



Innovative information security awareness programs

Business Case for an Information Security Awareness Program

Updated: 3rd June 2010

Executive summary

This paper lays out the case for investing in an innovative continuous security awareness program. By informing and motivating people, the program will create a strong security culture, improve security compliance and cut net costs.

The awareness program will address general employees, managers and IT people through three parallel streams of awareness material. Fresh materials will be circulated every month, continuously promoting and reinforcing information security while covering a succession of important topics.

The program will be managed by a dedicated Information Security Awareness Manager (ISAM) under the leadership of the Information Security Manager, and delivered with the assistance of other corporate functions as necessary.

Security awareness metrics will be used to manage and prove the cost-effectiveness of the program. 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 program costs (primarily the ISAM's salary).

Copyright © 2010 Isect Ltd.

The generic paper may be freely distributed in Adobe PDF format provided that it remains completely intact and unaltered, including this copyright notice. It must not be sold or incorporated into any other product. Please contact Isect Ltd. directly for an editable MS Word version of this paper. The Word version **must not** be distributed further.

To contact Isect Ltd., telephone: +64 6874 3344
email info@isect.com or visit www.NoticeBored.com

Contents

1	Introduction	3
1.1	Background.....	3
1.2	Purpose of this paper.....	3
1.3	Document approval.....	3
2	Awareness program overview	4
2.1	Aims of the program	4
2.2	Overall structure of the awareness program.....	4
2.3	Target awareness audiences.....	5
2.4	Management, delivery and monitoring of the awareness program.....	5
3	Awareness program content.....	6
3.1	Information security topics	6
3.2	Creative awareness techniques.....	6
3.3	Sources of awareness materials.....	7
4	Security awareness methods.....	8
4.1	Creative communication methods	8
4.2	Information Security's intranet website – the Security Zone.....	8
4.3	Branding	8
4.4	New employee orientation/induction training	8
5	Program management	10
5.1	Program governance	10
5.2	Information Security Awareness Manager (ISAM).....	10
5.3	Program plan and major activities	10
5.4	Measuring the awareness program	11
6	Cost benefit analysis	12
6.1	Program costs.....	12
6.2	Business benefits.....	13
6.3	Conclusion	13
6.4	References/further reading.....	14
	Appendix A – Target audience groups	15
	Appendix B – Potential information security awareness topics	16
	Appendix C – Outline program plan.....	18
	Appendix D – Communications methods.....	19

1 Introduction

1.1 Background

Information is a fundamental asset to the business. Security (that is 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, employees comply with the information security policies, standards, laws and other regulations but being human, they occasionally forget and sometimes make mistakes, such as sharing passwords and neglecting to take regular backups. Some let visitors roam about the offices unescorted, give out sensitive information over the phone and lose corporate laptops containing sensitive information. These are not merely theoretical examples but typical 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/industrial espionage, 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 improve information security policy compliance, reduce risks and hence cut costs.

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

1.3 Document approval

Name	Role/Position	Signed	Date
	Chief Executive		
	Chief Information Officer		
	Chief Information Security Officer		
	Information Security Manager		

2 Awareness program overview

2.1 Aims of the program

An information security awareness program is necessary to address 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 above) makes the point that raising security awareness is not an end in itself but an important a step on the way to the ultimate objective, reducing information security risks and costs.

2.2 Overall structure of the awareness program

The program will exploit NoticeBored, an innovative security awareness product from IsecT Ltd. NoticeBored delivers a range of high quality awareness materials covering a different information security topic every month. This monthly sequence keeps the program rolling indefinitely, introducing and later revisiting a broad range of information security issues from different perspectives. The continuous drip-feed of interesting and relevant awareness materials is designed to build and maintain a sustained, long-term improvement in security awareness, leading to a deep-rooted and widespread “security culture” throughout the organization.

