Obtaining support and funding from senior management

While planning an awareness initiative

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:

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

Obtaining support and funding from senior management

While planning an awareness initiative

September 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 "Obtaining support and funding from senior management while planning an awareness initiative". This VWG and its members are part of the ENISA Awareness Raising Community.

ENISA wish to acknowledge the efforts of Erik Heidt and Lucas Cardholm, whose initial support and co-operation have influenced some prevailing aspects of this project, the members of the VWG and their organisations, Brian Honan of BH Consulting, Colette Hanley of Betfair Ltd., Erik Heidt, Gary Hinson of IsecT Ltd., Kate Dodds of SAI Global, Lucas Cardholm of Ernst & Young, Paula Davis of SAI Global, Rebecca Herold of Rebecca Herold & Associates, LLC, Robert West of Echelon One, LLC, Stefan Karlsson of Volvo IT, who provided valuable inputs, material and prompt support for the compilation of the paper. A special thank you to Katerina Christaki of ENISA for her suggestions and support and to Shay Uzery of Accenture who provided a case study.

Finally, we would like to acknowledge the individuals who contributed to this document with informal reviews, valuable insights, observations, suggestions, and fixes. While this is undoubtedly not a complete list, this content would be incomplete and incorrect without their help.

Contents

Executive summary

In the digital age in which we live and work today, businesses find information communication technologies (ICTs) invaluable for carrying out their daily tasks. Hence, more and more businesses are at risk of information security breaches. This is due to vulnerabilities in these new and existing technologies, together with convergence, the growing use of "always on" connections and the continuous and exponential user uptake within Member States. Such security breaches may be IT related, such as computer viruses, system failure and data corruption, or they may be socially motivated, for example. theft of equipment. In an age ever more dependent on digital information, there is an increasing number of dangers. A considerable number of end-users are unaware of their exposure to security risks, as recent cases have highlighted.

The security landscape is an ever changing one. Having an organisational security policy does not in itself drastically reduce the proliferation of security breaches. Most analysts report that the human component of any information security framework is the weakest link. In this case, only a significant change in user perception or organisational culture can effectively reduce the number of information security breaches. ENISA recognises that awareness of the risks and the available safeguards is the first line of defence for the security of information systems and networks.

Information security is not only a technical issue but a business and governance challenge that requires the involvement of senior management and executives to assess how to react to emerging threats. The priority given by senior management to awareness initiatives has an impact on the extent to which these programmes will be successful. It is therefore crucial to gain management support and sponsorship for information security awareness initiatives, although this is often the most neglected aspect of an awareness initiative.

This paper points out the obstacles and challenges that often arise when trying to obtain support and funding from senior management and provides practical advice on how to overcome these issues during the planning and implementation phases of an information security programme. In particular, the document emphasises the importance of considering and assessing information security awareness initiatives in the context of corporate investments. To this end, five major areas were identified.

The definition of the investment rationale and stakeholders for the security awareness investment is recognised as critical to any programme's success. The investment process starts when the security manager has documented the identified need for risk mitigation. The main rationale for these needs varies, and will determine which methods to use to perform a useful cost benefit analysis. The security manager needs to address the correct stakeholders in order to avoid lack of investment or commitment where needed, as the stakeholders are often both formal investment decision makers and other indirect influencers.

The second area relates to building a persuasive business case which forms the foundation of a successful awareness initiative. A business case significantly improves the odds of successful project funding, since it helps senior management to better understand the value of the investment and decide whether to fund it or not. Furthermore, it generates stakeholder commitment, not just support, based on its credibility. With a strong business case the awareness initiative will also stand a good chance of staying focused on the targeted benefits.

The third area is the estimation of programme costs which allows organisations to identify the most common expenses they may incur and their rough estimates. This helps the readers by providing an example of programme costs which are used as a standard and which may be used as a benchmark for comparison against industry.

The fourth area is the provision of business benefits linked to an information security initiative. The document describes how to define and calculate performance metrics and the different types of calculations involved.

The fifth area, probably the most important and helpful for the readers, details a typical way of approaching a corporate executive. Effective communication is critical to an information security awareness initiative's success: the information needed should be delivered at the right time, in the right manner.

In addition, the paper provides examples and case studies from other organisations dealing with different awareness matters, to enable readers to identify key problems, issues and solutions, making the main outlines of the document more effective and concrete. This engages the readers and enriches their learning experience. Furthermore, it makes recommendations for overcoming obstacles within their organisations.

ENISA hopes that this document will provide a valuable tool to help private organisations' staff and decision-makers prepare and implement awareness initiatives.

PART 1: INFORMATION SECURITY GOVERNANCE AND THE INVESTMENT APPROVAL PROCESS

Introduction

Today organisations face an increased need to guarantee the integrity and confidentiality of information. Until recently, security has primarily been focused on protecting the information systems that process and store information, rather than on the information itself. This change is a necessity given the new business scenario. The UK Department for Business, Enterprise and Regulatory Reform (BERR) reported in their Information Security Breaches Survey 2008 that 77 % of UK businesses spent information security budget on protecting customer information and 72 % for maintaining information integrity ([1]).

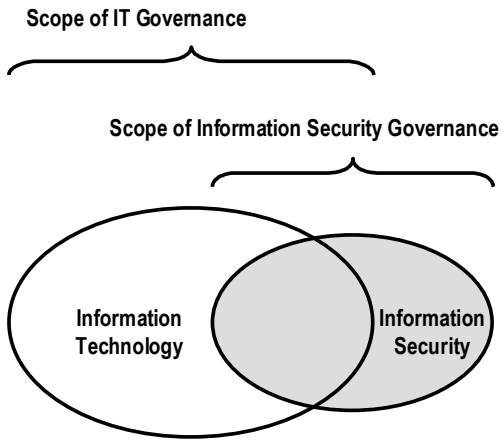


Figure 1: *IT governance*.

Information security is not only a technical issue, but also a business and governance challenge, the success of which hinges upon employee understanding of the importance of information security. Senior management and executives must be involved and clearly support, emphasise and model the appropriate ways in which information security must be addressed to handle current and emerging threats. The Information Technology Governance Institute (ITGI) states "Information security governance is a subset of enterprise governance that provides strategic direction, ensures that objectives are achieved, manages risks appropriately, uses organisational resources responsibly, and monitors the success or failure of the enterprise security programme […]" ([2]). Successful information security governance depends upon employee understanding and involvement.

Executive management and boards are increasingly looking for an information security governance framework that encompasses information technology and information security: a single framework through which all information assets and activities within the organisation can be governed, to provide the optimum capability for meeting the organisation's objectives, in terms of functionality and security. Information security governance is built into ITGI's model for IT governance, as shown in Figure 1 ([3]).

Having a security policy alone does not drastically reduce the proliferation of security breaches; policies must be supported with corresponding procedures and employee action. To accomplish effective action, organisations need to take some steps to raise information security awareness amongst staff as security depends not only on effective technology but also on informed and educated staff. Awareness initiatives ([4]) should be seen not simply as a means of allowing

([1]) BERR, *2008 Information Security Breaches Survey*, 2008, available at http://www.security-survey.gov.uk (last visited on 22 July 2008)
([2]) IT Governance Institute, *Information Security Governance: Guidance for Boards of Directors and Executive Management,* 2nd edition, USA, 2006; Corporate Governance Task Force, *Information Security Governance: Call to Action*, USA, 2004.
([3]) Poole, Vernon, *Why Information Security Governance Is Critical to Wider Corporate Governance Demands—A European Perspective*, available at http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=30681&TEMPLATE=/ContentManagement/ContentDisplay.cfm (last visited on 28 July 2008)
([4]) Within the paper, we refer to awareness initiative and programme indistinctly.

employees to recognise information security concerns and respond accordingly but also of incorporating information safeguards into their day-to-day job ([5]).

The priority given by senior management to information security awareness initiatives has a direct impact on the extent to which these initiatives will be successful. It is therefore crucial to gain management support and sponsorship for information security awareness programmes, this being the most fundamental aspect of an entire information security awareness initiative. It is vital to build consensus amongst corporate decision-makers that awareness programmes are important and worthy of funding. This is where the concept of stakeholder management comes into play. Depending on the organisation, there may or may not be a need to make a solid financial case for the investment. This is why information security governance, internal controls principles and communication need to be addressed while planning information security initiatives ([6]). If the key stakeholders do not understand the imperative of an information security awareness initiative, they will be unable to support its objectives and goals, and the initiative will not be successful.

Purpose

ENISA recognises that gaining senior management support and sponsorship for information security awareness programmes is crucial. This white paper aims to provide an introduction to the importance of gaining support and funding. It also aims to provide valuable tips on subsequently gaining the required support as well as taking the first steps towards the preparation and implementation of an information security awareness initiative.

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

- ✓ Information security governance and the investment approval process.
- ✓ Practical advice: recommendations, guidelines on how to approach senior management, case studies provided by a number of private organisations, tools and models.

Objectives

The objectives of this publication are for ENISA to:

- ✓ Illustrate a sample strategy for obtaining support and funding from senior management while planning and running an information security initiative.
- ✓ Highlight potential challenges and risks associated with the funding and support of information security awareness initiatives in an effort to avoid such issues in future programmes.
- ✓ Provide a communication framework to better champion an awareness initiative.
- ✓ Present case study 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 private organisations, when conducting information security awareness raising programmes. It also seeks to raise awareness among senior management of the importance and criticality of endorsing information security awareness within their organisation.

([5]) 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).

([6]) 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

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 "Obtaining support and funding from senior management while planning an awareness initiative", ENISA staff as well as through information that is publicly available or has been supplied to ENISA by appropriate organisations.

Obtaining support and funding from senior management while planning an awareness initiative

The need for information security awareness

Information is a fundamental asset for any organisation. Information security is therefore critically important to protect data against a wide variety of threats, such as unauthorized disclosure, data errors or loss of information, to guarantee its confidentiality, integrity and availability. There are unlimited reasons for these, such as data entry errors, computer viruses, hackers, technical problems, disasters, fraud and many others.

While most organisations previously have invested in information security technologies such as antivirus software and firewalls, significant information security risks remain as a result of the accidental or deliberate actions and inactions of people. As a consequence, the trend for information security investments is moving toward business objective alignment through increased management and employee awareness, and not just new technologies. Research by Ernst & Young shows that there is a significant decrease in the deployment of new technologies in organisations (30 % in 2006 to 14 % in 2007) compared with ensuring business alignment of the information security department plans ([7]).

Employees generally comply with information security policies, standards, laws and other regulations. However being only human, they occasionally forget the basics and make mistakes, such as sharing passwords with colleagues or neglecting to take regular backups. Some employees let visitors roam about the office unescorted, give out sensitive information over the telephone or lose corporate laptops containing sensitive information. These are not merely theoretical examples but typical everyday occurrences ([8]). Employees are also increasingly being exploited through methods such as social engineering to divulge sensitive corporate information.

