond with the targets of a financial organisation and that information security is incorporated in the organisational culture, awareness must be maintained or raised continuously. It is an ongoing process, a cycle of analysis and change, as we find it in many quality management systems, such as ISO 9001 or ISO/IEC 27001. "Taking [such] a change management approach to an awareness initiative is crucial as it helps close the gap between a particular issue and human responses to the need to change, even in the case of cultural change" ([12]).

The first step is to analyse the actual information security awareness and culture and to identify the main business drivers. If the culture does not fit with the organisation's targets, the culture must be changed. If it fits, it should be reinforced. The necessary controls such as an information security training programme or an awareness campaign must be chosen (planning and design) and realised (implementation). The success of the controls taken must then be evaluated and learning specified (measuring success and programme improvement). The process is illustrated in Figure 5.

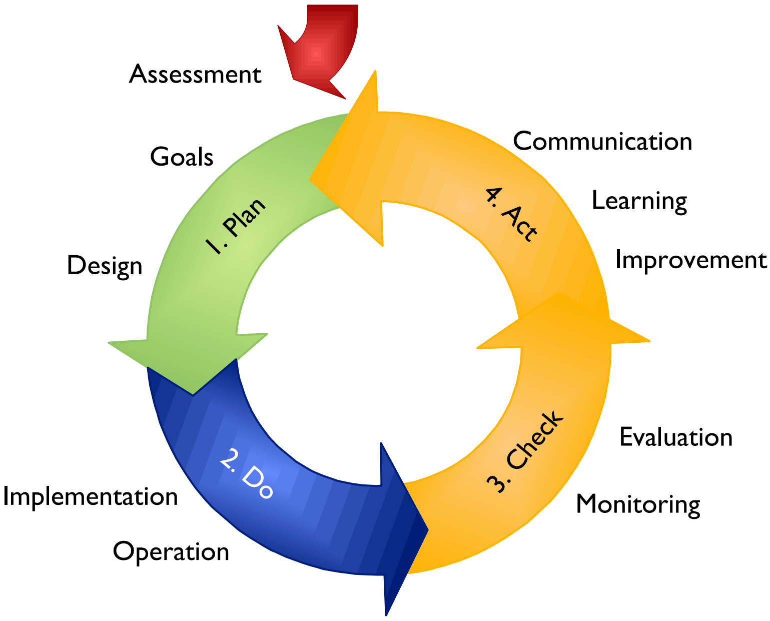

Figure 5: Overall Strategy for raising information security awareness in financial organisations.

Assessment

The need for information security awareness is widely recognised. In order to make a substantial contribution to the field of information security and to choose the appropriate controls, it is necessary to have a set of methods for its study. Despite the fact that information security awareness and culture can be measured, not many financial organisations have tried to quantify the value of awareness programmes.

[12] ENISA, *A New Users' Guide: How to Raise Information Security Awareness,* 2008, available at http://www.enisa.europa.eu/pdf/deliverables/new_ar_users_guide.pdf

According to Gartner, there are four main categories against which information security awareness can be measured ([13]):

1. Process improvement (development, dissemination and deployment of recommended information security guidelines as well as awareness training),
2. Attack resistance (recognition of information security event and resistance to an attack),
3. Efficiency and Effectiveness (efficiency and effectiveness with regard to information security incidents),
4. Internal Protections (how well is an individual protected against potential threats).

In practice, a wide variety of instruments targeting these four categories are used today to assess information security awareness, but there is little consensus on the most effective measures.

According to one ENISA study, the most popular source of information on actual behaviours is internal or external audit ([14]). The research shows that many survey respondents use their experience of information security incidents as a metric. Relatively few respondents find input metrics (for example 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.