This rolling approach contrasts markedly with traditional security awareness programs that have typically relied on an annual awareness/training session for all employees. Experience has shown that once-a-year awareness training sessions are simply not effective in practice: employees soon forget the security messages and return to their old ways, if indeed they even attended and responded to the training in the first place. It is disruptive and expensive to put large numbers of employees through such events. On top of that, the format severely constrains the amount of information that can sensibly be conveyed, meaning that much of the content appears irrelevant and/or annoying to attendees and doesn't stick.

2.3 Target awareness audiences

While awareness programs have traditionally addressed the entire organization homogeneously, it is better to focus on distinct groups of employees, reflecting their different security awareness requirements, backgrounds and needs. We recognize three target audience groups, namely (1) employees in general, (2) managers and (3) information technologists. [Appendix A](#) explains why we choose to divide the organization in this way.

2.4 Management, delivery and monitoring of the awareness program

The program will be run by an Information Security Awareness Manager (ISAM), reporting to the Information Security Manager.

We are planning to use a range of employee communications methods such as presentations, training sessions, facilitated seminars and quizzes/competitions, supplemented by posters, written briefings *etc.* circulated by email, intranet or on paper. The ISAM will work in conjunction with other corporate functions such as HR, Training, Internal Communications, Risk Management, Compliance/Legal and IT.

Using the pre-written security awareness content from NoticeBored will allow the ISAM to focus primarily on interacting with employees rather than having to research and write the awareness materials entirely from scratch. There is more on the awareness content in [section 3](#).

Metrics derived from measurement techniques such as surveys (described further in [section 5.4](#) below) will be used to report progress to management and adjust the awareness program as necessary. We intend to deliver a self-sustaining, continuously improving program.

3 Awareness program content

3.1 Information security topics

An innovative feature of our proposed approach is that we will concentrate on a different information security topic each month. A list of topics is presented in [Appendix B](#).

The monthly approach keeps the program rolling indefinitely and avoids employees becoming acclimatized to/bored with awareness messages that are simply repeated. At the same time, all the monthly topics relate to information security, constantly reinforcing key information security concepts such as confidentiality, integrity, availability, risk and control. The idea is to build and then sustain a higher level of security awareness.

The sequence of topics and their contents are not cast-in-stone but can be adapted dynamically according to the needs of the organization. This approach allows us to respond to information security events and incorporate new topics as they arise, and the program as a whole will gradually mature as time goes on.

3.2 Creative awareness techniques

Modern security awareness programs involve much more creative approaches than the posters and training sessions of old. Our awareness program will employ a variety information security awareness materials and methods:

- Information security policies and standards will formally clarify the organization's security rules for staff, managers, technologists, contractors, consultants *etc.*
- Relevant laws, regulations and best practice standards (e.g. data protection/privacy legislation, industry regulations, ISO/IEC 27001) will be referenced and integrated
- Straightforward plain English guidelines and procedures will advise employees on how to comply with the corporate policies, standards, laws *etc.* in practice
- Background information on fundamental information security concepts and issues, including newsletters, posters and screensavers on the monthly themes, will be used to promote the 'information security brand' (see [section 4.3](#))
- News of significant information security incidents will be included where appropriate. We may seek permission to circulate information from audit reports or other internal security assessments, for example, as well as referencing major stories from the information security and general news media. Incidents are an important element of the awareness program since people commonly underestimate or discount information security risks
- 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 staff, managers and technologists up to date with their respective interests
- Realistic case studies and presentations will make the topics more relevant to employees, and will be used to stimulate group discussion

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. information security awareness and training materials developed previously, information security policies, standards, guidelines *etc.*, whether from the Information Security function or other internal sources such as Site/Building Security, HR and Legal)
2. NoticeBored, an awareness product delivered to subscribers by information security awareness specialist IsecT Ltd. NoticeBored delivers high quality awareness content in the form of seminar presentations, newsletters, briefing papers, screensavers, checklists *etc.* The NoticeBored materials are supplied electronically in formats suitable for editing and inclusion in our awareness program with little effort on our part. Please visit www.NoticeBored.com for more information.
3. Public information on the Internet e.g. news stories about information security 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 and booklets on data protection
5. Where necessary, of course, we will create our own supplementary materials from scratch.