The cost of information loss due to human error is significant. An analysis of the reasons for information loss conducted by the Pepperdine University put human error at 29 %, as the second most common cause, second only to hardware failure at 40 %. As a comparison, software corruption and computer viruses amount together to 19 % of information loss ([9]).

In short, we ignore the human aspects of information security at our peril.

([7]) Ernst & Young, *Global Information Security Survey*, 2007, available at http://ey.com/ (last visited on 28 July 2008).
([8]) Noticebored , *Business case for an Information Security Awareness Program*, 2008, available at http://www.noticebored.com/NB_generic_business_case_for_infosec_awareness_program.pdf (last visited on 22 July 2008).
([9]) Pepperdine University, *The Cost of Lost Data: The Importance of Investing in that "ounce of prevention"* , Graziado Business Report 2003, volume 6, issue 3, available at http://gbr.pepperdine.edu/033/dataloss.html (last visited on 28 July 2008).

Aims of the security awareness initiative

An information security awareness initiative is an appropriate means of addressing this recognised control issue. Although the security risks caused by the human factor cannot be fully eliminated, increasing awareness of information security and its purpose will spread knowledge and thereby increase understanding of information security concepts and objectives. Widespread understanding will increase the extent of employee support of and commitment to the rules and motivate them to improve security.

Figure 2: ***Logical sequence of events.***

Security awareness improvements will both increase compliance and reduce risks, making security breaches less likely or less costly, in other words creating genuine bottom-line business benefits.

The logical sequence of events presented by NoticeBored.com (shown in Figure 2) makes the point that raising awareness of security is not an end in itself but an important step on the way to the ultimate business objective, whether that be cost–reduction, growth or profitability ([10]).

Obtaining support and funding from senior management

An information security programme will face many challenges if senior management does not actively support the initiative ([11]). Not only must senior management provide financial support to effectively develop the programme, but they must also provide visible support to demonstrate to the workforce the importance and necessity of information security efforts. Information security, privacy and compliance practitioners must obtain the support of senior management to be successful. This section describes the necessary steps, time-related actions and dependencies to do so.

Telecommunications provider – senior management commitment

A medium-sized telecommunications provider explained why information security is important to their business. One challenge they face is to engage senior management - with a pretty good understanding of security issues - in any awareness initiative. Senior management gives a very low priority to security and takes measures which are reactive, for example in response to a data loss incident.

A particularly successful way to overcome this issue has been the use of financial analysis to have the senior management better assess the information security awareness investment. It is important as well that the management is not solely funding the initiative but is also supporting it along the way.

Create a clear education strategy

First create a documented information security education strategy that includes your objectives for awareness and eventually training. Awareness is the "what" component of any education strategy which tries to change the behaviour and practice of its targeted audience and it is a distinct element from training. Training is the "how"

([10]) Noticebored, *Business case for an Information Security Awareness Program*, 2008, available at http://www.noticebored.com/NB_generic_business_case_for_infosec_awareness_program.pdf (last visited on 22 July 2008).
([11]) This section has been mainly based on Chapter 8 of the book by Herold, Rebecca, *Managing an Information Security and Privacy Awareness and Training Program,* Boca Raton: Auerbach, USA, 2005.

component to implement security. Awareness programmes start with awareness, build eventually to training, and evolve into education ([12]).

Within an education strategy be sure to include estimates for necessary personnel, materials, time schedules, and any other associated costs, such as videos, manuals, training content, training facilities, and so on.

A big mistake that many information security practitioners make is that they ask for resources for their awareness efforts, but then do not provide any solid numbers or documented activities to support why they need the resources. Most managers will, understandably, not give a blank cheque to you just because you say you need the resources, which certainly is a reasonable thing for a good leader to do. So you must plan, document and be specific about the activities that you want to carry out for awareness, along with the accompanying resources, and also provide justification for why such activities will benefit your business.

Ask senior management to provide funds to support the organisation's awareness compliance requirements. Make sure they understand that this will also demonstrate a standard of due care for your organisation. Obtaining this visible support of senior management is critical; if employees do not perceive that there is strong support from senior management for the awareness activities, it is likely you will encounter passive resistance from a significant percentage of personnel. They may not attend training for which they were scheduled, may ignore your requests to read and acknowledge policies and procedures, may ignore awareness activities, or may blatantly violate your policies and procedures. It is important to prevent this by having senior management clearly communicate the importance of everyone's participation prior to your awareness rollout.

You will find some senior management who already believe that information security education is an important endeavour and will be readily willing to financially support training efforts. However, it is likely that a larger proportion will mistakenly believe that such efforts should not take much, if any, budget and that personnel should learn about security and privacy issues as an effect of performing their job responsibilities. It is crucial to the success of your awareness initiative to first and foremost convince your senior management that information security is valuable and an essential part of doing successful business. Get senior management support through a strong and effective executive briefing.

The senior management briefing

Once you get your information security awareness strategy thoroughly documented, schedule a briefing with senior management well ahead of your initially planned awareness deliveries. A good rule of thumb is getting their support 6 to 12 months ahead of time. Use this briefing meeting to provide justification for the education, communicate your goals, and ask for their visible support.

Here are few high-level pointers for the briefing meeting:

- ✓ Keep it simple and succinct. Too many employees include insignificant details that senior management does not need, or want to know, such as your experiences with

([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

choosing a particular vendor, or the troubles you had, or could have, getting a room booked. Get to the point!

- ✓ Keep it non-technical. Don't talk about bits, bytes, internet protocol (IP) addresses or learning management systems (LMS) technical specifications. Express any issues related to storage and networking in words that the average, non-IT, person can understand.
- ✓ Use a peer-led roundtable discussion format. Get feedback and allow for plenty of questions. You need to get buy-in to be successful, and discussion meeting formats allow participants to obtain a sense of ownership for various aspects of the decisions you make based upon your meeting with them.
- ✓ Demonstrate value. Show how awareness activities will benefit the business. Relate these activities to improving your organisation's brand value. Give examples of organisations that use information security to improve their image.
- ✓ Discuss budget needs and strategy. Be clear about the resources you need, and why you need them. Break your resource needs down into categories, and don't ask for just one lump sum. Business leaders need to know specific details about budgets if you want them to approve your resource requests.
- ✓ Focus on senior management responsibilities. For example, when speaking to the Chief Information Officer (CIO), speak about business aspects of information and how it impacts the network. Or, when speaking to the Chief Financial Officer (CFO), describe the costs involved with breaches and incidents, and how much other organisations have lost as a result of them.
- ✓ Ask for sponsorship and support before leaving the meeting. To help emphasise the importance of an information security awareness initiative, and to persuade executive management to invest in and visibly support the programme efforts, make the following points when communicating to senior management to get their support:
  - Explain how an information security incident could potentially impact business.
  - Emphasise legal and regulatory requirements for education.
  - Explain how training helps retain employees. It is a common misconception that training personnel will cause them to leave and use the acquired knowledge at another organisation. This may be the case for a few employees. However, studies show that personnel who receive what they feel is adequate training and awareness to carry out their jobs to the best of their abilities are more likely to be satisfied with their employer and stay with the organisation.

  - Find an executive who will be an advocate for your education efforts and promote them to the other senior management. This ally should be able to speak positively about education efforts and needs in communications and conversations with the other senior management when you are not around and should keep the issue alive and top of mind.
  - When describing your awareness programme, clearly show how it reflects and supports the business goals and needs. You must be able to describe succinctly and clearly the benefits of your initiative. This means you must know and understand the current state of information security education, areas where weaknesses exist, and how to address these weaknesses. Furthermore, you will need to demonstrate and describe how the awareness programme will support the needs of all job functions.
  - Know how much funding to ask for and justify the amount you are requesting. If you know you will not be able to get the maximum, start by asking what you know is realistic. Do your best to make these initial activities successful and use these successes to ask for more support and resources. Senior management are more likely to support and dedicate

resources to your awareness programme if you have shown, even in a small way, that you can be, and have been, successful. See the section later in this report for more information about budgeting and funding.

- Anticipate senior management's objections prior to your meeting. Speak with others who have tried to do similar or parallel initiatives. What are the issues and problems that may be presented? What do the senior management like or not like in awareness programmes? Have the senior management had bad experiences with similar initiatives in the past? Use the answers and develop information in your presentation that will address these challenges.
- Always include, when possible and feasible, the management's ideas in your programme. They will take more ownership in the programme, and they will, of course, think the programme is even better.
- Some senior management like to be given alternatives. Present what you want, plus, perhaps, a scaled-down less expensive but adequate alternative, and let the executive choose. Even if you win the scaled down alternative, it is much better than what you had before the meeting. Also, the executive may be willing to spend more money after the initiative is successful.

Education strategy components

Demonstrate the importance of information security to senior management in your organisation. Business leaders relate to economic impact and how business can be affected. When seeking to get sponsorship, develop and present a documented strategy to your executive management that they can immediately relate to from a business perspective.

Consider including the following components, if they are applicable to your organisation, within the paper. You can also discuss them during your executive briefing if it will support your requests or answer any questions the senior management have.

Education strategy roles

Within your documented strategy, and during your executive briefing, clearly communicate and provide documentation for the roles you will need to successfully implement your strategy. There will be different roles for different organisations based on size, industry, location, regulatory requirements and so on. However, some of these roles that are in addition to the information security manager roles will include:

Roles	Responsible for
Business unit (BU) security and privacy managers	• Designing the BU deployment strategy. • Defining and documenting the associated organisation regional–country–business unit deployment model. • Being content specialisation resources.
Security and privacy advocates	• Forming the communication and implementation link between the corporate security and privacy offices and the field employees. • Being the first point of contact for BU personnel security and privacy questions and advice. • Ensuring personnel awareness and training activities occur.
Regional security and privacy managers	• Deploying core and functional, targeted training. • Communicating security and privacy issues for their region. • Being content experts on legal, regulatory, and country–specific issues.

Roles	Responsible for
Workforce management	• Visibly and actively supporting security and privacy awareness and training activities. • Ensuring staff participation in security and privacy education activities.
Executive security and privacy champions	• Providing local executive sponsorship for their business unit. • Promoting and supporting security and privacy implementation strategy. • Supporting the security and privacy advocates' network.

Awareness programme success indicators

It is common for senior management to ask which success indicators will be used for your awareness initiative before they give their support and funding. Think carefully about this as it relates to your organisation and be ready to list what you define as your organisation's information security awareness programme success indicators ([13]). A complete description of how to measure the value of an awareness initiative and a set of example are available in the section "Identifying opportunities to document and measure the value of the awareness campaign".

Provide examples of information security impacting events

Addressing information security concerns, implementing enterprise security, and ensuring compliance to applicable security and privacy laws are significant to achieving uninterrupted business processing, demonstrating due diligence, and minimising risks due to non-compliance. If unprepared, an information security breach could result in significant business downtime and monetary loss, negatively impact an organisation's reputation, generate legal fines and penalties, and possibly result in costly civil suits, and negatively impact customer satisfaction and loyalty.