Given the ease with which process improvement measures can be captured, the number of respondents using them is low. Organisations also appear to find it very difficult to put effective quantitative metrics in place. For example, only one third of respondents included questions on information security awareness in staff surveys. They then measure awareness levels before and after initiatives take place. Respondents following this quantitative approach highlight issues with the complexity of collecting and processing this data. Given a carefully designed and tested questionnaire, a staff survey on information security awareness provides valuable insights into the factors driving secure behaviour including leadership behaviour, know-how, attitude and motivation. Some case studies report excellent results by using surveys in financial institutes ([15]).

Bearing in mind the difficulties in comprehending all human behaviour and culture, the use of a combination of measurement tools and methods, as proposed by experts in organisational culture, would seem advisable. These allow verification of the results obtained by other methods. The financial organisations are thus able to pick the appropriate methods to assess their information security culture.

A grounded analysis framework allows the financial organisation to systematically analyse its information security culture, to quickly identify weaknesses and improvement actions and also to prove progress when improving an information security culture.

Planning and designing phases

When planning an information security awareness programme there are several factors which should be taken into account. In this section we will look at the most important issues, why they are important and how to deal with them.

([13]) ENISA, *Information security awareness initiatives: Current practice and the measurement of success*, 2007, available at http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_measuring_awareness.pdf

([14]) ENISA, *Information security awareness initiatives: Current practice and the measurement of success*, 2007, available at http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_measuring_awareness.pdf

([15]) Schlienger, T. and S. Teufel, *Tool supported Management of Information Security Culture: An application to a Private Bank*, The 20th IFIP International Information Security Conference (SEC 2005) - Security and Privacy in the Age of Ubiquitous Computing, Makuhari Messe, Chiba, JAPAN, Kluwer Academic Press, 2007.

Approval from the board

The most critical success factor in any project with organisation-wide focus is to obtain executive commitment. This is one of the most powerful levers inside any organisation since executive support not only provides funding, but also provides an example to all levels of the organisation.

Identify drivers

The main output of this activity is to understand exactly why the financial organisation needs an awareness programme. It is important to state the reasons behind a programme, so that it can be made more effective.

Among the most recent reasons for launching an awareness programme for information security we have the related controls imposed by regulations for example as SOX, BASEL II and other country-specific privacy laws.

It can also be a part of the organisation's strategy - several organisations are pursuing certification objectives such as ISO/IEC 27001 for Information Security Management and BS25999 for Business Continuity Management, which ask for a high level of commitment from every employee.

Some control frameworks, like CobiT, also emphasise the need for user training and awareness.

Other possible reasons for launching an

The board should appoint someone to formally sponsor the programme across the organisation. Doing so actively demonstrates to all employees that the programme is part of the organisation's strategy and also guarantees an alignment at all levels of the business.

International financial organisation – Information security awareness programme for all staff

An international financial organisation with substantial influence throughout Europe wanted to implement information security awareness programme for all staff. The aim was to make staff throughout the organisation aware of the seven most important information security rules to follow.

To demonstrate senior management's commitment, it was decided to make a management film featuring the head of the organisation. The management film is a direct message to all staff about the different information security threats and what the consequences would be if staff does not start making information security a part of their daily routines. In the film he also makes it clear that he, himself, will follow this workshop and that he trusts all staff to do their best to cooperate with the initiative; a very strong message from senior management to staff on all levels of the organisation.

The use of different learning methods was also seen as vital to a successful awareness programme. An awareness programme with eye-opening business film clips, learning material and self-tests was selected. This was to make the programme more interesting and to show practical examples of how security incidents could occur.

It was decided that the awareness programme would first be delivered in departmental workshops, utilising a face-to-face approach to engage staff directly and to encourage discussions. The workshop programme was supported with an e-learning version for staff not being able to participate in the workshops and for all new staff entering the organisation. Initiation of local action plans as a part of the workshop was seen as a way of making staff commit to including information security in practice in their place of work.

The test results from the self-test are recorded and MIS is available to show overall participation and the average scores achieved. It was decided not to measure individual results to avoid privacy concerns across the different countries.

awareness programme are changes in the institution's policies, implementation of new systems, employee know-how, corporate values, audit findings, results from risk analysis and so on.