4 Security awareness methods

4.1 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. facilitated information security seminar presentations at team meetings and Board-level discussions).

Please refer to [Appendix D](#) for further information on the communications methods.

4.2 Information Security's intranet website – the *Security Zone*

Information Security's intranet website is central to our employee communications approach. We will be revising and restructuring the existing site to create a "Security Zone" whose primary purpose is security awareness.

Through the Security Zone, current information security policies, standards, procedures and guidelines will be made available in one place to all employees. Approved new or revised policies *etc.* will be available instantly throughout the organization.

Fresh awareness materials will be added to the Security Zone every month, highlighting a succession of information security topics, policies *etc.* The engaging stream of new materials, news stories, competitions and so forth is designed to interest, inform and motivate the audiences. We aim to get employees to visit the Security Zone at least once a month.

In time, we may also use other social media such as blogs, wikis *etc.* to support the intranet website.

4.3 Branding

Because the awareness program will use various message communications methods over the long term, we will link the individual elements together through branding. This concept, used extensively in marketing, directly supports our aim to create a deep-rooted and all-encompassing security culture.

All the awareness materials will use the same logo. Consistent styles and formats will form a coherent and recognizable campaign theme. Employees will soon form conceptual links between the awareness materials and overt security messages, as well as gaining a deeper appreciation of the underlying information security goals. In time, information security will become an accepted part of the daily routine - business as usual, or 'the way we do things here'.

4.4 New employee orientation/induction training

An appreciation of the organization's information security values, policies and practices is an important part of introducing new employees to the organization.

We cannot safely assume that new people are sufficiently security-aware when they join up. While they *may* know about their obligations under applicable laws and regulations (e.g. copyright, privacy), they are unlikely to have seen our corporate security policies, standards, procedures *etc.* Therefore, new employee orientation or induction training in security is a necessity to ensure their understanding and compliance. It will also introduce new recruits to the information security people, helping to make them more approachable.

We will establish a standardized security orientation/induction course that can be delivered to all employees soon after they start work. In about half an hour or so, the session will cover the basics of information security, things such as:

- General security compliance obligations resulting from legal, regulatory and corporate requirements;
- Where to find security policies *etc.*, in other words the Security Zone;
- Choosing strong passwords and keeping them secret – an introduction to social engineering;
- Proper use of antivirus software and other important technical security controls, and responsible use of the IT network systems, email and the Internet;
- Reporting security incidents and near misses promptly through the IT Help/Service Desk.

The orientation/induction session will be based around a NoticeBored module designed for this purpose, and covering a limited range of basic information security topics. Essentially the same materials will be used to support the launch of the awareness program, bringing the whole organization quickly up to speed on the security basics.

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 awareness program as a whole. Once or twice a year, the ISAM (see [section 5.2](#)) will review the awareness program plans ([section 5.3](#)) and deliver formal progress reports and metrics ([section 5.4](#)) to the Forum, demonstrating the effectiveness of the program and discussing developments.

5.2 Information Security Awareness Manager (ISAM)

We propose to manage the program within the Information Security Management function. The Information Security Manager will nominate or recruit a full/part-time Information Security Awareness Manager (ISAM) to lead the program day-to-day, taking advice and assistance from other parts of the organization, including:

- Other information security and IT experts including information security managers, administrators and contacts throughout the organization (such as Risk Management, Compliance and IT Audit);
- Corporate Communications, HR 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 more formal materials such as policies.

