Computers & Security, 19 (2000) 337-347

Implementing Information Security In The 21st Century — Do You Have the Balancing Factors?

Julie D Nosworthy

Principal Consultant, Sherwood Associates Ltd, Management Consultants, 18 Braemore Road, Hove, BN3 4HB, UK

Introduction

Over the last 10 years or so the focus of 'selling' information security has been towards identifying the 'need' for information security, obtaining board approval and senior management support. Once this has been sold and the information security policy statement written, what happens then? How do we educate the people of the organization to successfully implement the requirements of the information security policy. Let's reflect briefly on what the information security policy is about.

Information Security Policy (ISP)

In short the ISP is a statement of intent from the board and the objectives of the policy are:

- To demonstrate board and senior management commitment towards information security.
- To set direction for implementation thereby emphasising that they see it as an important part of the organizations day to day operations.
- To maintain continuity of operations thereby continuing to provide services.
- To protect the company's assets.

Who Should the Policy Reach?

The ISP should reach the people of the organization and not just those responsible for the implementation process. From experience it has been a recurrent event to come into contact with people who do not know that the policy exists never mind know what to do with the implications of it.

'If we don't know what to do, then how can we do it?'

I wonder how many times that we've heard this axiom voiced. How can the people be expected to perform their duties to the required standards, policies, procedures, regulatory or legislative requirements, if they are not told in the first instance that the ISP exists and secondly how to initiate, implement and maintain the requirements?

Do you sometimes feel powerless and sit with your head in your hands feeling that the implementation of the requirements of the ISP should be more successful than it is? You feel that there is something missing, but you have no idea which piece/s of the jigsaw it is? It can be a frustrating experience.

The Balance of Risk and Control

In order to control the overall business risks a balance of business and technical controls should be implemented. In order for us to move into the 21st Century and counteract the imbalance in the implementation of a successful information security management (ISM) programme we first need to identify what the cause of the imbalance is.

Some Causes of the Imbalance

The imbalance of control is based on those factors that tip the scales, those that stall or prevent any attempt to effectively communicate and implement an (ISM) programme. The following is an outline of some of the causes of the imbalance experienced in the implementation of an ISM programme, but is by no means exhaustive:

'It will never happen to us' — In many cases the balance of control is weakened by the fact that organizations still have the mindset that 'It will never happen to us', 'it's always worked that way, we've *never* had a problem'. Never say never.

Emphasis *just*_on IT *not* the Business — Factors that influence the level of information flow control shouldn't just come from a technical view if it is to be effective business wide. There must be business risk control to meet the overall business objectives. When we speak about information security there is a majority that still believes and operates as though it is an IT issue. This is because in many cases the 'buy-in' process has been initiated in the IT department and remains there and doesn't reach the business. The cause for this maybe that the people are not able to express the risks, in simple terms, in order that they are understood by their managers and above.

Reluctance to Release Resources — There is a reluctance to release resources in a large number of cases. Maybe it is because people are already allocated on projects, or the business will 'stop' if X is released to help Y, or most of all a lack of understanding of the requirements of information security. Therefore it isn't known whom the right people will be to allocate the task to, or to give the people the necessary time to be trained effectively.

Lack of Understanding for Information Security — Information security is intangible, we cannot see or touch it, so why should we pay any attention to it? It, therefore, is difficult for some organizations to understand the purpose of information security and what it means to the organization and to them as individuals performing an important part of the organization's operation, and there are benefits as you will see as we progress through this paper.

Lack of Awareness for Responsibility and Ownership — People must be allocated responsibility and ownership for the information in its different forms and categories whether it is general security, specialist or role related issues. Information must be owned, but not just by one person.

Lack of Experience of HR Issues — Human Resources is, by its very nature, a people department. They are there to assist in the recruitment of the right people. They too are 'the people' and should also have an understanding of the requirements of information security in order that they are able to recruit the right people. They should also ensure people's welfare and incorporate operational and security education and training into roles and responsibilities. But, those members of the management teams who are responsible for recruiting in the business should also work with human resources in order to gain the right balance of requirements and thereby recruit the right people for the roles.