According to the Ponemon Institute - Vontu research study, in 2007 each compromised customer record cost a company $197, mostly from lost business. Most companies have had hundreds of thousands, and sometimes millions, of customer records breached. So, taking a conservative number and using the study results, if the company had a computer containing 100,000 customer records breached, it would cost the company around $1,970,000 in lost business, fines, penalties and other associated costs.

Include within your senior management briefing examples of some recent internal incidents or attacks, and incidents that have occurred in other organisations, particularly those in your industry. The following are just a few examples of security- and privacy-impacting events that have recently occurred:

- ✓ In August, 2008, the Royal Bank of Scotland reported that a computer belonging to archiving company Graphic Data and sold "inappropriately to a third party" had information on credit card applications from as many as over 1 million RBS customers and data from other banks. The computer contained account numbers, passwords, mobile telephone numbers and signatures. A former employee of Graphic Data sold a computer server used by RBS on eBay without wiping the internal hard drive.
- ✓ On April 22, 2008, U.K. Information Commissioner Richard Thomas delivered a speech at the Infosecurity Europe 2008 conference and indicated that leaders of public sector and private organisations must ramp up efforts to protect customer data because of growing numbers of

([13]) For more details see 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

incidents within the U.K. Since the U.K.'s tax authority lost the personal data of 25 million individuals in late 2007, the Information Commissioner's Office (ICO) has been notified of almost 100 data breaches; 66 in the public sector, 30 % in the private sector, and 4 % in an undisclosed sector.

- ✓ On August 11, 2008, Ireland's Department of Social and Family Affairs began notifying 380,000 social welfare customers whose unencrypted personal information was on a government audit agency's laptop that was stolen in early April 2007. The unencrypted information included records of welfare payments made in January 2005 and April 2005 for a wide range of social benefits, mostly state pensions but also information on single parent family payments, widows' non-contributory pensions, and orphans' contributory pensions.

Demonstrate how information security incidents are increasing

Do a little research and dig up statistics to support the need to have an effective information security awareness programme. Especially effective are statistics that show the trend for information security incidents is continuing to rise. A few good sites that provide such statistics include:

Web site	Address
Open Security Foundation	http://opensecurityfoundation.org/
OSF Data Loss Database	http://datalossdb.org/
Pogo Was Right	http://www.pogowasright.org
Educational Security Incidents (ESI) Year in Review	http://www.adamdodge.com/esi/year_review_2007
Privacy Rights Clearinghouse	http://www.privacyrights.org/ar/ChronDataBreaches.htm
Anti Phishing Working Group	http://www.apwg.org/
FTC News Releases	http://www.ftc.gov/opa/
US CERT Incident Trends	http://www.us-cert.gov/reading_room/#news

Demonstrate how information security is a core business issue

As awareness of information security and related issues grows, organisations must treat information security as a core business issue or find themselves at a disadvantage in the marketplace. Customers are increasingly inclined to seek to do business with organisations they trust and that can give them control over their personal information. Information security is becoming essential to maintain a competitive edge, profitability, legal compliance, commercial image, and to meet a standard of due care.

Businesses, including your organisation's competitors, are becoming acutely aware of the trend to address privacy and use privacy assurances as a differentiator for keeping and obtaining new customers.

Communicate the increasing information security threats and breaches

Increasingly, organisations and their information systems and networks face information security threats from a wide range of events and sources such as identity theft, mistakes, lack of knowledge, inappropriate business practices, computer-assisted fraud, network attacks, sabotage, vandalism, and fire or flood, to name a few. Security risks such as email schemes, phishing, social engineering, identity theft, fraud, and so on, have become more common, more ambitious, and increasingly sophisticated. Additionally, the number of security and privacy–related laws and regulations continues to proliferate at exponential rates throughout the world.

Dependence on information systems, application services, and employee knowledge of risk means that organisations are more vulnerable to information security threats. The interconnecting of public and private networks throughout the world, the trend to use distributed computing, connections to business partners and third parties, and sharing of information resources increase the difficulty of achieving adequate and acceptable information protection and access control.

A position should exist to ensure that the appropriate and applicable personnel get the information they need to comply with the laws. Organisations have been significantly impacted by security and privacy breaches. See the links provided above for some possible resources that you can use to find statistics and events to support your case to senior management.

The financial impact of security on business

An information security breach could significantly impact your organisation's business as it has impacted growing numbers of organisations. A breach could potentially cost hundreds of thousands to millions of dollars in human resources, communications, and materials expenses in addition to negative publicity, lost business, and legal counsel costs. Give your senior management an indication of how it could affect your organisation financially by providing a scenario showing the impact of an incident ([14]).

Communicate leading practices to senior management

What are you doing to address the impact that information security issues could have on your organisation? Do they correspond with leading practices? Your decision-making senior management will want to know the specifics to determine how much budget to assign to information security efforts. The following are steps organisations are increasingly taking to help ensure an effective information security awareness programme and to help demonstrate due diligence and align with leading practices:

- ✓ Provide on-going, visible security and privacy support, commitment, and participation from senior management.
- ✓ Implement information security policies, standards, procedures, objectives, and activities that reflect business goals and mission.
- ✓ Diligently stay aware of new and updated security and privacy– related laws and regulations applicable to the organisation.
- ✓ Develop and implement procedures addressing information security that are consistent with the organisational culture and support security and privacy policies and legal requirements.
- ✓ Make employees responsible for possessing a good understanding of information security requirements, risk assessment, and risk management.

([14]) See an abbreviated version of Rebecca Herold's privacy breach impact calculator at http://www.informationshield.com/privacybreachcalc.html. Input values into the fields that would represent your business situation to see the resulting financial impact to your organisation.

- ✓ Effectively market and communicate security issues and requirements to all managers, personnel, and business partners.
- ✓ Distribute, on an on-going basis, communications and guidance about information security issues to raise awareness for all personnel and third-party partners.
- ✓ Provide on-going, appropriately targeted security training and education.
- ✓ Use a comprehensive and balanced system of measurement to evaluate performance in information security management and compliance.

All personnel in the enterprise must be aware

Every individual within the organisation, from senior management down to junior staff, must consider information security as an integral part of the business, and not as an afterthought.

International energy and oil company – Employing best practice and methodology in the planning of an information security awareness programme

An international energy and oil company recognised the importance of raising the awareness of its staff to Information Security and compliance topics, and of providing continuous education to its Information Security staff on topics that are part of their roles and responsibilities.

Until then, the company was operating on an ad-hoc basis and did not have insight on the specific areas in which awareness and training were required. In addition, it did not have a process in place to regularly assess the requirements for those activities.

The senior management of the company recognised the importance of raising information security awareness of its staff and decided to contract a consultancy firm for supporting them while setting up an Information Security awareness programme.

As part of the methodology a complete planning process for requirements gathering, measuring the impact of activities provided, communicating the plans, and executing them was also provided.

The last recommendation was to collaborate with other businesses in order to learn from the experience of others and leverage activities developed by them.

The organisation's senior management decided to adopt them as suggested.

Taking security precautions is more than important; it is an essential and inevitable component of business success. Serious consequences to an organisation's goals and business success can result from inadequately and not continually addressing these risks. Following a well-thought-out security assurance and governance programme that includes effective on-going awareness will help an organisation successfully and effectively mitigate information security risks.

Effectively communicating the initiative to personnel, with the clearly visible support of executive management, is key to the success of your awareness programme.

Information security governance and internal controls principles

Information security projects, as with most projects, can be separated into two broad categories to meet the main value disciplines of the organisation. The first category consists of initiatives that strive to provide a new or enhanced service. The second kind of effort is not primarily concerned with providing the organisation with new functionality or services, but is focused on improving effectiveness, efficiency, or quality, usually through a process improvement or increased automation. In other words, these security initiatives support the organisation in using its resources and assets efficiently.

Awareness efforts associated with the second class of projects are not our focus here. The communications goals of such projects are to educate people about the business value of the project (for example the improved efficiency, improved quality of service, improved effectiveness). Communication planning of this nature is covered quite well in available project management literature. Instead, it is the first class of projects that is our primary focus in this white paper; awareness of information security threats and vulnerabilities may be the only effective control that is available, due to the dependency on human behaviour.

#	Questions
1	What kind of information security or risk management project is this?
2	What are the risk management objectives?
4	What controls are in place to support the risk management objectives?
4	How can information security awareness support those control objectives?
5	Are there other awareness and communications programmes in my organisation that would be willing to help "get the word out"?

Information security risk management and awareness

As mentioned previously, there are many information security threats to organisations ranging from computer system failures to human error, abuse and fraud. In information security and IT audit literature, control measures are used to mitigate these risks. These controls are a combination of people, processes and technology that are used to prevent, detect or correct issues caused by unwanted events.

Preventative controls

The objective of preventative controls is to manage an information security threat by pre-empting a mistake, an attack or exploit. Examples include:

- ✓ Badge scanners controlling physical access.
- ✓ Requiring user to logon prior to accessing services.
- ✓ Firewalls restricting ports/services.
- ✓ Written approval by superior required.
- ✓ Automated data input checks in computer systems.

The critical role that information security awareness plays in preventative controls is ensuring that the purpose and value of the control is well understood, responsibilities for implementing and enforcing the controls are established and understood, and that consequences of circumventing the control are also clearly understood.

All of these controls can be circumvented if not

properly managed and supervised. Badge Scanners are of limited value if "tailgating" is a common practice, or if doors are not otherwise properly secured. If users share logins and passwords rather than request individual authorised access, then network access controls fail and accountability is lost. Firewall configurations and input data controls cannot be properly managed unless their administrators understand how to evaluate change requests, enforce policy or properly escalate when required.

Detective controls

The objective of detective controls is to identify when a breach, attack, or violation may be occurring (or may have occurred), or a vulnerability has been exploited. Examples include:

- ✓ Physical intrusion detection.
- ✓ Log reviews.
- ✓ Approvals by superiors are reviewed.
- ✓ Doors that should be locked are also checked by a guard.

Awareness can sometimes be even more crucial to the functioning of detective controls than it is for preventative controls. It is people's awareness and sensitivity to the potential loss (from attack, breach, violation and so on) that generates a sense of commitment, urgency and importance in the careful execution of the investigation and responses that result from detective controls.

Detective controls are usually dependent on people for evaluation and response. For example, if alarms go off and are reset but not investigated, then they are of little value. To take another example, if guards and physical security staff do not know how to recognise and respond to problems, then their value is diminished. As yet another example, if log files or formal approvals are not reviewed in a timely fashion or with sufficient attention to detail, then their value is questionable and no valuable trend analysis can be undertaken.

Corrective controls

In the information security context corrective controls generally involve either triggering the organisation's Incident Response plan or behaviour modification for involved parties, aiming at restoring the situation to its expected state and preventing similar incidents from recurring.

