NOTICEBORED

Innovative information security awareness programs

Business Case

for an

Information Security Awareness Program

Executive summary

This paper lays out the case for an innovative program designed to raise awareness of information security, create a strong security culture and cut net costs.

The awareness program will separately address general employees, executive managers and technologists through appropriate materials. Different information security topics will be covered each month through a continuous rolling communications process. These two innovative features are designed to maximize the breadth and depth of coverage, respectively.

The program will be managed by a dedicated program manager under the leadership of the Information Security Manager, and delivered with the assistance of other corporate functions as necessary. The main expenses will be the program manager's salary and internal recharges for assistance to prepare and deliver the materials. The costs of producing awareness materials will be minimized by recycling existing materials and introducing inexpensive awareness content from a security awareness specialist.

We are confident that the business benefits (resulting from increased compliance, improved control, reduced risks and reduced losses through security breaches) will substantially outweigh the costs of the program. Metrics and methods borrowed from the field of marketing will be used to prove the cost-effectiveness of the program.

Contents

1 Introduction

1.1 Background

Information is a fundamental asset to the business. Security (confidentiality, integrity and availability) of information is therefore critically important to us. We have invested in information security technologies such as antivirus software and firewalls to protect our information assets. However, we are left with significant information security risks as a result of the accidental or deliberate actions and inactions of our people.

Most of the time, most of our employees comply with our information security policies, standards, laws and other regulations but being human, they occasionally "forget" and often make mistakes. They sometimes enter inaccurate or incomplete data into the systems and fail to configure technical security controls appropriately. They share passwords and neglect to take regular backups. They let visitors roam about the offices unescorted and give out sensitive information over the phone. These are not theoretical examples but real everyday occurrences.

A few of our employees, and outsiders in general, may not have our best interests in mind. At the risk of sounding paranoid, fraudsters, hackers and social engineers really are "out to get us". Deliberate threats to our information assets are increasingly prevalent, both non-specific (*e.g*. Internet worms) and targeted (*e.g*. information theft, extortion and targeted Denial of Service attacks).

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

1.2 Purpose of this paper

This paper documents the business case for investing in a cost-effective information security awareness program.

We propose an innovative communications program designed to raise awareness of information security concepts, requirements and controls amongst staff, managers and technologists within the organization. By informing our people about information security and motivating them to comply with the controls, we will establish a widespread, lasting and deep-rooted "**security culture**" that will reduce the organization's information security risks and net costs.

Compared to further investment in security technology, the proposed awareness program is a highly cost-effective means of improving information security controls and, in fact, will derive more value from previous security investments.

1.3 Document approval

Name	Role/Position	Signed	Date
	Information Security Manager		
	Head of IT		
	CEO		