Non-Acceptance of Importance of Security Education and Training — Because of the lack of understanding for information security, that we discussed earlier, this will, of course, have a knock-on effect to the non-acceptance of the associated training. But the people in the organization need to be made 'aware' of information security and what it means to the organization. They need to be educated to understand. They need to be encouraged, motivated and assured and know where to go to if they have problems.

No Training Budget — Budgetary requirements for operational and security education and training are not generally on the top of the list in the annual budget. When one first scrutinises this concept of implementing an on-going training programme at face value it will appear to be a very expensive overhead. However, those organisations who feel that they can commit themselves to such a program will find that the on-going programme will achieve more visible signs of improvement in the implementation of ISM than any technical solution could ever wish to accomplish.

So, which way now? What do we do? How can we balance all these factors and incorporate them into an effective ISM implementation programme in order to balance the scales?

Balancing Factors

After Initial Buy-In

There are a number of ways that the initial ISP can be 'communicated' to the people of the organization. It can be communicated in the monthly brief, posted in the in tray, etc. and no-one has spoken to anyone in the organization yet! In many cases it isn't evident how ISP has been 'communicated' to the rest of the organization. Humans will be humans, if the ISP is not voiced directly to the people and understood then, nothing may be actioned. The ISP may remain in the everlasting pending tray either because they don't know what to do with it, "it's the first that we knew about it", they may not know who to approach to obtain further details, they don't understand and so on. Can you be sure that you have really communicated the message to the People?

Getting the Message to Business and IT Managers

Information Security is still currently too orientated towards IT, protecting other operational aspects has become under prioritized. As we have just briefly discussed information security is not a technical issue although some of the nuts and bolts have a technical impetus, but not all of the answers lie in the IT department. Information security is about the Business *not just* IT. It deals with the critical business processes, the people and the associated tools which include for example:

Mobile Phones — Conversations on mobile phones can be intercepted, can you be sure you are speaking to the right person? Can you be sure that no one else is listening to your conversation? Do you leave it in your car? Do you store important telephone numbers in the memory and so on?

Presentation Slides — Meetings that are held on presentation slides can be the source of all kinds of useful information to the potential intruder. Where do you store them? Do you leave the meeting room unlocked when you go to lunch? How do you dispose of them and so on?

Briefcase — This can either be used to keep your sandwiches and newspaper in or can be the sole source of information carrying minutes of meetings, unpublished details of the annual figures, disks holding sensitive information and so on.

Architect's Pad — If you are purchasing or developing new buildings or just moving your secured areas etc., are you careful about who sees where you plan to locate your rooms? Are the rooms secured where the plans are currently being worked on? If not, are they stored away securely?

Portable Computer — What do you store on it when in transit? Do you take it with you when moving away from your vehicle and so on?

People — What information do you know? how do you use it? how do you control it?

ISM

ISM is about the 'business not just IT' and how 'we – the people' take care of and direct the business. It's about:

People — Where would we be without people? People make things happen. The ISP is useless without the people to make it happen.

Culture — The organizational culture plays a major role in information security, as this may hinder change and determine what type of change is practical and what is not practical to be done based on the critical business processes.

People's Attitude — The way in which people view information and its security and what it means to the organization and them as individuals, as part of the organization. It is paramount that the people are educated to want to be more secure in their day to day operation. The change of attitude is of utmost importance. A change in attitude automatically leads to a subsequent behavioural change. The people can then become the organization's most valuable assets!

Discipline — Having the ability to encourage and motivate one's self to make things happen and to be enable ourselves to be encouraged and motivated.

Organization — This is about the day to day way we go about our work….habit, routine, logical movements and life cycles of information. It is important to know where the information is at all times.

Management — It is the people who drive the business and the management of the whole ISM programme.