When detective controls indicate a pattern to a problem, it allows the organisation to consider deploying new preventative, detective or corrective controls. As a rule of thumb, preventative controls are often more cost-efficient than corrective controls as they actually prevent events from occurring while corrective controls may be used over and over again.

When detective controls indicate a pattern to a problem, it may result in the trigger of broad awareness campaigns. For example, if detective controls indicate that security policies are being disregarded leading to increased costs due to spend on non-productive time reacting to incidents rather than day-to-day for the organisation, a communications campaign discussing the value of the security procedures, managements support for them, and the consequences of non-compliance may be a corrective control chosen by an organisation.

Understanding awareness in the context of corporate investment approval processes

The information security investment approval process includes aspects such as:

- ✓ How much to spend.
- ✓ What to spend it on.
- ✓ How to reconcile the needs of different stakeholders.

To be able to properly address these concerns, the investment process needs to be understood from a governance perspective:

- ✓ Who makes investment decisions?
- ✓ How are investment decisions measured in terms of effective management?
- ✓ How will these decisions be captured and monitored in financial terms?

Information Security initiatives provide value to their organisations either through the management of identified risks and reduced incident costs such as increasing profit and enabling growth, or improved governance effectiveness and compliance.

As with any other investment, these value propositions are dependent on assumptions. In the case of risk mitigation the value proposition can be related to the probability, frequency, character, and magnitude of future events (such as threats, attacks, and so on.) and in the case of compliance it could for example be related to employee-time spent on non-productive corrections of information security breaches or to the cost of compliance breaches and associated fines and penalties.

Many security professionals struggle with the fact that costs associated with information security incidents can have large components which are difficult to quantify, such as loss of customer confidence, brand equity impacts and so on. This is not to say that organisations have to make their information security decisions with a complete lack of quantified value. Quite to the contrary, in the manner of any investment request, there are often numerous opportunities to collect data and trend information in order to measure the effectiveness of information security investments, as for any investment request.

Consider the following approach to cover these aspects:

- ✓ Understand the main rationale and identify stakeholders for the security awareness investment.
- ✓ Document the value of the effort to the organisation, using quantitative data whenever possible.
- ✓ Validate that the results are relevant to stakeholders and the strategic goals of the organisation.
- ✓ Develop a plan for how to communicate the value of the awareness investment.

European bank – entering new growth market

A European bank had decided to enter a new growth market. In order to meet local banking regulations, the online banking service was required to have certain controls in place regarding information security awareness.

To meet these requirements for the end-user (customer) community, the bank published educational information on how to identify potential fraud and how to behave 'securely' online as part of the main log-in procedure.

Identifying opportunities to document and measure the value of the awareness campaign

It is frequently difficult for information security programmes to provide "hard numbers" for the value of the initiative, but in the case of information security awareness programmes there may be a number of opportunities. In addition to the methods and ideas discussed in this section, seek out the people in your organisation who are involved with awareness, training, and learning programmes in other areas. You may find these individuals in roles responsible for communications regarding Human Resources policies, new employee orientation, professional development, sales training and employee safety programmes. These efforts may have established expectations in your organisation regarding what awareness and training programme funding requests are expecting to contain in terms of metrics, and general content. Avoid "reinventing the wheel" by partnering with, and leveraging, the experiences of these individuals.

Techniques for quantifying the value of an awareness campaign may include:

- ✓ Impact on a core information security metric.
- ✓ Impact on a knowledge benchmark.
- ✓ Reduction in employee-time spent on corrective controls.
- ✓ Incident avoidance benefits.
- ✓ Incident cost-reductions.

Impact on a core information security metric

If the objectives of the awareness initiative are to affect a core metric that is already tracked in your organisation, then clearly that metric should be leveraged as a portion of the case to senior management. Some examples of metrics such as this could include:

- ✓ Rate of loss of equipment (laptops, backup tapes, and so on).
- ✓ Virus and malware infection rates.
- ✓ Patch and remediation effort times.

If it is not already measured, identify clear metrics accepted by management and measure the before-after effect of the awareness initiative.

Impact on a knowledge benchmark

In adult and organisational learning, surveys are frequently used to assess the impact of awareness and educational activities. Do you have the opportunity to use a survey to clearly identify that a particular security threat, regulation, expected practice and so on is not as well understood as it should be? If this is the case, it provides an opportunity to clearly establish critical success factors and key performance indicators for your information security awareness programme. If you do not have a survey in place you should consider approaching senior management to conduct such a survey as part of the initial information security awareness initiative.

All modern e-learning solutions use this kind of functionality to show improvement in user awareness. There are stand-alone software solutions as well as enterprise-wide server based solutions. The server-based solutions also often have built-in functionality to remind users to perform their awareness training and evaluation until it is completed.

A multinational IT services company – A non financial way of measuring information security awareness

A multinational IT service company decided to use a self assessment test in order to measure how effective their information security e-learning course was. About 40 questions were written about different information security issues covered in the course. It was decided at what score someone should be considered as having passed the test. The questions were sent out to 20 % of all employees, using a random selection. One test was performed six months before launching the training, and then another one was carried out a year later. Finally, a third one was made three years later. From the beginning there was 50/70/90 objective. This means that at the first assessment they aimed for 50% employees to pass the test. The percentage of employees performing the test has always been satisfactory, which has made this method successful for the company.

Less employee-time spent on corrective controls

If employees spend time on corrective controls, you can estimate how much working-time is lost each month resulting from failures of the preventative controls. It is then possible to put the total costs for those hours in relation to the cost for the awareness programme.

With a sample measuring of time spent on corrective controls, or if the organisation is using detailed time-tracking systems, it is also possible to measure the before and after effect of the awareness initiative as illustrated in Figure 3.

Dep.	# employees	Avg. # hrs (per employee) for corrective controls per week	Cost per hrs	Avg. cost per annum
IT	21	6,5	€14	€ 91 728
HR	6	0,5	€11	€ 1 584
Finance (HQ)	12	3,0	€14	€ 24 192
Store A	18	0,2	€9	€ 1 555
Store B	26	0,3	€9	€ 3 370
....	…	…	…	…

Figure 3: ***Personnel costs of corrective control, European manufacturer of industrial products.***

The cost for corrective controls in the IT department may be lowered even if an awareness initiative is aimed solely at other employees. An illustration shown to management will clearly demonstrate the savings that the organisation can realise as a result of increased security awareness.

Incident avoidance benefits

When an awareness programme is targeted at avoiding potential incidents, the security professional making the investment request needs to be specific on what to estimate. It may be valuable to consider:

- ✓ Speaking to business managers with a profit-and-loss (P&L) responsibility in the organisation on how they measure (or estimate) their total costs for incidents per annum.
- ✓ Speaking to security professionals in peer organisations.
- ✓ Reading public research reports on frequency and cost of incidents for your industry, geography or company size.
- ✓ Contacting suppliers and consultants, who often provide reports for free.

The challenge with this aspect of quantifying awareness results is that it is actually avoidance of future potential incidents. If the awareness initiative is successful and incidents are avoided, you could seldom tell that they would have happened without the awareness initiative. Too often the analysis does not specify the specific key targets and strategic goals of the stakeholders that can be influenced along with the corresponding financial levels. There are no reasons not to include discussions about these in the analysis, for instance lack of awareness regarding controls in the revenue recognition process could lead to loss of revenues due to fraud.

Measuring, or estimating the average total cost for incidents per annum, may be valuable in terms of benchmarking your organisation against peers, industry, geography or size.

Incident cost-reductions

When an awareness programme is targeted at reducing the actual frequency or impact of certain types of incidents it is valuable to consider:

- ✓ Cost of business disruption.
- ✓ Cost of time spent responding to the incident.
- ✓ Direct cash spent responding to the incident.
- ✓ Direct financial cost of incident, such as loss of assets, fines and so on.
- ✓ Estimated cost of damage to reputation.
- ✓ Negative impact of brand value.

The most effective metric is to measure the before and after effect on actual costs for incidents. If that is not possible it can be useful to work with the tools of incident avoidance benefits (see above), in terms of benchmarking your organisation against peers, industry, geography or size.

Typically the most useful metric to use to obtain management support for awareness activities is to provide a realistic financial impact model to show what the impact of a security incident would be before an incident actually happens. By showing how much an incident can actually cost, based upon valid business cost variables, you can effectively show that the cost of prevention is considerably less than what the cost of just one incident could be. There are several ways that this can be done using costs areas to which your non-IT business leaders can best relate. An example of a tool that can perform such financial modelling is the Privacy Breach Impact Calculator ([15]).

Another useful option is to work with the tools that demonstrate the value of incident avoidance benefits, such as those shown in Figure 3, in terms of benchmarking your organisation against peers, industry, geography or size.

Main activities

Define investment rationale and stakeholders

The investment process starts when the security manager has an identified need for risk mitigation. The main rationale for these needs varies and determines what methods to use to perform a useful cost benefit analysis. Some of the most common driving forces that create the main rationale for an information security awareness investment are:

- ✓ That someone (from within or outside the organisation) identifies risks or gaps in the current control environment that need to be addressed, for example employee awareness of threats such as social engineering, fraud, and so on.
- ✓ Provision of security controls needed by a business or infrastructure program, for example security awareness training for users of a new product.
- ✓ Provision of a business enabler, such as security awareness programmes for customers to the organisation.
- ✓ To comply with the growing numbers of laws, regulations and industry standards that require information security training and awareness components to be part of a comprehensive information security initiative.

([15]) Herold, Rebecca, *The Privacy Management Toolkit*, Information Shield, Huston, TX, 2006.

Figure 4 provides a quick reference list of some of the business rationales for investing in information security awareness, and some of the corresponding business leader questions that must be answered.

Main business rationale	Key questions to address
Mitigate risk in current control environment	✓ What business values are at stake? ✓ Who decides which risk level should apply?
Business-driven investment require security measures	✓ What are the targets for the business-driven investment? ✓ Who decides which risk level should apply?
Opportunity for business improvement	✓ What types of improvement effects are anticipated (asset utilisation, profitability or growth)? ✓ Who decides which risk level should apply?

Figure 4: ***The business rationale for information security awareness.***

The core question is: "Why should we, as an organisation, invest in this awareness raising effort?" The most important aspect of this is being able to clearly articulate answers to the following questions:

- ✓ What is the precise effort in question?
- ✓ Who in the organisation will be affected by this effort?
- ✓ Who do we need support and participation from?
- ✓ What is the value of that effort to the organisation?
- ✓ How are we going to substantiate or measure that value?

These questions are not only presented in the sequence by which they will naturally be discussed, but they are also in the order of importance. This is because each builds on its predecessor such that if the former is not precisely defined then the next cannot be addressed effectively.

The security manager needs to address the correct stakeholders in order to avoid lack of investment or lack of commitment where they are needed. This is because these stakeholders are often both formal investment decision makers and indirect influencers. The following questions should be considered:

- ✓ Who will make the formal investment decision?
- ✓ Who will fund the investment?
- ✓ Which other stakeholders could have an impact on the decision?
- ✓ What are the key targets and strategic goals for these stakeholders?