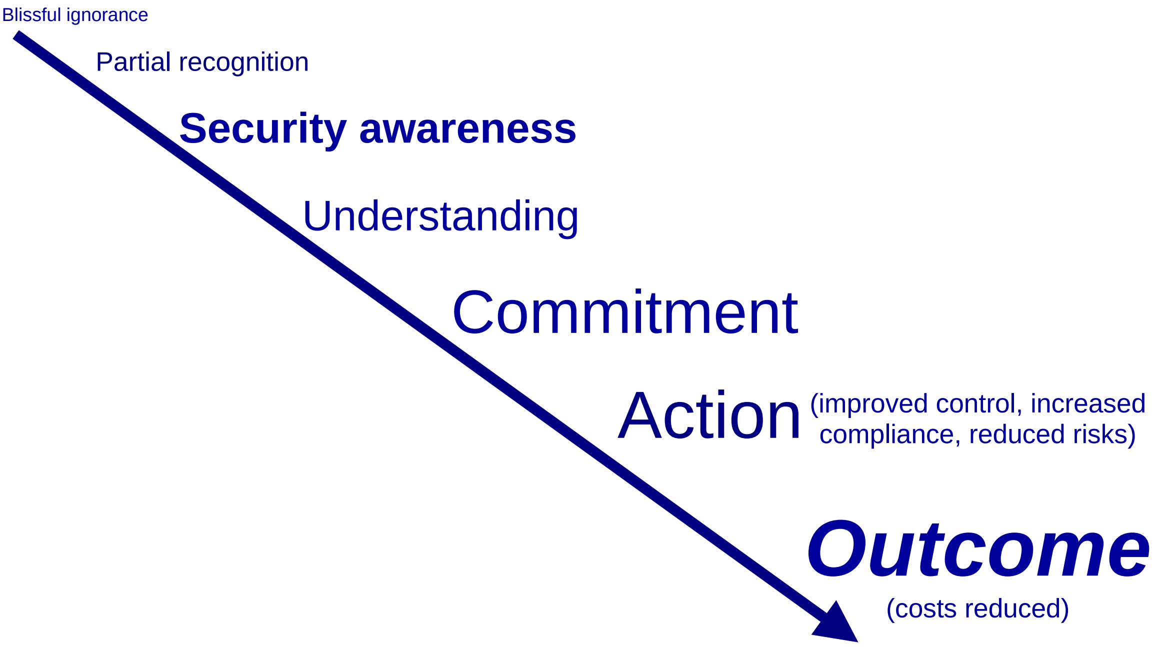
1.4 Document history

Author	Version	Date	Nature of change
	1		Adapted from NoticeBored generic version

2 Awareness program overview

2.1 Aims of the program

The program is necessary because lack of awareness on information security is a recognized control issue. Although the security risks caused by people cannot be totally eliminated, increasing awareness of information security will spread knowledge and thus increase understanding of information security concepts and objectives. Widespread understanding will increase the extent of support and commitment from employees to the rules and motivate them to improve security. Security improvements will both increase compliance and reduce risks, making security breaches less likely and/or less costly, in other words real bottom-line **business benefits**. The logical sequence of events (shown diagrammatically below) illustrates the point that raising security awareness is not an end in itself but is an important a step on the way.



2.2 Overall structure of the awareness program

The program will communicate a range of information security messages in various formats across the organization, focusing on a single information security-related topic every month. By using a monthly sequence of topics, we can keep the program rolling indefinitely, introducing and revisiting a broad range of information security issues from different perspectives. This drip-feed approach is specifically designed to keep introducing interesting and relevant materials, and thus to achieve a sustained, long-term improvement in security awareness.

2.3 Target audience groups

Whilst an awareness program could be designed to address the entire organization homogeneously, a better approach is to focus on distinct groups of employees. We recognize three main audience groups: general employees, executive managers and technologists. Please refer to Appendix A for further information on why we intend to divide the organization in this way.

3 Awareness program content

3.1 Information security topics

An innovative feature of our proposed approach is to concentrate on a different information security topic each month (please refer to **Appendix B** for a list of topics).

Drip-feeding information month-by-month will avoid overwhelming the target audiences with too much information, and allows us to respond dynamically to current information security risks and news, or to introduce new topics in response to emerging security risks (*e.g*. relating to new technology).

The monthly rolling approach also helps keeps the program going indefinitely without overtly repeating the topics (people become acclimatised to messages that are simply repeated, get bored and tend to ignore them). On the other hand, the topics are interrelated, meaning that we may raise an issue one month and revisit it (albeit from another perspective) later: this process acts as a constant reminder to reinforce key information security concepts.

The sequence of topics and their contents are not cast-in-stone at this point but can be adapted according to the needs of the organization. This dynamic approach allows us to respond to information security events and incorporate new topics (*e.g*. different security risks created by new technology) as they arise.

3.2 Types of awareness message

A wide variety of information security messages will be communicated during the course of the program:

- Background information on fundamental information security concepts and issues will be circulated to raise the general level of awareness
- Formal statements of the organization's 'rules' for information security (policies, standards, procedures), plus plain English guidance, will clarify the corresponding responsibilities on employees
- Relevant laws, regulations and best practice standards (*e.g*. data protection/privacy legislation, industry regulations, ISO 17799) will be referenced and summarized where appropriate
- Straightforward guidance on how to comply with policies, standards, laws *etc*. will incorporate practical advice
- News of significant information security breaches will be included where appropriate (we may seek permission to circulate non-confidential information from computer audit reports or other internal security assessments, for example, as well as referencing major external news stories)
- Technical details on specific information security risks plus advice on incorporating appropriate controls into IT systems, procedures *etc*. will help technologists build and maintain secure systems
- Briefings on emerging information security risks associated with new technologies, systems, business relationships, market conditions *etc*. will keep employees up to date
- Case studies demonstrating the design, implementation and use of appropriate information security controls will make the materials appear more relevant and realistic.