Communication — The requirements of the ISP and its implications should reach the people. The ISP has very little use if the people do not know how to begin to understand and act on the implication of a full implementation programme.

Security Education and Training — The people cannot make the ISP happen without it. Information security is such a wide topic, people will have different responsibilities, and one person can not know and/or do everything.

Ownership — Somebody needs to own the information.

Defining the Roles — It is more advantageous to define the role's objectives and scope for ISM dependent on the requirements for implementation and ongoing maintenance than to go rushing headlong into allocating the full responsibility of information security to one person. It is not possible for one person to take on all the criteria that is involved in the implementation and maintenance of an effective ISM programme. If specific roles are not practical to allocate or recruit into the organization for whatever reason then it may be more effective to share the responsibilities.

Job Descriptions — Job descriptions should state the:

- Role objectives, scope etc.
- Role responsibilities including information security responsibilities, should be documented. It is then clear as to what is required of the people.
- All education and training requirements.
- Specific operational training together with the security training requirements should also be documented. They can then be expanded into specific areas for the particular individual or sets of individuals as part of their goals to be achieved for appraisals.

Responsibility — The people must be responsible for information security requirements throughout the life span of the information from inception to destruction or disposal and must also be responsible for their own actions. Do we also still have the misconception that the responsibility for information security is his/her responsibility and point the finger to the nearest person available. Someone in the right place, at the right time? Passing the buck to someone else, 'it's not my responsibility' and so on? How many of you can relate to this, especially those who are on the receiving end? A common problem is that no one knows whom the job should really belong to. It is important to be able to define roles and identify the responsibilities and allocate the correct expertise and person to the role/s.

Incorporate into an Existing Role — Identify from the current staff which roles are able to

incorporate which information security responsibilities effectively as part of the day to day duties.

Create New Roles — In some cases the information security responsibilities are such that it would be impossible for that person to take on those specific responsibilities, in addition to their day to day tasks. Therefore, it maybe necessary to create a new role/s and either recruit internally if the expertise is there, recruit externally or outsource for a period of time etc. Dependent on how far the ISM implementation programme is with the overall business objectives it may be necessary to take on a consultant with the relevant expertise for a period of time as an exercise for the transfer of knowledge. Whatever you decide to do it is important to remember that … ISM is Everyone's Responsibility! Including third parties, i.e. Customers, Suppliers, contractors etc.

Human Resources

The role of human resources is to help recruit the right people. Management and human resources should work together in order to obtain the 'right' person for the roles even if they are not directly related to any specific security responsibilities. Information security should be addressed at the recruitment stage and monitored and managed throughout the individual's employment with the organization. Not forgetting to readdress the employee's responsibilities when moving around the organization should the individual make a sideways move or be promoted or demoted.

Specialist Advertising — As the search for the right specialist skills becomes more difficult worldwide human resources and management sometimes need a helping hand too. There are agencies specializing in information security positions who are able to assist in the search for the right person for the role guided by the requirements from human resources and management responsible for the position advertised.

Recruitment Screening — Screening should be carried out specifically for those roles that require specialist knowledge to obtain access to sensitive information and technology holding sensitive information.

Confidentiality Agreements — All employees and third party users should sign a confidentiality (non-disclosure) agreement.

Education and Training — If organizations have training departments they are normally attached to human resources. If programmes for training are developed internally then the management and relevant members of staff should work in conjunction with human resources to develop the right training for the right people. Likewise, if external sources are used then human resources, management and relevant staff should work in conjunction with the third party. The third party could develop the programme on a transfer of knowledge basis such that the organization, when ready, could take on the whole training programme themselves.

Budget — Human resources and all levels of management who are responsible for the budgeting process must provide for all education and training requirements when preparing the annual budgets.