It is important to remember that different areas of the organisation have different needs. The programme manager should meet with top management in order to identify what kind of information their employees should receive regarding information security. For example, if the employees are not aware of the organisation's information security policy that should be the first action of the programme.

The drivers should be included in the programme so that there is good general awareness of why the organisation is investing resources in the project.

Identify requisites and needs

There are different types of requisites, needs and constraints to be identified before programme design.

Depending on the size of the institution, the project managers might want to look at different geographical and cultural details, for instance country-specific laws and languages in the first case and cultural values in the second case.

International Swiss private bank – Information security culture assessment & awareness programme

Information Security (IS) is an important issue for private banks. A number of steps, such as staff information and clear desk flyers, have been and are being taken to address and improve the quality of information security. However, to ensure that the required level of security is maintained, staff trainings are a vital part of this process.

The management has requested suggestions on steps that can be taken to implement a security awareness programme and seeks assistance in a companywide rollout of this programme.

Firstly, the IS-culture was assessed by means of a quantitative staff survey. Different subcultures have been identified. This is the effect of a merger which resulted in the creation of one company.
Secondly, countermeasures were defined in order to raise the maturity level of IS awareness. These measures were realised within a global awareness programme.

The global IS awareness programme included:

- ✓ CEO film demonstrating the commitment of the management to the IS programme.
- ✓ Definition of six golden security rules.
- ✓ An e-learning programme including a test.
- ✓ Management workshops.
- ✓ IS awareness promotional material like posters and flyers for all staff and locations.
- ✓ New IS awareness intranet presence.

For the successful realisation of this IS awareness programme two factors were essential: first that key people from Marketing & Communications as well as from Human Resources were part of the project team; second that the executive board members were fully committed. Indeed, these two factors were crucial for the success of this IS awareness programme. In addition, it was important to use a unique IS awareness brand. A unique branding was created for all communication measures such as the e-learning programme, posters, flyers, management workshops and the intranet portal. The branding was represented by a photo which was created thanks to the active cooperation of employees. It was a true eye catcher solution. While it perfectly represented the programme it also raised the consciousness for the project. Hence, the programme was very well perceived by the staff.

In a next step it is planned to evaluate the outcome of the IS awareness programme through another quantitative assessment approach. Furthermore an IS awareness management process is going to be installed to constantly optimise the IS awareness level at the bank.

The requisites and constraints relating to end users need to be identified and related to each other in order to build more effective training curricula that align with the institutions' objectives. All these points should be validated with the Human Resources department.

Budgetary and resource requirements must also be determined; different media and methods have different costs, and the organisation may be willing to invest different resources for different awareness methods.

Another provision which might impact on your planning or content is the requirements of regulations and standards. For example, if the organisation is planning to obtain certification against ISO/IEC 27001, there are two key factors to consider regarding the timing and the type of training. Firstly, new personnel need to understand the organisation's information security policies and expectations before being allowed to use the services or access the organisation's information and secondly the need to provide ongoing training programmes to ensure personnel continue to understand the organisation's information security controls.

Design the programme

Having identified the factors that influence and impact the design of the programme, it is now time to begin building the programme itself.

At this stage and based on the identified education and training needs, identify the following:

- ✓ Target groups and their members. Some examples are the administration board, the CxO level, the operational risk team(s), IT teams, employees by role and so forth.
- ✓ Efficient delivery mechanisms, for instance computer based training (CBT), classroom training, intranet materials, posters etc.
- ✓ Timings. If the project has different phases it is very important to plan the right beginning and duration of each so that information overload to the employees can be avoided and the

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.

momentum of the programme maintained.

- ✓ Session performance evaluations and benchmarking. In order to assess the effectiveness of the programme, metrics should be defined at this stage in order to provide for monitoring and reporting on training effectiveness. One method for achieving this is to conduct a survey before and after the training sessions.
- ✓ Metrics for evaluating training content, quality, effectiveness, cost and value. These metrics will allow for future curriculum definition.