3.3 Sources of awareness materials

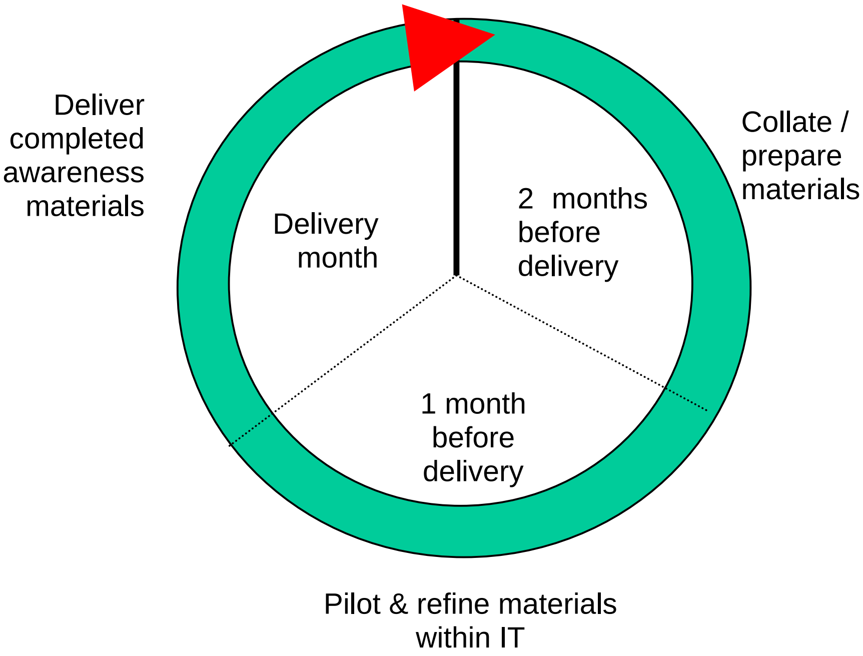
Awareness materials will be derived from several information sources including:

1. Relevant materials already available within the organization (*e.g.* contents of previous awareness programs, internal training courses, information security policies, standards, guidelines *etc*., whether from the Information Security function or other internal sources such as HR)
2. Information security awareness materials from NoticeBored, a monthly information service from British information security consultancy IsecT Ltd. NoticeBored delivers high quality awareness content in the form of newsletters, briefing papers, screensavers, checklists, hyperlinks to relevant Internet resources *etc*. The materials are delivered electronically in formats suitable for inclusion in our awareness program with little effort on our part. For more information, visit www.NoticeBored.com
3. Public information on the Internet *e.g*. news stories about infosec breaches, virus updates, Microsoft, IBM and SANS security briefings *etc*.
4. Materials published by the Government, industry bodies and others *e.g.* laws and regulations, information security surveys, guidelines & booklets on data protection
5. Where necessary, of course, we will create our own materials from scratch.

4 Awareness program methods

4.1 Cyclical delivery process

Monthly delivery of topics (appendix B) naturally suggests a cyclical delivery approach:


Deliver completed awareness materials
Collate / prepare materials
Delivery month
2 months before delivery
1 month before delivery
Pilot & refine materials within IT

At any one point, therefore, activities will be in progress for three different topics in parallel but at different stages. If a new information security risk emerges, we can issue urgent awareness materials more or less immediately and adapt the planned topic sequence to cover the new risk as soon as the materials are ready.

4.2 "Branding"

This concept, borrowed from the world of marketing, is central to our aim to create a deep-rooted security culture. Because the awareness program will use various message delivery mechanisms and will be continuous, we feel it is important to link together the individual elements by branding them. All the awareness materials will be labelled with a logo and use consistent styles and formats to bind them together into a coherent campaign. Employees will soon start to form conceptual links between the awareness materials and overt security messages, as well as gradually gaining an appreciation of the underlying information security goals.

4.3 Creative communication methods

Creativity and diversity in the way we communicate information security messages are important aspects of the awareness program since they increase the chance of getting through to and motivating all our employees. We therefore plan to combine communication methods traditionally used for awareness programs (posters, newsletters *etc*.) with modern electronic methods (*e.g*. intranet, EMAIL, SMS) and other innovative ideas (*e.g*. information security presentations at team meetings and Board meetings).

Please refer to Appendix D for further information on the communications methods.