Induction — It is important that as soon an employee joins the organization they are given their induction schedule such that they are indoctrinated from day one with the standards, regulations and rules of the organization. Ideally, until the employee is trained on their particular responsibilities they should not have unsupervised access to any sensitive information or technology holding sensitive information and they have to understand this. Sometimes this is not practically possible, where this is the case, the situation should be supervised and managed effectively.

Incentive Schemes — Since we are dealing with people's behaviour and it is the behavioural pattern that we are trying to change then it is essential that the motivation of the people be maintained. In order to encourage staff to maintain the required level of ISM it may be necessary to develop some sort of an incentive scheme. Humans, by their very nature, like to be rewarded if they have achieved and in order to reinforce these achievements they need to be able to see their reward and for them to encourage those that are not quite so easily motivated.

Define Measurement Factors — For example: an award scheme could be initiated for say, participation in organizing and presenting at work shops, developing new ideas for effective ISM, have occasional competitions, award certificates of achievement and so on. This maintains the people's interest, raises moral and motivates.

Performance Appraisal Scheme — Integrate the award scheme into the performance appraisal scheme.

Disciplinary Process — When anyone says these words, it makes you wince. The mere mention of discipline is a de-motivator. The procedure is there to act as a deterrent to those employees who may have tendencies towards disregarding company procedures. There should be a disciplinary process in place and understood by all employees should there be any alleged violation of organizational policies and procedures. The process should be jointly written and managed by human resources and the senior management team highlighting the process and any associated penalties for none compliance with the ISP requirements. It should also be pointed out that the welfare of the business is linked to them as employees, as we said earlier without the people we can not make it happen. It also impacts on their financial security as well as the company's, without them there wouldn't be a business. The people are the business.

Enhancing Security Through Endorsement at All Levels

It's peculiar to think that we managed years ago with just filing cabinets, keys and safes etc. Today, the way we handle, process, store and dispose of information and the associated technology which equates to the old filing cabinets and so on, is a rapidly changing environment. No sooner has one piece of technology been installed, implemented then another one pops along and raises its ugly head. Bring back filing cabinets all is forgiven!

This rapid change in today's environment further enforces the need for ISM and on-going security education and training. Because of increasing volumes of information and the ability of the old technology to handle it, new technology is obviously going to always be introduced. The new technology causes change in itself and generally causes an initial reduction in control and it is important that information security is maintained from inception of the new and changing technology.

Each person in the organization from the CEO to the House Keeping staff must be aware of and trained to exercise their responsibilities towards information security. Inevitably people's responsibilities will differ because there is a cross section of skills and expertise within any organization and information security awareness has to reach every one of them. Therefore, the training programme needs to be a simple, comprehensive, flexible and must be understood by everyone, i.e. board, senior management, line management, security management, data owners, specialists, users, all staff.

Specific awareness issues should be directed at specific staff and directed in different ways. Never assume their knowledge of information security, they need to be told.

Implementing Ongoing Security Education and Training

Ongoing security education and training is a preventative approach to illustrate methods of accepting, avoiding, reducing or transferring the risks of information security. Obvious risks to the organization should be highlighted. There must be an initial understanding of the day to day risks to the organization from a business perspective as well as an IT perspective. Unless the staff are aware of the issues that the organization faces then they cannot be expected to apply the necessary countermeasures. It must encourage and motivate people in order to make them want to learn and to be secure in their day to day operations. An effective ISM programme will only be maintained successfully once the people are motivated towards such a programme. This motivation is the critical factor in an ongoing training programme. They need to understand the importance of security education and training

and familiarize themselves with the security education and training life cycle to be incorporated into all critical business processes.

Understanding the Importance of Security Education and Training

The education and training programme is there to help understand the ISP requirements and minimize risks to the confidentiality, integrity, accountability, authentication and availability of information in any form during the course of their work. Security education and training must also be fun!

Provides a Forum for Communication — Enabling staff to speak if they don't understand, to discuss current issues and problems and so on.