Review the design

After finishing the information security awareness programme it is time to present it to the board and top management for reviewing and final sign-off.

At this time, special care should be taken to show that the programme's objectives are directly connected to the organisation's objectives and explicitly support them.

Implementation phase

This section of the report covers how to deploy a successful awareness campaign and considers:

- ✓ Building a platform for delivery.
- ✓ Assigning project resources.
- ✓ Planning and executing the roll out.

Build a platform for delivery

One of the key challenges for any IS training project is the roll out, administration and management of the various learning solutions that will ultimately make up the full awareness programme.

Most organisations that are seeking to deploy comprehensive and ongoing awareness solutions implement a learning management system (LMS). These systems typically:

- ✓ Track employee usage of e-learning, recording progress, completion rates and other performance data such as test scores.
- ✓ Produce a range of management reports that can be accessed by administrators and managers at the centre and in the regions.
- ✓ Import and export data from and to other applications (for instance the HR system).
- ✓ Allow for user profiling in order that content can be assigned to users according to pre-defined characteristics (for example job role and/or preferred language).
- ✓ Manage the roll-out of learning solutions across the business in order to minimise impact on business and network resources.

A learning management system allows the organisation to deliver a range of awareness solutions to a variety of target audiences while allowing the system administrator to track usage and completion rates and to assign content to individuals based on, for example, their job role or department. These systems are purpose built and are particularly effective when large, complex and ongoing awareness initiatives are being implemented.

Although students can self-enrol in most LMSs, the full potential of the system is best realised when the database is pre-populated with appropriate student data. In particular, pre-population of the database allows the administrator to control the assignment of learning materials to pre-defined groups of students and hence to carefully manage the roll out of courses. Also, if the database is pre-populated, tracking and reporting (particularly of students who have been assigned to, but have not completed courses) is much easier.

Assign project resources

Adequate resourcing of large-scale information security awareness initiatives is critical for their success. Outlined below are some of the key roles and responsibilities that would typically be required for the completion of a project of this nature.

Role	Tasks	Commitment
Project manager	✓ Monitors progress against plan. ✓ Co-ordinates internal resources. ✓ Manages the relationship with vendors.	Involved throughout the project – participates in regular progress meetings.
Subject Matter Expert	✓ Agrees the overall approach to the content of the awareness programme. ✓ Approves content.	Involved in the early stages of the project in defining requirements and reviewing content Subsequently, occasional contact with instructional designers and developers to maintain relationship and identify any future developments that are required.
LMS Administrator	✓ Maintains the LMS. ✓ Produces management information and reports	The time commitment for the LMS Administrator depends upon how frequently changes to the configuration of the system are required and what the MI and reporting requirements are.
IT Help Desk	✓ Provides support to users once the programme is rolled out.	IT Help Desk should provide support to users regarding the operation of the LMS and any e-learning courseware as part of the routine Help Desk duties. It can be helpful to provide a short training session for Help Desk staff during the implementation.
Corporate Communications	✓ Provides support and advice regarding internal marketing issues, branding and so forth.	Involved in the early stages of each deliverable approving visual identity, styles etc. Can help to plan and execute internal marketing campaigns to promote awareness of the training initiative.
Line of Business Representatives	✓ Provides liaison with key business lines.	Involved in supporting and promoting the internal communication campaign and the roll-out strategy May also be involved in user acceptance testing and piloting of learning tools to generate buy-in from specific businesses.
IT and /or HR Representative	✓ Provides interface to HR systems for pre-population of the LMS	Involved in the initial set up and pre-population of the LMS

	database.	database and subsequent updates to the system for joiners, leavers and movers.

Figure 6: Key roles and responsibilities. Illustrative only.