Develop the business case

The investment proposal will encourage management to allocate sufficient resources to deliver the awareness programme. The business case lays out the business rationale for the awareness initiative together with a reasonable assessment of the projected costs and benefits related to it.

Building a persuasive business case forms the foundation of a successful awareness initiative. A business case significantly improves the odds of successful project funding since it helps senior management to better understand the value of the investment and decide whether to fund it or not. Furthermore, it generates stakeholder commitment and not just support based on its credibility.

With a strong business case the awareness initiative will also stand a good chance of staying focused on the targeted benefits ([16]).

Programme costs

The programme costs need to be assessed in order to fund the initiative. The costs will vary greatly from one organisation to another depending on their structure, availability of supporting assets (such as e-learning systems), previous projects and so forth. Nevertheless, Figure 5 summaries some of the most common cost elements for Information security awareness initiatives, including illustrative cost-estimations based on actual figures given from an airline corporation ([17]):

Cost	Description		€ Estimate
Personnel	Personnel working on the information security awareness initiative. Whether they are full or part-time depends largely on the size of the organisation and the importance of information security relative to other priorities.		60 000
Operational Costs	The operational costs include rent, website maintenance – extranet and intranet -, information security awareness materials – posters, briefing papers, office miscellaneous costs.		25 000
Advertisement and Promotion	Branded coasters, pens, prizes for information security tests, quizzes and competitions, coffee for brown-bag meetings and so on.	Promo material cost	2 000
		Promo distribution cost	
		Advertisement creative cost	
		Advertisement media cost	
Training	In the event an organisation organises awareness training sessions.	Individual materials cost	
		Training rooms cost per session	100
Contingency	Further funds may be needed to purchase additional security awareness materials, external training courses and so on.		20% on total
Total budget request			**TOTAL**

Figure 5: ***Common awareness costs, airline corporation*****.**

When the cost elements of the cost benefit analysis have been identified they need to be put into the proper financial context for the organisation. Remember that if investments in information security are assessed alongside other investment projects, it helps to consider them on an equal footing, implying the use of similar (and ideally the same) methods of financial cost projection.

Even though we have not identified any benefits at this stage, it is possible to perform a TCO calculation (Total Cost of Ownership), should this be relevant to the organisation. The only variables

([16]) 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

([17]) 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; Noticebored, *Business case for an Information Security Awareness Program*, 2008, available at http://www.noticebored.com/NB_generic_business_case_for_infosec_awareness_program.pdf (last visited on 17 July 2008).

to be added are how many training sessions are performed (in this case 20 training sessions were run at a cost of € 100 each) and for how long the awareness initiative will run, used to normalise all investments across an organisation. In this case the time frame was 2 years. The TCO formula would look like this:

$$TCO = \frac{\sum_{t=1}^{t=\text{end of awareness initiative}} \text{one time costs} + \text{recurring costs (t)}}{\text{awareness initiative duration}}$$

Figure 6: ***TCO formula.***

In the case of the Airline Corporation, the results of the TCO formula look like this:

$$TCO = \frac{60000 + 25000 + 2000 + (100 \times 20) + (0{,}2 \times 89000)}{2} = 53400$$

Bank – awareness programme costs

A bank explained that in 2004 they had a year one awareness budget of $200 000 and planned to increase it by 20% per year over a three year period. Costs were relatively low because they had internal developers write an awareness application to test developers' knowledge. Otherwise, the costs for an awareness application to be used across the organisation would be approximately. $500 000. This is in comparison to an annual information security budget of $10 million.

In 1999-2002, the bank had similar numbers although they spent quite a bit in filming an awareness video and printing high-quality materials. They spent $750,000 on printed materials for an awareness booklet for each employee. They decided to stop printing the materials and made them available electronically.

Business benefits

The security manager needs to identify what non-financial metric, or combination of metrics, to use in order to capture the stakeholder values previously identified.

An overview of the many business benefits linked to an information security initiative will help and lead the organisation to reach an informed decision. The following benefits have been identified by the authors:

- ✓ Comply with the three pillars of information security — confidentiality, availability and integrity — and security standards.
- ✓ Defend the organisation from information leakage.
- ✓ Enforce mandatory organisation-wide security policies.
- ✓ Provide both a focal point and a driving force for a range of awareness, training and educational activities relating to information security, a few of which are already in place but are not well coordinated or particularly effective.
- ✓ Communicate and clarify the organisation's overall strategic intent to secure its information resources, both to its employees and externally (information security awareness is an essential requirement for ISO/IEC 27001 certification for example, and is increasingly required for legal and regulatory compliance).
- ✓ Provide general and specific information about security risks and controls to those who need to know it.
- ✓ Make staff, managers and IT professionals aware of their respective responsibilities in

relation to information security.

- ✓ Motivate employees to comply with the organisation's information security policies, procedures, standards and guidelines, and with applicable laws, thereby increasing compliance in practice.
- ✓ Create a strong security culture that is to say a broad understanding of, and demonstrable commitment to, information security right across the organisation.
- ✓ Help improve the utility, consistency and effectiveness of existing information security controls, and where appropriate stimulate the adoption of additional cost-effective controls (and possibly lead to the relaxation of excessive or unnecessary controls).
- ✓ Help reduce the number and extent of information security breaches, reducing costs both directly (for example information damaged by viruses; sensitive information disclosed; compliance failures leading to fines etc.) and indirectly (such as less need to investigate and resolve breaches).
- ✓ Compliance with increasing numbers of laws and regulations that require some form of training and awareness activities.
- ✓ To gain and keep customer and employee trust and satisfaction.
- ✓ To support compliance with the organisation's documented information security policies.
- ✓ To demonstrate due diligence that management is following a standard of due care to ensure adequate protection of corporate assets.
- ✓ To preserve corporate reputation, this is a valuable business asset.
- ✓ To establish accountability for employee activities.

Benefits that are identified but cannot be measured with quantitative values may mean less to senior management. Therefore, when analysing awareness initiatives that improve the internal controls of the organisation, the principles for effective governance defined by the Massachusetts Institute of Technology's Sloan School of Management can be applied. The expected effectiveness of the information security investment can then be assessed by how well it meets four objectives (see Figure 7) weighted by their importance to the organisation ([18]).

Importance of information security investment	
How important are the following outcomes of your information security governance, on a scale from 1 (not important) to 5 (very important)	
Importance	**Outcome**
	Cost-effective use of information security
	Effective use of information security for growth
	Effective use of information security for asset utilisation
	Effective use of information security for business flexibility

Importance of information security investment	
What is the anticipated influence of the proposed information security investment in your business on the following measures of success, on a scale from 1 (not successful) to 5 (very successful)	
Importance	**Outcome**
	Cost-effective use of information security
	Effective use of information security for growth
	Effective use of information security for asset utilisation
	Effective use of information security for business flexibility

Figure 7: ***Management questions for awareness investment*.**

The approach is based on asking the senior management team – the Institute recommends at least ten managers – to answer questions by giving them a score between 1 and 5 in Figure 7. Then take

([18]) Weill, Peter and Jeanne W. Ross, *Governance Arrangements Matrices By Industry,* Harvard Business School Press, Boston (MA), 2004 (II).

an average of the results and look at variation by business units and level of management to meet the stakeholder composition for the investment decision.

The first question assesses the importance of a particular outcome related to information security governance and the second question assesses how well the proposed information security awareness investment contributes to meeting that outcome.

Since not all organisations rank the outcomes with the same importance, the answers to the first question are used to weight the answers to the second question. Then the weighted scores for the four questions are added and divided by the maximum score attainable by that organisation. Therefore, mathematically, information security governance performance =

$$Governance\ effectiveness = \frac{(\sum_{n\ 1\ to\ 4} (\text{importance of information security governance outcome}\{Q1\} \times \text{influence of proposed awareness investment}\{Q2\})) \times 100}{\sum_{n=1\ to\ 4} (5 \times (\text{importance of information security governance outcome}))}$$

Figure 8: ***Information security governance performance.***

Given that there are four objectives, the maximum score for the investment is 100 and the minimum score is 20.

Figure 9 provides an example from a Consumer products manufacturing company of a how to present the relevance of a proposed information security awareness programme from a governance effectiveness perspective. It is suggested that the programme run for 3 months, involving approximately 100 employees working in the financial controlling functions throughout the business units of an organisation in the airline industry. The purpose of the training will be to strengthen the commitment to manual internal controls within the financial reporting processes. The CFO and six other senior managers were interviewed on how this awareness initiative could fit with the corporate agenda.

Importance of information security investment	
How important are the following outcomes of your information security governance, on a scale from 1 (not important) to 5 (very important)	
Importance	**Outcome**
4.2	Cost-effective use of information security
2.2	Effective use of information security for growth
4.6	Effective use of information security for asset utilisation
3.2	Effective use of information security for business flexibility
Importance of information security investment	
What is the anticipated influence of the proposed information security investment in your business on the following measures of success, on a scale from 1 (not successful) to 5 (very successful)	
Importance	**Outcome**
4.0	Cost-effective use of information security
1.1	Effective use of information security for growth
3.5	Effective use of information security for asset utilisation
3.0	Effective use of information security for business flexibility

Figure 9: Example of results from a Consumer products manufacturer.

$$Governance\ effectiveness = \frac{(4{,}2\times 4 + 2{,}2\times 1{,}1 + 4{,}6\times 3{,}5 + 3{,}2\times 3{,}0)\times 100}{5\times(4{,}2+2{,}2+4{,}6+3{,}2)} = 63$$

Figure 10: ***Governance effectiveness.***

To provide value to management, the result of the governance effectiveness assessment needs to be compared in relation with other competing investment requests, or against a baseline where no initiatives with anticipated governance effectiveness below a specified amount such as 50 are accepted.

Calculate performance metrics

The security professional developing the cost benefit analysis should aid management by addressing relevant financial performance metrics of the organisation.

As discussed earlier, information security projects can be separated into two broad categories to meet the main value disciplines of the organisation. The first category consists of initiatives that strive to provide a new or enhanced security service. Efforts in this category are generally targeted at better managing a specific risk or threat to the organisation, thus either improving the profitability of the organisation or enabling growth. The second kind of effort is focused on improving the effectiveness, efficiency, or quality, usually through a process improvement or increased automation. In other words, these security initiatives support the organisation in efficient asset utilisation.

With regards to the financial metrics of a cost benefit analysis, both categories are handled in a similar manner, simply with shifted focus between different types of calculations. Some formulas are clearly focused on one of the value disciplines. For example TCO, Total Cost of Ownership, does not consider profits, while EVA, Economic Value Added, reflects growth by value-add to shareholders only. Despite this, there are no clear-cut lines between the majority of different calculations, as shown in the Figure 11 ([19]).