Raises Awareness and Importance — Security education and training raises awareness and importance of any information security issues. We all know that we only take away approximately one third of the knowledge from training sessions, presentations etc. in our heads. There is always reference material to refer to, but the one-third stays with us for a while and if we have been encouraged and motivated enough, we will act on it. If the reference material is prepared such that it can be used on a daily basis then the staff would be encouraged even more to use what they have learned. What you don't use you loose!

Changes Attitudes — Security education and training teaches you to have a different approach on how you view issues. It enables you to view things objectively.

Modifies Behaviour — Security education and training encourages the people to want to behave differently. If they can see the purpose and benefits of the ISM programme and its effects on the business as a whole and more importantly the effect on them as individuals as an important part of the business operation, they will behave differently.

Enables Ownership — Staff will understand their responsibilities more and will be more able to take on ownership for their part of the implementation of the ISM programme. They will be more armed with the tools enabling them to communicate any 'new' issues, or problems with the next person in the operational chain or who is part of a particular working team. Together they should then be able to work it through to its successful conclusion if there are any security loopholes.

Introduces New Skills and Enhances Existing Skills — Introduces and/or updates knowledge for those skills and techniques required to make the ISM programme happen.

Encourages and Motivates Staff — Staff are encouraged and motivated by the fact that the organization has recognized their needs and is investing in them. It's also time off the normal working day and an opportunity to network with other members of the organization, not necessarily from the same department.

Maintains Continuity of Operations — Security education and training ensures continuity of operations ensuring that all staff are armed with the necessary tools. It therefore:

- Enables an Effective ISM Implementation, and
- Gives Third Party Satisfaction – if third parties can see that the organization is committed to investing in the needs of the people then in turn they will get a more efficient service.

Security Education and Training Programme Life Cycle

The Simplest method of managing the implementation of an ongoing training programme is to logically map it out (life cycle)and incorporate it into the organizations critical business processes:

- Define what to do
- Do it …now
- Manage and review effectiveness.

Figure 1 below shows an education training programme life cycle in more detail.

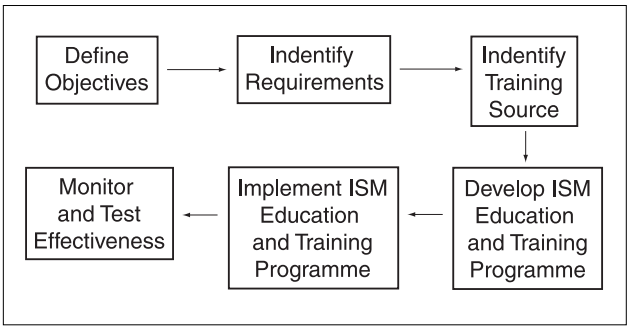

Figure 1: ISM Education and Training Programme

Define Objectives

State clearly what the overall business objectives are and what is expected of everyone.

Identify Requirements — what are your requirements?

You need to enable a method of security education and training that will suit your organization and will communicate the message of information security effectively to all employees. For example, you may decide you would like to have an 'in-house' training programme and therefore wish to identify requirements for training staff internally who will then go on to train the people that they are responsible for information security. You also need to decide what type of security education and training is required and so on? Once you have decided this you can define further requirements for:

Awareness Training — This is relevant for all staff but specifically includes the board, senior management and heads of department which ensures their commitment and full support to information security. When this sort of programme is introduced to an organization it first has to reach all existing employees. An overall awareness framework is advantageous for maintaining a consistent level of awareness in order to understand the concepts.

The staff who are tasked with managing those people with specialist skills need to undergo suitable awareness training to give them a potted view of the specialist training. They will then be armed themselves with an appreciation of the risks and associated countermeasures of the day to day operation that they are responsible for.

Induction — New recruits — ensures all new recruits are aware of the company's policies, standards and procedures.

On-Going Security Education and Training — All staff — Ensures all staff within the organization are aware of their responsibilities for information security. Thereby maintaining confidentiality, integrity, accountability, authenticity, and availability of information.