Plan and execute the roll out

There are several key factors to consider when planning the roll out of a comprehensive awareness programme:

- The roll out plan should include pilot testing of all materials before "going live". Pilot programmes should test the effectiveness of the content of the learning tools from an instructional perspective. Importantly, where technology-based training is being delivered, there needs to be pilot testing from a technical perspective to ensure that the training functions adequately in all of the proposed business environments.
- Where a learning management system is being used to manage any or all of the roll out, there should be sufficient time to ensure that it contains all of the required student data, and that invitation and reminder emails have been drafted, tested and approved. Roll outs can often fail because learners experience difficulty accessing the content via the LMS or because email invitations are not clear or helpful.
- A phased roll out (other than in the most urgent of circumstances) is usually preferable to a "big bang" approach because:
    - It minimises the impact on network resources for technology-based training
    - It minimises the impact on "business as usual" for the organisation
    - It allows for issues to be identified and addressed on a rolling basis so that they are not experienced by large sections of the target population
- The roll out should prioritise any areas of the business that are considered high risk from an information security perspective.
- Consideration should be given, in global organisations, to the requirement for language versions of any training content. Ideally, the roll out strategy should allow for the full completion and testing of a "base" language version (usually the main business language of the organisation) prior to the development of further language versions. This approach ensures standardisation and consistency across languages and minimises the management, administrative and financial overhead of maintaining multiple language versions during the development phase.
- The roll out should be planned around other known initiatives within the business (such as major training initiatives, product launches, financial year ends and so forth) so as to minimise competition for the attention of the intended audience groups. Liaison with Learning & Development, HR and internal communications departments will usually yield much useful information about other initiatives.
    - The visible commitment of senior managers within the business units to the aims and objectives of the awareness programme is a critical success factor. Any awareness initiative should therefore begin with events (presentations, briefings and so forth) to engage the attention and active support of senior management. Many large organisations take a cascade approach to management communications, providing managers with their own presentation packs or "meetings in a box" to drive the message down the management line.
    - High quality learning tools often fail to have impact in organisations because of a lack of internal marketing and PR. Information security is not a topic of inherent interest to many employees yet their "buy-in" to the key messages of any awareness campaign is critical to bringing about any meaningful behavioural change and embedding a culture of security. The active support of the Internal Communications department should be sought in "selling" information security and security awareness to the target population. Typically this can be achieved using a variety of internal communication

tools and channels to create the initial "launch campaign" as well as ongoing communications to help maintain levels of awareness.

- If the planned programme included external vendors and suppliers it is important to ensure that they:
  - Have strong internal procedures and project management capabilities to ensure delivery of solutions on time, on budget and to the desired quality.
  - Have an appropriate combination of learning and development expertise and subject matter expertise to deliver effective learning solutions.
  - Consideration should be given to providing feedback to managers and the wider target audience about the successes and impacts of the training campaign so that individual employees are aware of the outcomes of their learning activity and can be encouraged to see the time investment as worthwhile.

Full service bank — Creating an enterprise-wide security training and awareness campaign covering both general users and technical specialists.

This project, for a global financial institution, was designed to bring about a step change in information security training and awareness at an enterprise level. With 50,000 employees in over a dozen countries, the brief was to reach all employees and deliver training customised to meet varying job roles and responsibilities.

After a detailed consultancy phase a three-strand solution was recommended. This comprised general information security training and awareness for non-technical employees with concurrent training for managers and executives. The solution was delivered in several languages via a Learning Management System, complete with evaluation tools, and a follow up programme of refresher training.

In addition, a detailed series of workshops and support materials was developed for technical and security employees, comprising a core curriculum covering secure application development, access controls and intrusion management for developers, technical architects and systems administrators. These were delivered across several international locations, but with stranded material reflecting particular job roles and responsibilities. The training initiatives were combined with an overall internal marketing campaign. Deliverables included a detailed communication campaign with tag lines, newsletters, presentations "in a box", executive briefings and a revamped information security portal for the corporation.

The Outcome...
Reduced vulnerability and heightened awareness of business critical security issues and responsibilities across the enterprise.