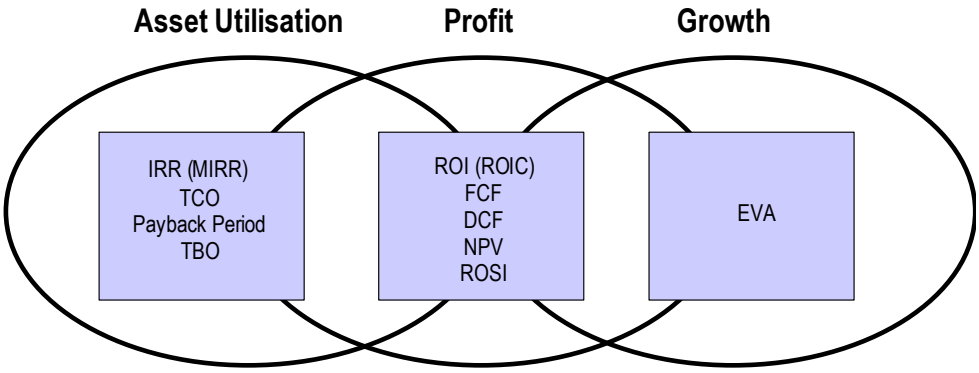


Figure 11: ***Metric relationships.***

These aspects need to be considered not only during the financial calculations, as the use of non-financial metrics helps to identify and quantify key performance indicators and variables used in the financial part of the cost benefit analysis. As a result, the security professional needs to perform the

([19]) Cardholm, Lucas, *Adding value to business performance through cost benefit analyses of information security investments*, University of Gävle, 2007, available at http://urn.kb.se/resolve?urn=urn:nbn:se:hig:diva-238 (last visited on 28 July 2008).

non-financial and financial parts of the cost benefit analysis iteratively to be able to identify and capture value to the stakeholders.

The iterative process of using financial calculations and non-financial metrics is critical to success in this work.

Once the financial metrics have been identified, the actual calculations are seldom challenging to a professional with a financial background.

Figure 12 provides an example from a European headquartered technology company of financial calculations motivating an information security awareness initiative. The programme is planned to run for eight months, involving approximately 2 000 employees at a national retail company with a little more than 100 stores. After the initial round of training, there will be a follow-up period of reminders and additional training sessions where needed. The follow-up activities are called contingency cost in Figure 12. In total, the awareness programme in this example will be a two year investment. The expected benefit of the initiative is improved operational efficiencies by lowering the amount of time spent on corrective controls. The company will measure the improvements over a two-year period.

Investment Rationale: *To increase the effectiveness in daily operations by lowering the costs related to time spent on corrective controls, per annum.*	
Projected Costs	
Onetime costs	€ 87 000
External cost for training during project	€ 11 000
Cost of employee time for training	€ 20 328
Initial cost (sum of cost elements above)	€ 118 328
Project duration (months)	8 months
Recurring costs after project (contingency), per annum	€ 35 498
Projected Benefits	
Current average total cost for corrective controls, per annum	€458 784
Expected improvement	22 %
Cost-reduction in corrective controls, per annum	€ 101 887
Improvement period (months)	24 months
Company prerequisites	
Time to measure costs and benefits	24 months
Company's rate of return	10 %

Figure 12: ***Investment values from a technology company.***

In this information security awareness initiative, we calculate the value of employee-time. A prerequisite for all the calculations to be relevant is that the time being freed up due to the

awareness initiative really is put into useful work. If you do not include this perspective it will appear that you have only added cost without gaining any operational efficiency.

Return on Investment (ROI) is a straightforward financial tool that measures the economic return of a project or investment. It measures the effectiveness of the investment by calculating the number of times the net benefits (benefits minus costs) recover the original investment. ROI has become one of the most popular metrics used to understand, evaluate, and compare the value of different investment options.

$$\mathrm{ROI} = \frac{net\ benefits}{\mathrm{costs}} \times 100\ \%$$

Figure 13: ***ROI Calculation.***

Using the values from Figure 12 with this calculation, you get the following ROI value:

$$\mathrm{ROI} = \frac{(101887 - 118328) + (101887 - 35498)}{118328 + 35498} \times 100\ \% = 32\ \%$$

Figure 14: ***ROI example calculation.***

There are several variations of the Return on Investment (ROI) equation, given the multiple interpretations and applications in different industries. This lack of consistency in the definition of ROI causes confusion when comparing the ROI values of several projects. For further details on ROI variations and other financial formulas, please refer to Appendix A.

Validate investment rationale

Before presenting the investment request to the decision makers, the security manager should ensure an understanding of how the proposed investment will fit with the decision makers' key strategies and goals. The security manager should be able to answer the following questions:

- ✓ What process changes or enhancements that are strategically important are included in the proposed investment?
- ✓ What are the distributions in the current and proposed project portfolios? Will the acceptance of this investment keep the portfolios consistent with the organisation's strategic objectives?
- ✓ What is the relative importance of enterprise-wide versus business unit investments? Does the proposed investment reflect their relative importance?

How to communicate within your organisations

In previous sections, we highlighted how awareness raising is a critical component in the successful use of information security controls. Given this, why is it sometimes difficult to gain support for awareness raising activities?

Senior management is barraged with requests

Management at every level and in every organisation, from the largest global corporations to your local family-owned shop, take decisions every day about how to focus and balance their resources, including people, time, money, and so on. Every day, almost every one of those managers will be

asked to change something about that focus and balance. This constant barrage comes from many sources:

- ✓ Sales people (who always have a better/faster/cheaper solution to some problem you have).
- ✓ Employees (who always have ideas about how things could be done better/differently).
- ✓ Customers (who always love something and hate something about the product or service they are getting, and who someone else always wants to steal away).
- ✓ Peers and colleagues (who want to compare notes, celebrate their victories, and seek counselling on their failures).
- ✓ Industry (every trade publication is full of ideas for doing things differently).
- ✓ Geography (in this community/city/country we do it this way).

Of course there is always a level of risk associated with any resource allocation choice.

The general result of all of this is that many people naturally develop a habit of rejecting ideas almost as a reflex. Even if some requests are approved, others are bounced, and the rest are asked to "redo the business case" or "provide more information". We will discuss how to structure approaching senior management to avoid being lumped in with these unsolicited requests for change. The goal whenever you approach senior management should be to get a "fair hearing" of the awareness proposal.

The synergy between awareness and risk control may not be understood

There is a general belief, often quoted, as "You cannot manage what you cannot measure". This leads to behaviour of "Manage the easily measured" which causes many organisations to focus on the tangibles, while undervaluing intangibles.

Awareness impacts are mostly intangible by their very nature. Certainly there are ways to get some measurements of people's level of information security knowledge through surveys and other instruments. But there is a significant difference between people understanding what they are supposed to say and their behaviour. For example, if you surveyed people and asked them if they should write down their passwords, most people probably would respond that they should not. But if you actually conducted a "desk check" and looked to see if people are in fact writing the passwords on a note stored under the keyboard you may find that people are doing the opposite of what they indicated they "should do".

Awareness, as an information security risk moderator, is not just about people understanding what the rules are, but having the rule and its philosophy become a part of their behaviour; this is the investment rationale for an information security awareness investment.

How do we build the business case for senior management?

Based on the challenges in building a case for awareness training, we need to:

- ✓ Clearly articulate the value of information security awareness for risk control.
- ✓ Structure our proposal to effectively communicate with senior management.

Our proposal is to compose the business case so that concepts are quickly introduced, presented in business, not technical language, and move directly to the point without wasting time. In many organisations a programme such as this may only get a few minutes of time and attention from senior management, so the time must be used very efficiently.

The six topics or parts of a quick business case which have been identified are:

Each organisation's culture has a preferred format for presenting information to management. Some organisations thrive on structured memorandums, while others expect bound reports with colour-coded covers. The following method of building the business case and presenting the business case is provided with the "slide presentation" style in mind, but can be adapted to fit your organisation's preferences.

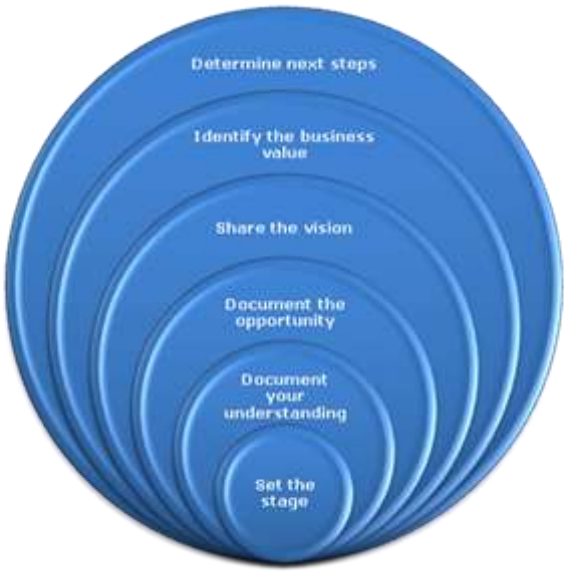


Figure 15: ***Six topics of a quick business case.***

Set the stage

The goal here is to provide a brief statement that focuses and frames the discussion. It quickly communicates the scope and purpose of the proposal – your investment rationale. In the context of promoting an information security awareness campaign it is important to identify the business risks (costs, inefficiencies and so forth) that you wish to address. Here are some possible "Set the Stage" statements:

- ✓ "In support of the business decision not to permit wireless routers to be connected to the corporate network, which was taken to avoid customer data confidentiality breaches, we wish to ensure that branch offices are aware of this restriction and understand how to recognise violations."
- ✓ "In support of the business decision to improve the organisation's overall profitability, we wish to increase employee awareness of how time spent on corrective controls can be minimised, in an effort to drive down cost by 20 % per annum."
- ✓ "Law enforcement has informed us that more than one third of our peer banks have been the target of ATM skimming rings. To date, we have not been a target, but we wish to increase employee and ATM operator awareness of this problem in an effort to identify tampering early."

It is very helpful to stay up-to-date with current information security incident and privacy breach reports and news and use them within your "set the stage" statements. You will grab management's attention and keep it more successfully by providing information of an event that actually happened, or validated research about how business is impacted.

Document your understanding

Now that you have "Set the Stage" you have, in effect, identified the scope of the business case. Now demonstrate that you, in fact, understand the business problem well enough to credibly present solutions.

Senior Management must:

- ✓ *Conceptually agree to the existence of the threat or problem.*
- ✓ *Understand the threat in terms of this organisation.*
- ✓ *Believe this is properly understood by you.*

The goal here is not to spill out every fact that has been collected, but to provide a quick and pointed summary to demonstrate your understanding of the issues as they relate to business.

There are two major goals for structuring the business case:

- ✓ Document the business problem to be addressed.
- ✓ Identify any potential adverse impacts that the awareness initiative may have.