5.3 Program plan and major activities

A high-level program plan is included at [Appendix C](#). In summary, the plan is as follows:

- **Update Information Security's intranet Security Zone** – the intranet website will be revised and re-launched to become the focal point or shop window for security awareness. The site will be updated regularly to reflect the monthly awareness topics, and will become the definitive source of reference materials for information security including policies, standards, procedures and guidelines. Security awareness materials such as the briefings, presentations, crosswords and a hyperlinked information security glossary will be made available to all employees through the Security Zone.
- **Update/prepare the awareness materials** – each month, a fresh 'module' (ZIP file) containing new NoticeBored security awareness materials will be received through the Internet. The NoticeBored materials are camera-ready with only minor customization required by the ISAM (e.g. applying the security awareness branding/logo, checking against and aligning with existing corporate security policies, entering contact details for the ISAM or Information Security Manager, and incorporating proprietary awareness content). Existing information security awareness materials and activities that are already in progress will gradually be absorbed into and superseded by the new awareness program.
- **Deliver the awareness materials** – through a range of interactive and stimulating communications techniques, we aim to engage and motivate the three audience groups using the awareness materials, rather than simply broadcasting information at them. Materials will be delivered in person, on paper, by email and on the intranet. A paper suggesting creative awareness activities relating to the topic at hand is provided in each NoticeBored module. *This will be the main part of the awareness program.*
- **Monitor and manage the program** – the effectiveness of the program will be measured through awareness surveys, feedback forms and other means (see [section 5.4](#)). 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 and improve the program month-by-month.

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
<p>Program delivery (management)</p>	<p>Materials prepared, reviewed & issued on time; cost of preparing and issuing materials, and of managing the program, kept within budget</p>	<p>Conventional governance methods using a defined budget, rolling project plan, specific monthly deliverables and proactive program risk management</p>
<p>Message delivery (brand recognition)</p>	<p>Widespread coverage of each target audience, and strong brand recognition (this is a leading indicator: the trend should be generally positive month-by-month, at least until the program settles down and achieves real results – see below)</p>	<p>Feedback comments, surveys (potentially including intranet-based surveys and interviews) <i>etc.</i> The Security Zone will provide on-line quizzes, surveys <i>etc.</i> 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 <i>etc.</i>). Evaluation scores and feedback comments from those attending awareness activities, presentations <i>etc.</i>, will be collected, collated and analyzed systematically. Page view and visitor statistics from the Security Zone will demonstrate the popularity of the site as a whole and may be used to ask more detailed questions about specific security topics and materials (e.g. “How many people have accessed the contingency planning materials in the past year?”). 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 <i>etc.</i></p>
<p>Business value (outcome)</p>	<p>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 awareness topics.</p>	<p>Various, some depending on the topic e.g. the trend of virus and network worm incidents should fall but the number of associated Help/Service Desk calls should rise after the awareness program covers the “malware” topic</p>

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

6 Cost benefit analysis

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 ISAM's time, 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). The cost estimates are summarized in the table:

Cost element	Notes	\$ estimate
ISAM salary	Whether this is a full- or part-time rôle depends largely on the size of the organization and the important of information security relative to other priorities.	<i>X man-days per annum at \$? per man-day</i>
Information Security intranet website redesign	The "Security Zone" is a central feature of the awareness program. We need to set aside some funds to redesign and relaunch the site. Thereafter it will be managed by the ISAM.	<i>\$?</i>
Security awareness materials	Existing awareness materials will be supplemented by those from NoticeBored and other sources (e.g. professional information security magazines)	<i>NoticeBored subscription*</i>
Promotional materials	Branded coasters, pens, prizes for information security tests, quizzes and competitions, coffee for brown-bag meetings etc.	<i>Promo & prize fund!</i>
Printing	Most awareness information will be circulated electronically using email and the intranet but some hardcopies will be required (e.g. posters).	<i>Color printer or printing service</i>
Contingency	Further funds may be needed to purchase additional security awareness materials, external training courses etc.	<i>Add ~20%?</i>
Total budget request		<i>Total the above</i>

* Contact IsecT for a NoticeBored price quotation for your organization.