5 Program management

5.1 Program governance

The organization's Information Security Forum will act as the senior management body responsible for overseeing and steering the program as a whole. Once or twice a year, the program manager (see section 5.2) will deliver formal progress reports and metrics (section 5.4) to demonstrate the effectiveness of the program and the plans (section 5.3) will be reviewed. This business case will be revisited and refreshed at least annually.

5.2 Program manager

We propose to manage the program within the Information Security Management function. The Information Security Manager will nominate or recruit an Information Security Awareness Program Manager to lead the program day-to-day but he/she will rely on advice and assistance from other parts of the organization, including:

- Other information security experts including information security managers, administrators and contacts throughout the organization
- Corporate Communications, Human Resources and Training functions who routinely communicate with employees
- Legal department will be consulted on obvious legal matters and may wish to advise on appropriate forms of words for the most formal awareness materials

5.3 Program plan and major activities

A high-level plan is included at Appendix C. Rather than a one-off awareness-raising project, we are proposing an ongoing (rolling) program to establish and then maintain increased awareness, with the following three activities running in parallel:

- **Prepare/update awareness materials** – Awareness materials will be updated from time to time to reflect the ever-changing information security environment, new technology, new threats and vulnerabilities *etc*.
- **Deliver the program** – through a range of interactive and stimulating communications techniques, we aim to engage and motivate the three audience categories rather than simply broadcasting information "at" them. In practice, we intend to deliver a dynamic stream of awareness materials covering different information security topics each month, supplemented where appropriate with static materials such as information security policies *etc*.
- **Monitor and manage the program** – the effectiveness of the program will be measured through awareness surveys, feedback forms and other means. A progress report containing key statistical information will be presented to management annually to justify continuation of the program, and metrics will be used to manage the program month-by-month

Note: information security awareness activities that are already in progress may continue but will be co-ordinated with, if not gradually absorbed into, the new awareness program.

5.4 Measuring the awareness program

The awareness program will be measured for two reasons: firstly, to help manage and improve the program (*e.g*. identifying and promoting security controls that are not widely supported, or improving the quality of the awareness materials), secondly to justify the organization's investment in the awareness program (*e.g*. we will generate management reports on the program delivery against plan plus statistical data to demonstrate its cost-effectiveness). Measurement criteria and methods similar to those used to track an advertising campaign are shown in the table:

Element	Measurement criteria	Measurement methods
Program delivery (management)	Materials prepared, reviewed & issued on time; cost of preparing and issuing materials, and of managing the program, kept within budget	Conventional governance methods using a defined budget, rolling project plan, specific monthly deliverables and proactive program risk management
Message delivery (brand recognition)	Widespread coverage of each target audience, and strong brand recognition (targets are irrelevant so long as the trend is generally positive month-by-month, at least until the program settles down and achieves real results – see below)	Feedback comments, surveys (potentially including intranet-based surveys and interviews) *etc*. The Information Security intranet website will include on-line quizzes, surveys *etc*. on a more or less continuous basis to test visitors' knowledge of information security issues relating to the monthly topics, and perhaps more general knowledge (*e.g*. refresher questions relating to previous topics, company policies *etc*.). Evaluation scores and feedback comments from those attending awareness activities, presentations *etc*., plus student scores from Computer Based Training courses and other training activities will be collected, collated and analyzed systematically, Occasional structured interviews with managers and staff in various departments will assess their knowledge of information security concepts, and gather feedback comments and suggestions on the awareness program – this information will add to unsolicited comments received by EMAIL *etc*.
Business value (outcome)	This is the most compelling result but the hardest to measure. Indicators that the program is effective would include generalized reductions in information security incidents, and specific reductions linked to monthly topics.	Various, some depending on the topic *e.g*. the trend of virus and network worm incidents should fall after the awareness program covers the "malware" topic

Note: the measurement processes should start as soon as possible in order to create a reliable basis for comparison.