Specialist Security Training — Security management, system administrators, users, auditors etc. — In addition to the awareness training there needs to be additional more detailed training for those staff tasked with specialist security responsibilities.

Operational Training — All staff — Ensures staff and their deputies understand what is demanded of their appointed roles. Relevant security education and training requirements should be integrated into all operational training.

What to Communicate

Company Policies, Standards, and Procedures — high level relationships, e.g. health and safety, emergency procedures, physical security, logical security, virus control, quality procedures etc.

Basics of Information Security — Confidentiality, integrity, accountability, authenticity and availability.

Purpose of Business Impact Analysis and Risk Analysis — To assess the level of risk within the organization together with the probability and impact of the risk, should it happen.

Purpose of the ISP — discussed earlier.

Translate the ISP — It is important that the people know what is expected of them and should be armed with the necessary skills to identify the requirements

of the ISP and translate the policy into the associated standards and procedures in order to make it happen.

Specialist Areas of Information Security — As we have discussed it is important for those people requiring specialist skills to have the necessary ongoing and up to date specialist training to equip them for day to day management.

Identify Training Source

Awareness raising — is often best communicated from external consultants or representatives from 'like' organizations already operating an information security programme. Conferences are also a source of awareness raising. External parties are seen to be viewed more seriously without affecting the moral of the staff. Also if they have had first hand experience they will be seen as more credible to the organization and thereby convince the board and senior management of the real risks that the organization faces if an effective ISM programme is not implemented. External sources, as we discussed earlier can prepare programmes in order that the knowledge is transferred to the organization in such a way that the awareness raising and the ongoing training programme can become an internal discipline.

Induction — This is generally carried out by human resources or training departments linked to human resources for organizational issues and by line management for those more specific issues.

Ongoing Security Education and Training — The information security manager and their deputy should work in conjunction with human resources to develop a method of operating an ongoing training programme. This should be communicated such that everyone is aware of the information security policies and sub sections there of, the reasons for its existence, what it means to them and the process for implementation and maintenance. The main reason is to keep issues at the forefront of people's minds. You can also encourage staff to take responsibility for company newsletter productions, including information security articles, competitions, etc., also to design posters. There are videos on the market available for hire or purchase, which can be used either as part of an internally tailored programme or in conjunction with external training sources. Other methods to use in order to maintain an ongoing training programme and to continually retain staff motivation are; competitions with a small prize e.g. a shield, trophy, stationery (pens, pencils etc.), mugs, coffee mats with slogans etc. The rewards themselves are also a method of keeping the message alive.

Specialist Security Training — Practical training for those employees who have specialist skills for ISM may also be performed by an external resource for larger organizations. Smaller organizations may be able to set up their own in-house training tailored to the business. If the training is performed from an external source it may also be advantageous to find an organization that has experience in a 'like' business situation.

Operational Training — This is usually in-house training for all staff which is essential to carry out the day to day operation.

Develop and Implement Education and Training Programme

You then need to put all of this together and develop and implement the training programme in line with the company's business plan, critical business processes and project plans.

In order to justify time, effort and money spent it is advantageous to be able to assess the success of the programme by:

Monitoring and Testing Effectiveness

There are a number of ways that this can be achieve, for example:

Walkabouts — Take a wonder around and observe people's habits especially out of hours, e.g. clear desk policies, destruction procedures and the like. It's amazing what you find!

Questionnaires — Develop ad hoc questionnaires either to ensure newly communicated issues have been understood or maybe to see whether all the ongoing stuff is still at the forefront of their minds. Responses to questionnaires can determine the level of security awareness and hence indicate the need for additional or reiterative training requirements.

Training Course Assessment Forms — Determines the quality and relevance of the training given and ensures that the information is always applicable and up to date.

Incident Reporting etc. — Although 'nothing to report' would be the ideal result on any incident report … but unfortunately we don't live in an ideal world. Inevitably there will be incidents, weaknesses etc. to report. Encourage the people to be alert, to report disgruntled or dishonest colleagues, to challenge strangers in the camp and to highlight potential or actual security loopholes and weaknesses.