Measure the success and improve the programme

Measuring success provides valuable information about the efficiency and effectiveness of the controls implemented. It helps to evaluate the controls taken, to define necessary follow-up and also to legitimate investment in information security awareness. This is especially important in applying for the following year's budget. Evaluation of a campaign or training programme is essential to understand its effectiveness, as well as to use the data as a guide to adjust the initiative to make it more successful.

To highlight the changes achieved in a culture, the same measurement instruments as during the assessment should be used. They can be complemented by specific evaluation on the controls taken to reveal its effectiveness. If for example an awareness training programme was implemented know-how test can assess the learning goals reached.

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.

When measuring success, qualitative and quantitative instruments can be put in place. Regardless of the measure used, it is important that any organisation address these issues ([16]):

[16] ENISA, *Information security awareness initiatives: Current practice and the measurement of success*, 2007, available at http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_measuring_awareness.pdf

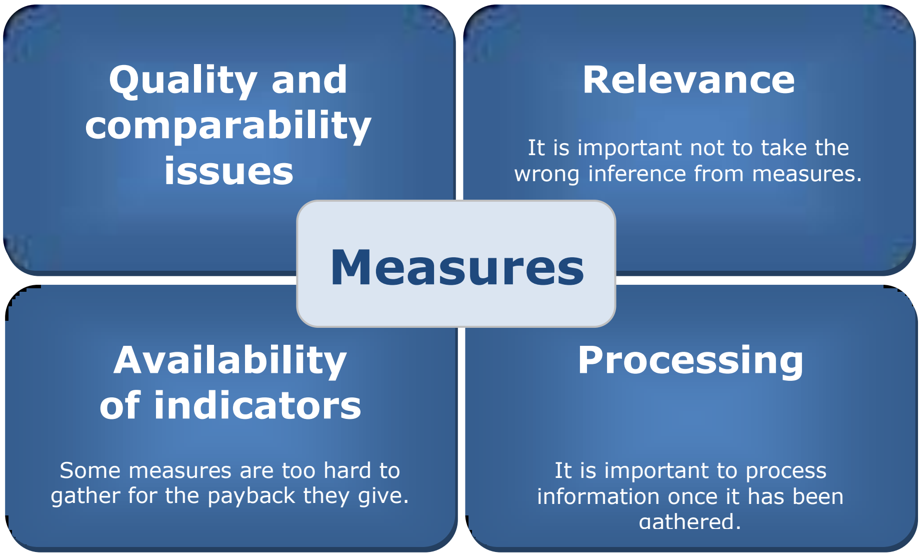
Quality and comparability issues
Relevance
It is important not to take the wrong inference from measures.
Measures
Availability of indicators
Some measures are too hard to gather for the payback they give.
Processing
It is important to process information once it has been gathered.

Figure 7: Measuring the effectiveness of awareness programmes.

Evaluation can evidence change and improvement in an information security culture and also reinforce organisational learning thereby encouraging continuous improvement and a strong information security culture.

PART 3: Guidelines for good practice

Good practice guidelines

Based on the information gathered and subsequent analysis, this section provides good practice guidelines that can help readers and their organisations while looking at data security and planning effective training and awareness activities.