6 Program costs and business benefits

6.1 Program costs

Through this paper, we are requesting the allocation of resources to deliver the awareness program. The main expense will be the Information Security Awareness Program Manager's salary, plus the costs for generating and delivering awareness materials (primarily staffing costs including internal re-charging for the assistance from other corporate functions, plus a subscription to the NoticeBored service). Some additional funds may be needed to purchase additional security awareness materials, external training courses *etc*. The cost estimates are summarized in the table:

Cost element	Estimate
Information Security Awareness Program Manager (salary and recruitment costs)	
Staff to assist Program Manager (from time-to-time, we will draw on the assistance of Information Security, IT, Risk Management, Corporate Communications, HR, Site Security and other functions: some of this may be internally re-chargeable)	
Website costs: authoring software (*e.g*. NetObjects Fusion), hosting, network bandwidth, design/development costs *etc*. (internal web development resources may be available but a professional high-quality look and feel are very important)	
Enterprise license subscription for NoticeBored (electronic delivery of monthly security awareness content in the form of briefing papers, newsletters, presentations, screensavers, checklists *etc*.)	[Consult IsecT for the latest price]
Other sources of information (we will make good use of free Internet resources but may take out subscriptions to information security publications *etc*.)	
Security awareness/promotional activities such as competition prizes, brown-bag meetings, sponsored outings *etc*.	
Printing of hardcopy materials such as posters, leaflets, marketing gizmos *etc*., ideally using in-house printing facilities to achieve consistency and minimize costs (most information will be circulated electronically using EMAIL and the intranet)	
Total estimates	

6.2 Business benefits

The information security awareness program will:

- 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 co-ordinated nor particularly effective
- Communicate and clarify the organization's overall strategic intent to secure its information resources, both to its employees and externally (information security awareness is an essential requirement for ISO 17799 compliance for example)
- Provide general and specific information about information security risks and controls to those who need to know it

- Make staff and managers aware of their respective responsibilities in relation to information security
- Motivate employees to comply with the organization's information security policies, procedures, standards and guidelines, and with applicable laws, thereby increasing compliance in practice
- Create a stronger security culture *i.e.* a broad understanding of, and demonstrable commitment to, information security right across the organization (this may even enhance our brand)
- Help improve the 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. This will reduce costs both directly (*e.g.* data damaged by viruses) and indirectly (*e.g.* less need to investigate and resolve breaches) [**These are the main financial benefits of the awareness program**]
- Facilitate disciplinary or legal action against people who deliberately break the information security rules (ignorance will no longer be a reasonable defence)

6.3 Conclusion

In line with our increasing dependence on high quality, up-to-date and complete information to manage the business, information security has become crucially important to us. In the face of increasingly sophisticated technologies and risks, it is vital that employees are aware of, and comply with, their evolving information security obligations. The information security awareness program described in this proposal will strengthen the weakest link in our security infrastructure, our people, and create a stronger security culture. We welcome your support.

6.4 References

- "Information Security Policies, Procedures, and Standards" book by Tom Peltier
- "The Art Of Deception" book by Kevin Mitnick
- "Building An Information Security Awareness Program" book by Mark Desman
- "Building an Information Technology Security Awareness and Training Program" NIST Special Publication 800-50
- "Marketing Management" book by Philip Kotler
- www.NoticeBored.com website describes the NoticeBored information security awareness service from IsecT Ltd.
- "Implementing User Security Awareness Training" paper by Kelly Allison
- "Security Awareness – Are Your Users 'clued in' or 'clueless'?" paper by Robert Held
- "Implementing a Security Awareness Training Program in Your Environment for Every Day Computer Users" paper by Kelly Nichol
- "Social Engineering Fundamentals, Part I: Hacker Tactics" and "Part II: Combat Strategies" papers by Sarah Granger