'What Do We do If Something Goes Wrong?' — The people need to know who to go to for help and to report problems, people very often feel that if they 'tell', they are telling tales out of school. They need to be encouraged as to the reasons for reporting problems, issues etc. It needs to be understood that it is in the company's interest and most of all their interest and it is directly linked to them as employees and the company's survival and their employment and financial capacity! They need to know that it is not 'snitching'. So how can we effectively report and monitor the types and frequency of security incidents etc.? You could, for example, set up a Help Desk.

Help Desk — A help desk can be set up as the first line of contact with an say a manual or electronic incident reporting system.

Incident Report System — The purpose of the incident reporting system is to effectively record and monitor the reporting of:

- Security Incidents
- Security Weaknesses
- Software malfunctions
- Etc.

and escalate the problem to a level of authority with powers to act and also have the ability to monitor the results.

Feedback — There should also be a feedback method indicating the status and action required etc. of the reported problem, issue etc.

Advantages of Incident Reporting:

- Monitors Recurring Security Incidents etc.
- Measures Response Time to Incidents
- Tracks Software/Hardware Faults etc.
- Measures Effectiveness

The objective is to minimize the damage from security incidents and malfunctions and to monitor and learn from such incidents. They should be reported as quickly as possible in order to monitor and test effectiveness in a timely manner.

Maintaining a High Profile for Security

Be Seen to be Doing

If senior management can be seen to be complying with the ISP and the associated procedures then the more likely the rest of the organization will be encouraged and motivated into improving the level of information security. Also, as we said earlier if third parties can see that the organization is committed to investing in the needs of the people then in turn they will receive a more efficient service.

Incorporate Requirements Into Third Party Contracts

In order to maintain the level of information security within your organization, it is advisable to incorporate your security requirements into any third

party agreements and contracts including security education and training requirements. Likewise if you are acting as a third party to another organization, it is in your interests to ensure that they have a level of information security that will not jeopardize anything you have when interacted with your information process. As we are all aware there are increased risks when working with intertwining networks across departments, organizations, and the world!

Legal Requirements

You also need to ensure that your company complies with the legal, regulatory and company requirements for information security, e.g. UK Data Protection Act 1984, BS7799, Company laws, etc.

Communicating New Issues and Strategies

Provision should also be made for communicating new issues, strategies and for the discussing of any new or unforeseen risks etc. So you need to Define Methods — e.g. meetings, workshops, newsletters etc. Frequency of delivery — e.g. weekly, monthly, bi-annually etc.

Other Means of Keeping up to Date are:

- External — Conferences, workshops, memberships, magazines, user groups, etc.
- Self — Books, research, writing for publication, etc.

Benefits of a Security Education & Training Programme

The benefits of a security education and training programme are that it:

- Involves everyone
- Increases awareness and enables us to..
- Learn from mistakes/incidents
- Increases control
- Reduces risk
- Maintains continuity and there is a
- Potential for long term financial savings – e.g. discounts on insurance policies if information security is in place. If the company hasn't implemented an ISM programme then it may be forced to pay a higher premium.
- Gives peace of mind.

Let's take the lessons learned into the 21st Century. Implementing information security is a continuing process balancing the business risks with the appropriate level of controls — do you have the balance right?

The 21st century started with a small contraction caused by the dotcom crises. However, exports continued to be high until 2007. Since the onset of the global financial crises world trade volumes have lagged behind GDP growth. While the 20th century globalization drivers have played their role and lost steam, no new innovations significantly driving globalization have occurred so far. The political climate deteriorated resulting in the beginning of a process of disintegration.Â One of the new forces driving globalization in the 21st century could well be platformization, through players like amazon, alibaba and eBay. 2.9k views Â· View 1 Upvoter Â· Answer requested by. Eva Tindemans.