Recommendations

	#	Recommendations
Information security policies and procedures	**1**	• Define written information security policies and procedures to ensure data security. Define who has access to which type of document. Specify in which format documents can be accessed, either electronic or paper-based. • Avoid giving access to all personal and financial information to all staff, including for example bank account and credit cards details, recording of telephone conversations. It is a quite common practice for financial call centres to record telephone conversations containing sensitive data. Particular attention should be given to this. • Include a monitoring access mechanism to personal and financial data. • Include a reporting mechanism in case of data loss including when and how to notify affected customers. Specify roles and responsibilities for financial organisations' employees. • Provide laptops and mobile devices such as PDAs only to senior management and staff who work offsite regularly. • Only give access to the internet and email to staff with a business need. • Encourage the use of strong passwords.
Physical security	**2**	• Regulate access to corporate premises including visitor access. • Implement a clear-desk policy. • Store personal and financial records in a locked cabinet when leaving the office. • Dispose shredders.
Data security risks	**3**	• Personal and financial data security is a crucial responsibility for every organisation. Every piece of data can be of value to fraudsters as they can access multiple sources of information and aggregate it.
	4	• Review the quality of risk assessment and related processes.
IT controls	**5**	• Define access rights on recruitment, when employees change job or leave the organisation. • Define individual user accounts. • Back-up data on a regular basis. • Encrypt data when necessary. • Establish procedures for business continuity and disaster recovery. • Explain to employees the importance of personal and financial data security and the risks associated with the use of mobile devices, such as laptops, PDAs and USB flash drives, the internet and email.
Controls	**6**	• Coordinate different business areas such as Human Resources, physical security, and information security so as to avoid focusing only on IT controls. • Apply the same type of controls in all sites regardless of their geographical locations. This applies to offshore operations as well.
Internal audit and compliance	**7**	• Conduct internal audit and compliance reviews of data security on a regular basis.

	#	Recommendations
Staff recruitment and vetting	**8**	• While recruiting personnel, conduct high level vetting for all staff. • Keep in mind that junior, temporary and call centre staff often have a wider access to personal and financial data. • Even if under pressure to fill vacancies quickly to maintain a good level of customer service, ensure that appropriate vetting is always carried out.
Third parties	**9**	• Define within the corporate information security policy if third parties, for instance call centres, archiving firms and IT consultancies, can access personal and financial data and how.
Awareness and training initiatives' setup	**10**	• Most important is to get support and funding from senior management. The board must understand the organisation's dependence on information, recognise its value and importance as well as understand the regulatory and legal business environment.
	11	• Information security awareness is never an IT business only. The most important aspects of an awareness programme are communication, marketing and training. It is therefore strongly recommended to set up an interdisciplinary project group with members of the internal communication department, marketing department, human resources department, physical and information security department.
	12	• Keeping the pace during the project is an important success factor in every project. It may be good in some situations to plan different stages instead of committing to a more complex and longer plan.
Customisation of the awareness programme	**13**	• The awareness programme must be customised to the needs of the organisation. Generic programmes most of the time fail because of the missing business link and non-specific content.
	14	• A tailored programme needs defined cultural values related to risk awareness. An information security document framework with an issued policy statement, guidelines and standards defines these values. The documents must be up to date, approved by the board and they also must reflect the way of working at the organisation. In many cases the policies are not up to date and do not reflect the implemented procedures. In this case it is recommended that the policies be reworked.
	15	• It is essential to understand the levels of awareness in the organisation. Workforce time is very precious. A training programme should be as short as possible and as long as needed. It is therefore wise to know the strengths and weaknesses of the information security culture and to tailor a programme targeting on the specific weaknesses of the organisation.
	16	• It is critical to tailor the programme to the specific needs of the target audience group. Not every user needs the same information. People will ignore the message if they receive too much or un-specific information.
	17	• Minimum recommended target groups for financial institutions are: ○ Senior Management ○ All staff ○ Staff working with confidential data.
	18	• The programme must also respect the different cultures in different countries. Cultural surveys show that people in Europe, South America and Asia have a different perception and attitude towards information

	#	Recommendations
		security.
Change management process	**19**	- Never think that a one-off project will change information security awareness in the long run. Information security awareness follows the curve; at the beginning one can measure increased awareness and motivation, but then the curve flattens and even may drop to its original state. Awareness deals with changing the behaviour of people and that may need years.
	20	- It is therefore recommended to follow a change management process. Continuous awareness communication and training are good examples of how the attention on the topic can be kept high. It is also very important to evaluate each step and to adjust the goals and measures if needed. This requires you to take into account the feedback of your target audience.

Figure 7: Recommendations.