6.2 Business benefits

We believe information security is a bit like having brakes on a vehicle: yes, they slow you down but they also make it safer for you to go faster. **Information security lets us do business more safely in today's interconnected and complex world.**

The information security awareness program, specifically, 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 coordinated 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/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 organization's information security policies, procedures, standards and guidelines, and with applicable laws, thereby increasing compliance in practice;
- Create a strong 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 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 (*e.g.* data damaged by viruses; sensitive information disclosed; compliance failures leading to fines *etc.*) and indirectly (*e.g.* less need to investigate and resolve breaches) [**The main financial benefits of the awareness program are here**];
- Facilitate disciplinary or legal action against people who deliberately break the information security rules (ignorance will no longer be a reasonable defense).

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, by creating a deep-rooted security culture. We welcome your support both for the investment proposal and for the program itself.

6.4 References/further reading

- [“Managing an Information Security and Privacy Awareness and Training Program”](#) book by Rebecca Herold (highly recommended for the ISAM)
- [“Spies Among Us”](#) book by Ira Winkler (highly recommended for managers)
- [“Information Security Policies, Procedures, and Standards”](#) book by Tom Peltier
- [“The Art Of Deception”](#) book by renowned hacker/social engineer 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
- [ISO/IEC 27001 and 27002](#) ISO standards for information security management systems
- [www.NoticeBored.com](#) describes the security awareness product from IsecT Ltd.
- [“The True Value of Information Security Awareness”](#) white paper by Gary Hinson
- [“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

Appendix A – Target audience groups

Group	Reason for grouping	Members
General employees	<p>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 a breach.</p>	<p>Practically all our employees plus contractors, consultants <i>etc.</i> working on our premises. Membership includes everyone in the two remaining groups. Awareness materials based on those in this stream may also be disseminated to customers and other relevant third parties via Marketing/PR.</p>
Managers	<p>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 themselves understand and comply with their information security obligations). 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.</p>	<p>Management from the CEO to team-leader level. Some items may be circulated more narrowly <i>e.g.</i> to specific directors or managers.</p>
Technologists	<p>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 <i>etc.</i>) 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.</p>	<p>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.</p>

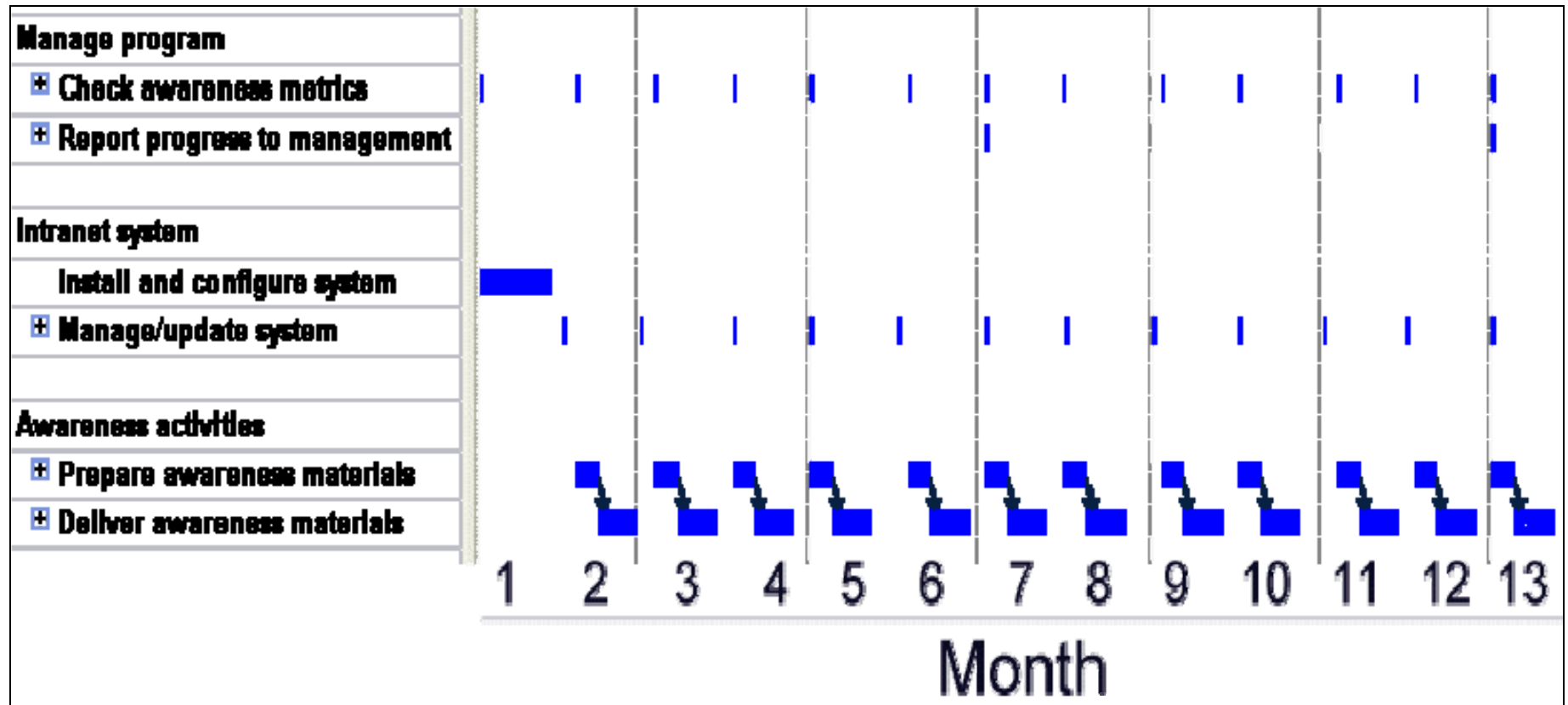
Appendix B – Potential information security awareness topics