For example, let us assume that you are implementing an awareness programme to reduce the amount of unprotected confidential information in emails. In this section you might initially discuss topics such as:

- ✓ The importance of email to the organisation.
- ✓ The total volume of email within the organisation.
- ✓ The portion of that email that contains confidential information.
- ✓ The business impact of inappropriate communication of that confidential information to the public.

Secondly, you will want to briefly document that you understand the business impact. This would include consideration of such things as:

- ✓ Will the awareness effort result in a sudden change in critical business processes?
  How has this been researched?
- ✓ How will this effect customers and suppliers?
- ✓ What email-protection tools are available?

A key component in communicating your understanding of the business problem is addressing the issue, head on, of painful business impacts.

Document the opportunity

In the previous section you documented that you do, in fact, understand the business, as well as the risks of adverse impact on the business. Now, you need to document what the opportunity is. What is the business value of addressing the risks you need to control with this awareness effort?

Frequently the business value will be qualitative. Do not shy away from documenting qualitative benefits, but do try to enrich them with applicable qualitative and quantitative data from outside sources.

In this portion of the business case, you need to lay out the specific value proposition provided by the awareness efforts you are about to propose.

It may be difficult to provide hard data regarding the return on investment, but often there will be information available from industry analysis or from the cost of incidents that have occurred at peer organisations, or that have been published in news reports.

Share the vision

So far we have been discussing "Why do we need this awareness programme", now it is time to describe the programme itself. At a high level, what are the actual awareness activities that you are seeking support and funding for? It will be critical to your funding success to make this communication of your vision as clear as possible.

Identify the business value

In the "Document the Opportunity" section the business value was discussed, but probably as a negative. Take an opportunity to restate the business value of the programme in positive language.

Determine next steps

Why did you want to give this presentation to senior management? You have something you want to ask for, now is the time to ask for that support, identify any final steps that are needed, or determine what is missing.

Main challenges and risks to obtaining sufficient investment

There are numerous challenges to obtaining sufficient funding for awareness initiatives. If you consider them ahead of time, you will be better prepared to respond to them. Figure 15 provides a few of these challenges, along with some ways in which you can respond to these roadblocks.

	Description	
Challenges	**Insufficient management understanding of the net value of security awareness**	It could be argued that management needs to be security-aware to appreciate the value of security awareness, a chicken-and-egg situation. One answer might be to use initial seed funding to work first on demonstrating the value of security awareness to senior management using terminology and high level issues that are most relevant and of concern to senior management such as governance effectiveness, compliance or cost reductions.
	Insufficient confidence in the cost-benefit analysis, particularly the estimated financial benefits of improved security awareness.	A possible approach here is to deliver a limited pilot study (such as covering a single department, site, business unit and so on) to prove the awareness methods and validate the projected numbers, which implies that suitable metrics must be in place.
Risks	**The programme takes too long to get going or runs out of steam.**	This has indeed been the fate of many awareness programmes that relied on once-a-year awareness events. After the initial enthusiasm has waned, the event loses all relevance and is soon forgotten. The organisation returns to its old ways, if indeed it ever changed. Behavioural research indicates that short one-off events are unlikely to have much if any long term impact, especially if the events are relatively banal.
	The programme does not receive the necessary widespread management support to have the desired effect	If management does not understand the rationale for the programme, there is less chance of it receiving the necessary level of support. Even worse, if the programme is seen as someone's costly project, perhaps just another example of information security controls that interfere with business, the lack of support may evolve into proactive dissent.
	The programme is too costly or disruptive to operations.	As with any investment, mismanagement of the awareness programme carries a risk of runaway costs and failure to deliver the anticipated benefits.

	Description	
Risks		Costs for an awareness programme stem not only from preparing and delivering the awareness messages (the transmission side) but also from absorbing and responding to the messages (the reception side). The true cost of a traditional one-day training course, for example, includes the day away from normal activities for each student as well as charges for the trainer, venue and materials.
	The programme "fails to deliver" *i.e.* is actually ineffective or is perceived as such.	The cultural changes that accompany even an effective security awareness programme are likely to be quite subtle, so subtle in fact that they may not be recognised or appreciated as such. The key to addressing this risk is to plan for the long term, not expecting to achieve dramatic results in the first few months of the programme. Setting management's expectations realistically is therefore something to be taken into account when preparing the investment proposal. A parallel requirement is for someone to monitor the organisation for signs of cultural change, report them and indeed vet them, encouraging further changes in a positive direction. Extending conventional numeric metrics with words illustrating and explaining the changes that are taking place is one way to do this. Examples or case studies are worthwhile, especially in relation to pilot studies.

Figure 16: ***Main challenges to obtaining investment.***

PART 2: 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 perform cost benefit analyses for information security awareness programmes.

Recommendations

There are a number of recommendations to ensure the support and funding of senior management.

#	Recommendations	Details
1	Raising information security awareness is not a one time effort	As there is continual change, it is hugely important to ensure an on-going programme to raise awareness in employees on the value of proper information security management.
2	Analyse your target group	It is important to analyse the needs, interests, information security knowledge of the target group of the initiative and prepare an investment rationale accordingly.
3	Prepare a business case	A business case is a decision support and planning tool that could be used to obtain funding from senior management. Financial analysis is generally central for a good business case, and will help awareness investments competing for limited funds. Ensure the team preparing the business case has the skills and experience needed to cover both information security and business knowledge.
4	Plan how to measure success	Non-financial measures that can be used include: ✓ Impact on a core information security metric. ✓ Impact on a knowledge benchmark. ✓ Less employee-time spent on corrective controls. ✓ Incident avoidance benefits. ✓ Incident cost-reductions. Financial measures should be related to standard calculations, for example Return On Investment (ROI), Net Present Value (NPV), Investment Rate of Return (IRR) or Discounted Cash Flow (DCF).
5	Plan and implement the awareness initiative appropriately	Use plans and phases to help make the tasks and activities more manageable. Also create a communication plan. The whole awareness initiative should be an on-going and not a static process.
6	Keep senior management interested in the initiative	Offering regular updates on topical subjects or directly contacting senior management can be an effective method of keeping the senior management involved and supportive.
7	Ensure to have senior	Involve senior management during all phases of the initiative and

#	Recommendations	Details
	management support during the entire lifecycle of the initiative	always ensure you their support. Otherwise the initiative will not go forward as it will encounter passive resistance from employees.
8	Show results	Follow up on the metrics you have chosen and communicate these regularly.
9	Share success	Celebrate success and use the intranet and management meetings to ensure that a successful initiative is noticed.

Figure 17*: Obtaining funding.*

Conclusions

The security landscape is continually changing. Having an organisational security policy does not in itself drastically reduce the proliferation of security breaches. Human error can undermine even the most stringent information security framework. Awareness of the risks and available safeguards is the first line of defence for the security of information systems and networks.

Information security is not only a technical issue but a business and governance challenge that requires the involvement of senior management to assess how to react to emerging threats. The priority given by senior management to awareness initiatives makes an impact on the extent to which these initiatives will be successful.

ENISA hopes this paper will provide organisations with a valuable tool to take the first steps to gain management support and sponsorship for information security awareness 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).

Cardholm, Lucas, *Adding value to business performance through cost benefit analyses of information security investments*, University of Gävle, 2007, available at http://urn.kb.se/resolve?urn=urn:nbn:se:hig:diva-238 (last visited on 28 July 2008).

Corporate Governance Task Force, *Information Security Governance: Call to Action*, USA, 2004.

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

Erik T. Heidt, *Basics of the Quick Business Case: How to Champion Your Next Information Security Initiative*, RSA Conference Europe 2007, 2007, available at http://artofinfosec.com/22/art-of-info-sec-001-quick-business-case/

Ernst & Young, *Global Information Security Survey,* 2007, available at http://ey.com/ (last visited on 28 July 2008).

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

Herold, Rebecca, *The Privacy Management Toolkit*, Information Shield, Houston, TX, 2006.

http://www. informationshield.com/privacybreachcalc.html.

IT Governance Institute, *Information Security Governance: Guidance for Boards of Directors and Executive Management,* 2nd edition, USA, 2006.

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).

Noticebored, *Business case for an Information Security Awareness Program*, 2008, available at http://www.noticebored.com/NB_generic_business_case_for_infosec_awareness_program.pdf (last visited on 22 July 2008).

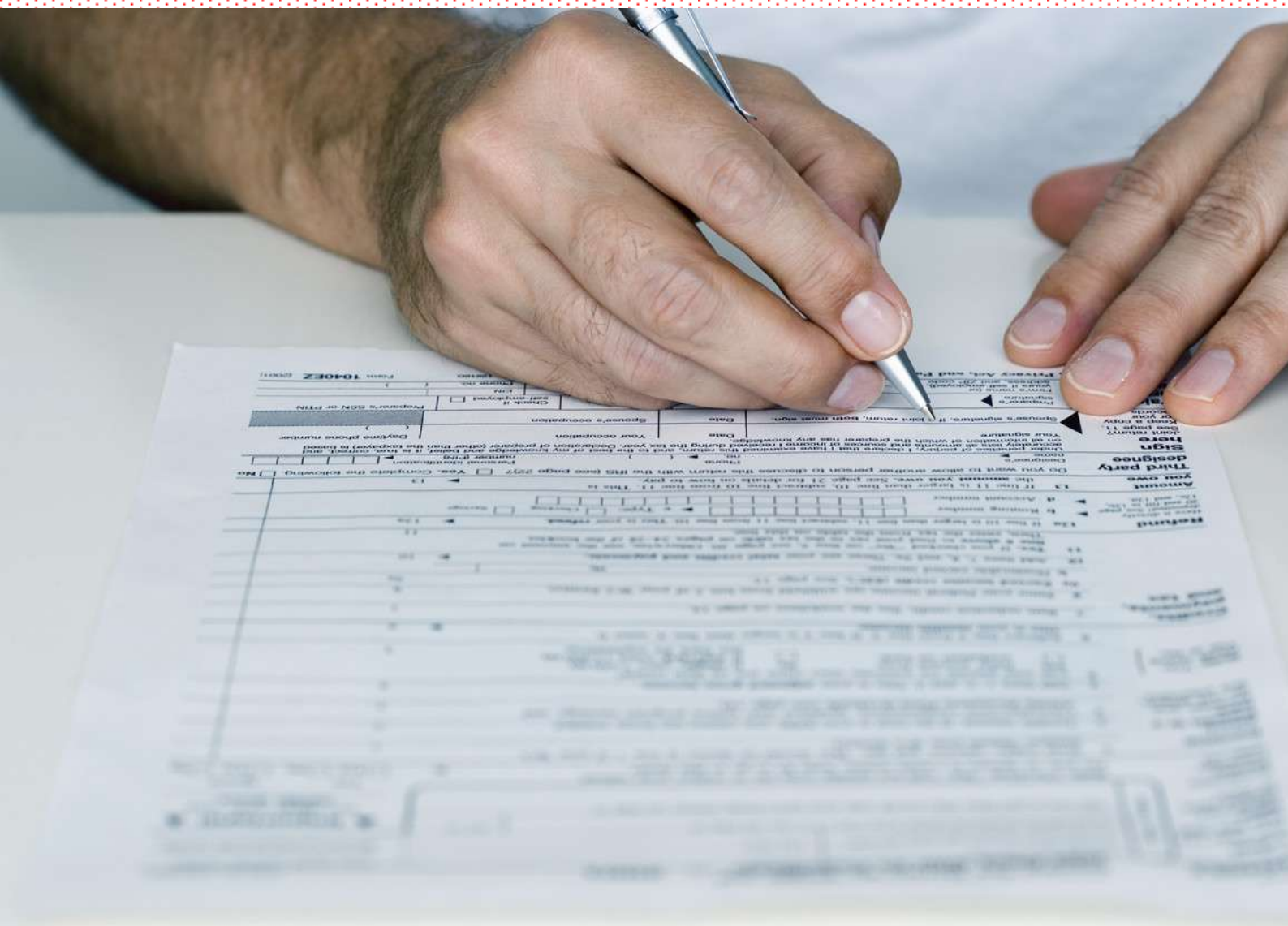
Pepperdine University, *The Cost of Lost Data: The Importance of Investing in that "ounce of prevention"*, Graziado Business Report 2003, volume 6, issue 3, available at http://gbr.pepperdine.edu/033/dataloss.html (last visited on 28 July 2008).