Conclusions

Recent incidents involving data loss have forced many organisations to consider how they can significantly improve their data security. In particular, safeguarding personal and financial data is a key responsibility for the financial services industry. The mismanagement of data security is a significant risk for financial organisations due to the nature of their business as they generally hold large volumes of personal and financial data about their customers, such as names, addresses, dates of birth, bank account details, transaction records, PIN, national insurance numbers and so on. Thus, the financial services industry needs to pay close attention to how they handle this type of data.

Financial organisations are becoming more aware of the potential costs of losing data. However, corporate information security policies, procedures and controls are not enough to prevent data loss through lack of employee awareness about the risks related to handling information.

Effective training and awareness mechanisms are crucial in these organisations as the risks to which they are exposed, for instance identity theft, money laundering, market abuse may all result in considerable inconvenience and possible financial loss to the victims as well as damage to the organisation itself.

ENISA hopes that this paper will provide financial organisations with a valuable tool to understand the importance of data loss and prepare and implement awareness raising and training programmes.

References and sources for further reading

BERR, *2008 Information Security Breaches Survey*, 2008, available at http://www.security-survey.gov.uk (last visited on 22 July 2008).

'Data-leak security proves to be too hard to use', *Infoworld.com*, available at http://www.infoworld.com/article/08/03/06/10NF-data-loss-prevention-problem_1.html (last visited on 2 June 2008).

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281 of 23.11.1995.

ENISA, *A New Users' Guide: How to Raise Information Security Awareness,* 2008, available at http://www.enisa.europa.eu/pdf/deliverables/new_ar_users_guide.pdf

ENISA, *Information security awareness initiatives: Current practice and the measurement of success*, 2007, available at http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_measuring_awareness.pdf

ENISA, *Raising Awareness in Information Security – Insight and Guidance for Member States,* 2005, available at http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_cd_awareness_raising.pdf

ENISA*, Secure USB Flash Drives*, 2008, available at http://www.enisa.europa.eu/doc/pdf/publications/Secure%20USB%20drives_180608.pdf

Financial Services Authority, *Data Security in Financial Services*, United Kingdom, April 2008.

Heiser, Jay, *Understanding data leakage*, Gartner, 21 August 2007.

Herold, Rebecca, *Managing an Information Security and Privacy Awareness and Training Programme,* Boca Raton: Auerbach, USA, 2005.

Herold*,* Rebecca, *Information security and privacy awareness program,* Auerbach Publications, USA, 2005.

McGlasson, Linda, 'ID Theft Red Flags Rule: How to Help Your Business Customers Comply', *BankInfoSecurity.com*, 8 September, 2008 http://www.bankinfosecurity.com/articles.php?art_id=960andrf=090908eb

NIST, *Building an information technology security awareness program*, NIST — SP800-50, NIST, 2003, available at http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf (last visited on 17 July 2008).

NIST, *Information technology security training requirements: A role- and performance-based model,* NIST — SP 800-16, USA, 1998, available at http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf (last visited on 21 July 2008).

Schlienger, T. and S. Teufel, *Tool supported Management of Information Security Culture: An application to a Private Bank*, The 20th IFIP International Information Security Conference (SEC 2005) - Security and Privacy in the Age of Ubiquitous Computing, Makuhari Messe, Chiba, JAPAN, Kluwer Academic Press, 2007.

‘The State of Banking Information Security 2008 - Survey Executive Overview’, *BankInfoSecurity.com*, available at http://www.bankinfosecurity.com/whitepapers.php?wp_id=143 (last visited 20 November 2008).

Information security awareness in financial organisations

ISBN: 978-92-9204-017-8

Catalogue number: TP-80-08-395-EN-N

TP-80-08-395-EN-N

enisa

European Network
and Information
Security Agency

ISBN 978-92-9204-017-8

PO Box 1309, 71001 Heraklion, Greece, Tel: +30 2810 391 280
www.enisa.europa.eu