Topic	Outline content
Accountability and responsibility	Examines and explains these two commonly misunderstood concepts in an information security context. What are common roles and responsibilities relating to information security?
Authentication and ID management	Everything from choosing strong passwords to smart cards, biometrics and access control.
Bugs!	Errors/flaws in program specification, design, coding or configuration by software development professionals and end-users can create significant security vulnerabilities.
Change management	Security aspects of IT-related changes including patching, testing and configuration management.
Compliance	... with relevant laws, regulations and standards such as copyright, privacy, ISO/IEC 27000-series, ITIL <i>etc.</i>
Confidentiality	All about keeping sensitive corporate and personal information private.
Contingency management	Planning for success by preparing to cope with the worst. Includes Disaster Recovery Planning, and more.
Cryptography	Covering encryption, digital signatures and other applications of cryptography and cryptanalysis (but no heavy mathematics!).
Database security	Securing large collections of valuable data against hackers, corruption, loss <i>etc.</i>
Digital forensics	Obtaining, securing and analyzing digital data from scenes-of-crime and internal security incidents.
Ethics	Explores the ethical and moral side of information security, going beyond the written rules of society.
Gizmos	Security aspects of portable IT devices: cellphones, USB sticks, PDAs and more.
Governance	The framework within which information security is managed, such as rôles and responsibilities.
Hacking	Tips to counteract hackers, crackers, industrial spies, fraudsters, criminals and other adversaries.
Human factors	What makes employee awareness an essential supplement to technical information security controls?
Identity theft	Based on user authentication topics (such as passwords and multifactor authentication), this module focuses specifically on identity theft methods such as phishing and counterfeiting of credentials.
Incident management	Reacting to, containing, resolving and learning from information security events, incidents and near-misses.
Information security 101	Introduce the awareness program, explain the objectives, confirm that information security is everyone's responsibility. This topic will form the basis of the information security element of induction/orientation training for new employees.
Information security risk management	Explains the processes of analyzing and controlling/managing information security risks.
Insider threats	Covering the security threats created by employees and others working in a similar capacity.