Poole, Vernon, *Why Information Security Governance Is Critical to Wider Corporate Governance Demands—A European Perspective*, available at

http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=30681&TEMPLATE=/ContentManagement/ContentDisplay.cfm (last visited on 28 July 2008)

Weill, Peter and Jeanne W. Ross. *Governance Arrangements Matrices by Industry,* Boston (MA): Harvard Business School Press, 2004 (II).

APPENDICES



Appendices

Appendix I - Financial calculations used for investment requests

Financial performance metrics

The collection of financial performance metrics collected below covers well-known examples used to justify investments. The security manager should look at which of these best suits the value and investment disciplines of the organisation and the nature of the information security awareness initiative.

ROI (Return on Investment)

Metric	Description
ROI (ROIC)	There are several variations of the ROI equation, given multiple interpretations and applications in different industries. This lack of consistency in the definition of ROI complicates the comparison of ROI values of several projects unless they are calculated on the same basis.

$$\mathrm{ROI} = \frac{net\ benefits}{\mathrm{costs}} \times 100\ \%$$

Definition of terms

- ✓ Net benefits: Benefits minus costs.
- ✓ Costs: Initial and recurring (or on-going) costs.
- ✓ Time Period: The standard ROI equation is usually calculated for the first year of the investment. A one-year time period has become an industry standard since companies seek to recover their investment on the first year of operations of the project. This rule of thumb may not be applicable across organisations but it can give a first estimate of the benefits of a project.

$$\mathrm{ROIC} = \frac{NOPAT}{\mathrm{invested\ capital}} \times 100\ \%$$

Definition of terms

- ✓ NOPAT: Net operating profit after taxes.
- ✓ Invested capital: Initial and recurring (or on-going) costs.

NPV (Net Present Value)

Metric	Description
NPV	The NPV of a project or investment is defined as the sum of the present values of the annual cash flows minus the initial and subsequent investments. Future values are discounted according to the organisation's cost of capital and the risk inherent in the investment. NPV is one of the most robust financial evaluation tools to estimate the value of an investment.

$$\mathrm{NPV} = initial\ \ investment + \sum_{t=1}^{t=end\ of\ project} \frac{(Cash\ Flows\ at\ Year\ t)}{(1+r)^t}$$

Definition of terms

- ✓ Initial investment: This is the investment made at the beginning of the project. The value is usually negative, since most projects involve an initial cash outflow. The initial investment can include hardware, software licensing fees, and start-up costs.
- ✓ Cash flow: The net cash flow for each year of the project: Benefits minus Costs.
- ✓ Rate of Return (r): The rate of return is calculated by looking at comparable investment alternatives having similar risks. The rate of return is often referred to as the discount, interest, hurdle rate, or company cost of capital. Companies frequently use a standard rate for the project, as they approximate the risk of the project to be on average the risk of the company as a whole.
- ✓ Time (t): This is the number of years representing the lifetime of the project.

IRR (Investment Rate of Return)

Metric	Description
IRR	IRR is defined as the discount rate that makes the project have a zero Net Present Value (NPV). IRR is an alternative method of evaluating investments without estimating the discount rate.

The IRR uses the NPV equation as its starting point, but calculating the IRR is done through a trial-and-error process that looks for the Discount Rate that yields an NPV equal to zero, typically accomplished by using the IRR function in a spreadsheet program:

$$\mathrm{NPV} = 0 = initial\ \ investment + \sum_{t=1}^{t=end\ of\ project} \frac{(Cash\ Flows\ at\ Year\ t)}{(1+IRR)^t}$$

Definition of terms

- ✓ Initial investment: The investment at the beginning of the project.
- ✓ Cash flow: Measure of the actual cash generated by a company or the amount of cash earned after paying all expenses and taxes.
- ✓ IRR: Internal Rate of Return.
- ✓ N: Last year of the lifetime of the project.

FCF (Free Cash Flow)

Metric	Description
FCF	FCF represents the cash that a company is able to generate after laying out the money required to maintain/expand the company's asset base. Creative accounting can cloud earnings, but it's tougher to fake cash flow. For this reason, some investors believe that FCF gives a much clearer view of the ability to generate cash (and presumably profits).

There is a risk with focusing short-sightedly on earnings while ignoring the "real" cash that a firm generates. That is why free cash flow is important, because it allows a company to pursue opportunities that enhance shareholder value. Without cash, it's tough to pursue new opportunities, make acquisitions, pay dividends, and reduce debt and so forth

It is important to note that negative free cash flow is not bad in itself. If free cash flow is negative, it could be a sign that a company is making large investments. If these investments earn a high return, the strategy has the potential to pay off in the long run.

DCF (Discounted Cash Flow)

Metric	Description
DCF	DCF analysis uses future free cash flow projections and discounts them to arrive at a present value, which is used to evaluate the potential for investment. If the value arrived at through DCF analysis is lower than the current cost of the investment, the opportunity may be good.

$$\mathrm{DCF} = \sum_{t=1}^{t=end\ of\ project} \frac{CF_t}{(1+r)^t}$$

Definition of terms

- ✓ CF: Cash flow: net cash flow for each year of the project: Benefits minus Costs
- ✓ r: discounted rate (weighted average cost of capital)

TCO (Total Cost of Ownership)

Metric	Description
TCO	The goal of TCO is to determine a figure that reflects the total cost of the investment, including one-time purchases and recurring costs, not just the initial start-up cost. Because benefits are not considered in TCO, the overall financial analysis is simplified.

$$\mathrm{TCO} = \sum_{t=1}^{t=end\ of\ project} \frac{\text{One time costs} + \text{recurring costs(t)}}{\text{project duration}}$$

Definition of terms

- ✓ One-time costs: These are the costs that are derived at one stage during the implementation or operation of a project. One-time costs could include personnel training, new processes being introduced that yield one-time cost, or investment in infrastructure assets.
- ✓ Recurring costs: These are costs that continue over time or repeat, for example continuous monitoring of performance.
- ✓ Project duration: This is the project lifespan or a standard duration that is used to normalise all the TCO calculations across an enterprise.

TBO (Total Benefit of Ownership)

Metric	Description
TBO	The idea of TBO is to emphasize that the benefits of an implementation may be greater if other hidden benefits are included, such as customer satisfaction and product up-sells (persuading customers to buy more expensive items or enabling new business channels). Because costs are not considered in TBO, the overall financial analysis is simplified.

$$\mathrm{TBO} = \sum_{t=1}^{t=end\ of\ project} \frac{\text{One time benefits} + \text{recurring benefits(t)}}{\text{project duration}}$$

Definition of terms

- ✓ One-time benefits: These are the benefits that are derived at one stage during the implementation or operation of a project. For example, one-time benefits could include personnel reductions, process changes that yield one-time payoffs, or consolidation of assets.
- ✓ Recurring benefits: These are benefits that continue over time or repeat, such as improvements in productivity or performance, or increases in customer satisfaction.
- ✓ Project duration: This is the project lifespan or a standard duration that is used to normalise all the TBO calculations across an enterprise.

EVA (Economic Value Added)

Metric	Description
EVA	In the field of corporate finance, working capital management is useful to improve a company's financial performance metrics. Economic value added is a way to determine the value created, above the required return, for the shareholders of a company.

$$EVA = (r - c) \times K = NOPAT - c \times K$$

Definition of terms

- ✓ r: The return on capital employed (ROCE) defined as $\mathrm{r} = \frac{NOPAT}{K}$
- ✓ NOPAT: The Net Operating Profit After Tax
- ✓ c: The Weighted Average Cost of Capital (WACC)
- ✓ K: capital employed.

ROSI (Return on Security Investment)

Metric	Description
ROSI	The risk mitigation effects show the benefit of a security investment: it is basically a "savings" in Value-at-Risk; it comes by reducing the risk associated with losing some financial value.

Financial performance measures do not consider security-specific data (such as threats, vulnerability, and risk) as a decision variable. As a vehicle, security professionals – striving to find variables to judge the need for a particular investment – have developed models in the field of cost benefit analyses for information security. The effects are the consideration of risk effects and the ability to integrate those in common accounting concepts.

The Return on Security Investments (ROSI) formula was developed by a team at the University of Idaho led by researcher HuaQiang Wei. They used what they found in the research area of information security investments and combined it with some of their own theories, assigning values to everything from tangible assets to intangible assets.

$$ROSI = R - (R - E) + T$$

or

$$ROSI = R - ALE$$

Definition of terms

- ✓ ALE: What we expect to lose in a year (Annual Loss Expectancy)
- ✓ R: The cost per year to recover from any number of incidents.
- ✓ E: These are the financial annual savings gained by mitigating any number of incidents through the introduction of the security solution.
- ✓ T: The annual cost of the security investment.

The impracticality of ALE-based methodologies, with their massive assessment needs, has forced security professionals to develop alternative strategies that would be less prone to controversy and more easily implemented. Some remove the "likelihood half" of the risk definition while others depend upon full statistical data to ensure validity. Both examples show the downside of relying on ROSI, especially if competing with other investments, not depending on this formula.

Appendix II - Legend

Examples and case studies from other organisations dealing with different awareness matters.	**Description of the company – main topic of the case study/example** Case study / example description
Key problems, issues and solutions are identified, making the main outlines of the document more effective and concrete.	*Outlines of the document*

Obtaining support and funding from senior management while planning an awareness initiative

ISBN: 978-92-9204-013-0

Catalogue number: TP-30-08-572-EN-C

TP-30-08-572-EN-C

enisa
European Network and Information Security Agency

ISBN 978-92-9204-013-0

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