Appendix A – Target audience groups

Group	Reason for grouping	Members
General employees	Prime targets for the awareness program are the people who use our IT systems, handle corporate/personal information or control IT assets. In practice, this means practically everyone within the organization (including those in the next two groups), and perhaps some others (such as contractors and consultants working for us). Managing information may or may not be a central part of their daily working lives but we believe everybody has a part to play in the information security culture. We will update the information security content for the new employee induction process, for example, and introduce a refresher program. All employees will be encouraged to keep track of information security policies and issues through general awareness materials, and will in future be required to acknowledge their acceptance of information security responsibilities formally once a year. Wide coverage will reduce the chance that anyone can reasonably claim to be ignorant of their information security responsibilities and/or the rules: demonstrable awareness of the organization's information security rules is vital if we are to take disciplinary or legal action following an breach.	Practically all our employees plus contractors, consultants *etc*. working on our premises Membership includes everyone in the two remaining groups
Executive managers	Staff look up to their team leaders, supervisors, junior/middle/senior managers and executive directors for direction and guidance in all sorts of areas. In the case of information security, managers should openly demonstrate their commitment and support for the system of controls, implying the need to inform them about the controls and their obligations (naturally, it is important that managers comply with information security rules). Furthermore, managerial oversight is itself an important class of information security controls, so managers need to be aware of their governance responsibilities including monitoring and supporting their subordinates.	Management from the CEO to team-leader level Some items may be circulated more narrowly *e.g*. to specific directors or managers
Technologists	This category includes IT network and systems managers, application developers, information security administrators, computer auditors, "power users" (end-users who develop and share spreadsheet and database applications *etc*.) and various others. Technologists are largely ignored by traditional information security awareness activities yet we expect them to understand, implement and operate most of our technical security controls. The awareness program will redress the balance through technical briefings, white papers and possibly training courses. Technical details relating to design and operation of information security controls will be most relevant to these people. Improved understanding of information security will help persuade technologists to incorporate appropriate technical controls in systems they build and operate, and make use of controls in systems they use.	Most IT/technical staff especially IT operations, developers and others with obvious information security responsibilities. Also "power-users" within the business Some sensitive or highly-detailed items may be circulated more narrowly

Note: over time, we may further subdivide the audience for more specific communications but we feel these three categories are a good starting point.

Appendix B – Potential information security awareness topics

Topic	Outline content
Launch	Introduce the awareness program, explain the objectives, outline the importance of information security as everyone's job
Malware	Viruses, worms, Trojans
Confidentiality	Secrecy, access control, privacy, encryption, ID theft
Availability	QA, backups, contingency & DRP, high-availability, DDoS, maintenance & support, critical staff, SLA
Integrity	Data/systems/personal integrity & trust, validation, authorization
Mobile working	Security for wireless and mobile devices, PDAs, wLANs; physical security & backups
Ownership	Data and system ownership concepts – custodianship, duty of care, responsibility, accountability
Internet security	WWW, EMAIL, Java/script, webserver, DNS, DDoS, worms, fraud, domain name hijacks & trademark protection
Software copyright	Licensing, piracy freeware, shareware, IT procurement controls
[IT] Fraud	Fraud indicators, holiday cover, whistleblowers, Divisions of Responsibility (4 eyes), expenses, training facilities
EMAIL security	Libel/slander, personal use, disclosure, contracts, monitoring
Personal data	DPA, HIPAA *etc*., privacy, ID theft
Contingency	DCP, BCP, incident response (intro), crisis planning, preparation, testing
Human element	Explain the need for policies, procedures and awareness to supplement technical controls
Accountability	Authentication, audit records/logs, responsibility, delegation
Incidents	Incident identification, reporting & response, forensics, DCP, dealing with the Press, legal aspects
Physical security	Perimeter & layered protection, value of data *vs*. kit, asset management, physical intrusion alarms & locks
Standards	ISO17799 *etc*. *etc*. – structure, common criteria, utility, certification process, business value
(Computer) audit	Independent review, non-financial, value & security controls; audit trails and built-in application audit functions
Governance	IT governance in relation to general business governance; intro to risk management
Risk management	Risk assessment, risk analysis, risk reduction, risk mitigation – primarily in an IT security context
Hacking	Hacking *vs*. cracking, malicious/curious intent, opportunistic/pre-planned, coordinated attacks, know your enemy
Change mgmt	Techniques for managing & controlling system changes, integrating security & change mgmt, patching
Bugs!	Secure programming tips for technologists & end-users; development methods & QA; evaluating & testing software

Note: The list is liable to change in practice to reflect emerging information security risks and issues, new technologies *etc*., both the content and the (implied) delivery sequence.

Appendix C – Outline program plan

(Insert your high-level one-page GANTT chart or equivalent here)

Appendix D – Communications methods

There are many different ways to get the information security messages across to employees and indeed we intend to use a wide range of communications methods, *but not all at once* – in practice, the choice depends largely on accepted practice for the intended audience and the specific message content. Where possible, we will work with IT, HR and Corporate Communications to use existing communications vehicles. The following list of communications methods is not exhaustive:

- The **Information Security website** on the corporate intranet will be a focal point for the awareness program, and will expand month-by-month into a useful reference resource. It is therefore important that the site is widely accessible throughout the organization, and is well organized and engaging. The branding and monthly topic themes will be reflected on the website. The website will contain or reference information policies, standards and guidelines (see below). It will include information security news stories and case studies, plus Information security competitions, quizzes, polls and tests. A resources section will include hyperlinks to other related Internet/intranet websites, and we will seek reciprocal links back to this intranet website from others through promotional banners *etc*. The website will solicit feedback from users and may include moderated bulletin-board facilities to encourage discussion of information security topics.