Topic	Outline content
Intellectual Property Rights	Protecting our own IPR and respecting the rights of others, through copyright, patents, trademarks <i>etc.</i>
IT auditing	Understand what makes IT auditors tick, what they do and how to work with them most effectively.
IT governance	Controlling and minimizing IT risks forms an integral and vital part of corporate governance.
IT-related fraud	About frauds committed with and exploiting computer systems and IT networks.
Malware	Viruses, worms, Trojans, key loggers, spyware, rootkits and more.
Mobile and home working	Information security considerations for road warriors and those working from home.
Network & Internet security	All manner of information security issues linked with networking in general and the Web in particular.
Network & systems management	Processes for securely installing, configuring, monitoring and managing IT.
Office & email security	Considers information security issues in a typical office/corporate setting, including those associated with electronic mail and similar personal messaging services.
Privacy	Focuses specifically on the protection of data and other forms of information about individual, identifiable people.
Physical security	Protecting corporate facilities against unauthorized access, fires, floods, overheating, power disturbance, lightning ...
SCADA/ISC security	While this may appear relevant only in an industrial context, we will point out the security risks associated with embedded controllers in buildings, machinery and vehicles.
Software development	Integrating information security into the system development lifecycle from initial specification and design through testing and configuration to use, maintenance and eventual retirement.
Social engineering	Covers social interaction techniques used by unethical hackers and competitors to manipulate people into disclosing sensitive information.
Social networking	The security aspects of Web 2.0, Facebook, Twitter, LinkedIn, blogs and other social media.
Third parties	Information security issues resulting from the increasing interconnectedness of modern business <i>e.g.</i> sharing information through Non Disclosure Agreements and auditing third party connections for evidence of suitable security controls.
Trade secrets	Covering a spectrum of activities ranging from competitive intelligence to information warfare.

Note: The list of about 30 topics is liable to change in practice to reflect emerging information security risks and issues, new technologies *etc.* In some months, we may cover additional related topics. The full cycle of topics repeats every two or three years but will of course be updated to reflect current risks. Every topic reinforces fundamental information security concepts such as confidentiality, integrity, availability, risk, control, governance, compliance *etc.*, while a number of core topics (such as passwords, Internet security, malware and social engineering) will be covered annually.

Appendix C – Outline program plan



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 Security Zone**, Information Security's intranet website, will be the centerpiece of the awareness program. Month-by-month the site will expand into a useful source of information and advice on information security. It will be the definitive location for information security policies, standards, procedures and guidelines. The program branding and monthly topic themes will be reflected in the Security Zone. Items related to the monthly awareness topic will be specifically updated and highlighted, including information security news stories and case studies, plus information security competitions, quizzes, polls and tests. A resources section will have hyperlinks to other related Internet/intranet websites, and we link to the information security website from other relevant intranet sites. We 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.
- **Face-to-face meetings, presentations and seminars** e.g. team briefings, facilitated seminars, 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. Extensive speaker notes will be provided (part of the NoticeBored delivery).
- **Training courses** are appropriate for in-depth education on certain topics. Selected employees (e.g. help desk staff, receptionists, security guards, development project managers) 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 analyze 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/orientation 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 regularly to avoid 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.
- **Physical security materials** will be updated to incorporate relevant messages e.g. warning notices saying "This is a secure facility: we conduct random spot-checks for unauthorized information and IT equipment"; similar security messages will be printed on the rear of the

standard staff and visitor passes. We will liaise directly with facilities management on these materials and ensure consistency across all our sites.

- **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 freebies** 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. We will also offer worthwhile security-themed prizes as inducements for the security awareness competitions/quizzes *etc.* (the Information Security 101 module proposes a suite of gold-silver-bronze level awards).
- **Reference materials** – information security videos, books, journals, interactive presentations, Computer Based Training and other resources will be made available through the company library and promoted in the awareness newsletters, training courses, presentations *etc.*
- **System messages** – we propose to introduce a standard screensaver displaying awareness presentations on the monthly information security topics. Over time and by cooperating with the system/network administrators and application developers, appropriate security awareness messages will 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 champions or ambassadors 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 to assist with security awareness is a natural extension of their rôle.