- **Written materials** such as information security newsletters, handouts, leaflets, brochures, white papers (technical briefings and reports), posters, security alerts *etc*. will either be EMAILed or printed and distributed. Such information will either be sent to all employees or to defined distribution lists or individuals, and may be cascaded internally through the organization structure. There will also be a regular information security column in the staff magazine.

- **Physical security materials** will be updated to incorporate information security messages *e.g.* warning notices saying “This is a secure facility: we conduct random spot-checks for unauthorized information and IT equipment”; information security messages will be printed on the rear of the standard staff pass.

- **Information security policies, standards, procedures and guidelines** – in conjunction with others, we will prepare/review/refresh and publicize the formal materials, most likely through a formally-controlled area on the intranet. Items related to the monthly awareness topic will be specifically updated and highlighted.

- **Face-to-face meetings, presentations and seminars** *e.g.* team briefings, “brown bag sessions” (working lunches), traveling conference-style promotional stands and possibly a security fair. Rather than ‘death by PowerPoint’, we plan to deliver a series of succinct seminar sessions on specific topics that will aide understanding, stimulate discussion, encourage interaction and persuade attendees to act appropriately. Led by information security managers, other professionals and pre-briefed managers (possibly including external speakers), the presentations will incorporate case studies and news to bring home the realities of information security.

- **Training courses** are appropriate for in-depth education on certain topics. Rather than sending all employees through generic ‘sheep-dip’ training, selected employees will be eligible for specific information security training provided this is necessary and directly relevant to their job roles and responsibilities. Wherever possible, we will use internal training resources to contain the costs, and will cooperate with HR to analyse ‘training needs’. Information security awareness materials will also be incorporated into Computer Based Training, either through specific information security training modules or by incorporating information security messages into other training courses where appropriate (*e.g.* advice on information security risk assessment and security design to be included in courses for software developers).

- **Induction sessions** for new employees or those recently promoted will incorporate a selection of appropriate security awareness materials lifted from the main awareness program. The induction materials will be updated every quarter or so, rather than becoming stale. We also plan to contact new employees individually in their first few weeks by phone or EMAIL to offer further assistance, invite them to awareness presentations *etc*. and draw them into the program.

- **Security awareness events and activities** – information security tends to be quite esoteric and a rather dry subject, but we will introduce quizzes, prize competitions, group outings and various other creative activities to liven things up. Whilst we must avoid trivializing the subject, gentle humor and fun will help put the information security messages across. Certificates of achievement and relevant prizes/incentives will help.
- **Promotional "gizmos"** such as stickers, mouse mats, mugs, pens, reminder cards, bookmarks, lapel pins *etc*., each printed with succinct information security messages, will be used to launch and promote the security awareness 'brand'.
- **Reference materials** – information security videos, books, journals, interactive presentations and other resources – will be made available through the company library and promoted in the awareness newsletters *etc*.
- **System messages** – we propose using the screensaver to display information security presentations on the monthly awareness topics, provided it can be updated automatically at low cost on most if not all desktops. Appropriate security awareness messages can also be incorporated into system login banners, desktop backgrounds, application messages, help text *etc*.
- **Voicemail broadcasts and SMS messaging** may also be used where appropriate, particularly to communicate messages relating to securing the telephone system.
- **An information security suggestion scheme** will be introduced once the awareness program is established to solicit improvement suggestions and feedback.
- **Liaison with Internal Audit, Risk Management, HR and Site Security** will help align related activities *e.g*. physical site security reviews and quarantining of sensitive items left unprotected (to coincide with the physical security topic); logical network security reviews with follow-up on sensitive items left unprotected (network security topics). Selected non-sensitive information from management reports on security incidents, audits and other reviews may be circulated through the awareness program *e.g*. as case studies, and we will use statistical data to reinforce the importance of the program.
- **Departmental contacts**: we will use a human network of departmental information security contacts to disseminate key information security messages and channel feedback comments from staff back to Information Security Management. Most departments have already nominated contacts for security administration purposes – using the network for security awareness is a natural extension.