Business case for an

Information Security Awareness Program

July 2016

Summary

This paper makes the case for investing in a continuous (rolling) security awareness program. By informing and motivating our people to think and act more securely, the program will create a strong security culture, improve security compliance and cut costs.

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

Business case for an information security awareness program

Background

Information is a valuable yet vulnerable business asset. 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 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. 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.* ransomware) and targeted (*e.g.* information theft/industrial espionage, fraud, extortion and targeted Denial of Service attacks).

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

Purpose of this paper

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

We propose an ongoing, continuous or rolling internal communications program designed to raise awareness of information security concepts, requirements and controls among staff, managers and specialists within the organization.

By (a) informing workers about relevant information security matters and (b) motivating them to think and behave more securely, we will establish a widespread, lasting and deep-rooted **security culture.** That in turn will:

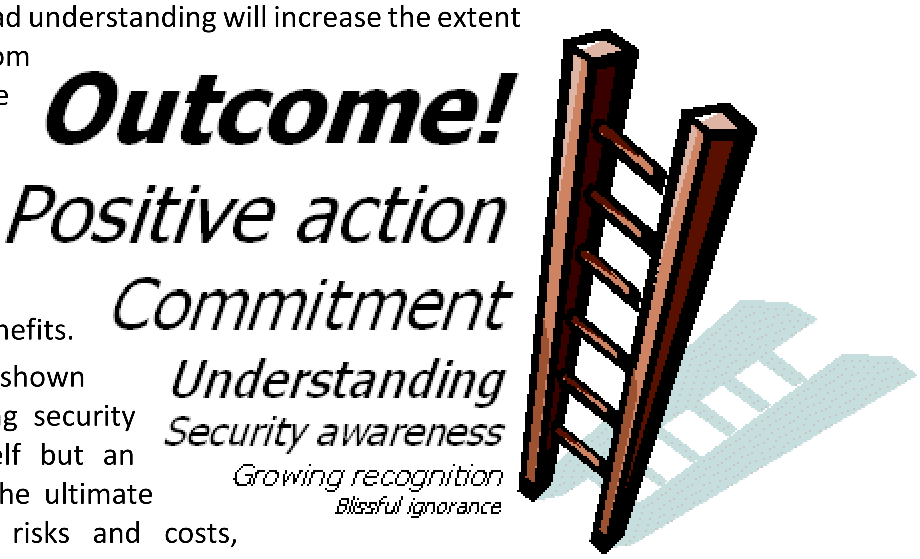
- Improve compliance, reduce information risks and increase assurance;
- Maximize the intended effects and benefits of other information security controls;
- Minimize the number and severity of incidents, cutting costs.

It is obvious from the news headlines that inadequate security awareness can prove *very* costly for any organization. We are assaulted on a daily basis by numerous cybersecurity issues such as phishing, malware, hackers and software bugs. We face insider threats ranging from inept workers who accidentally expose or damage valuable business and personal information, to fraudsters and industrial spies in our midst. Our suppliers, business partners, customers, authorities and competitors don't necessarily share our interests and concerns, while the damage caused by the loss of knowledge workers, or trusted workers who turn out not to have been trustworthy, may be literally impossible to repair.

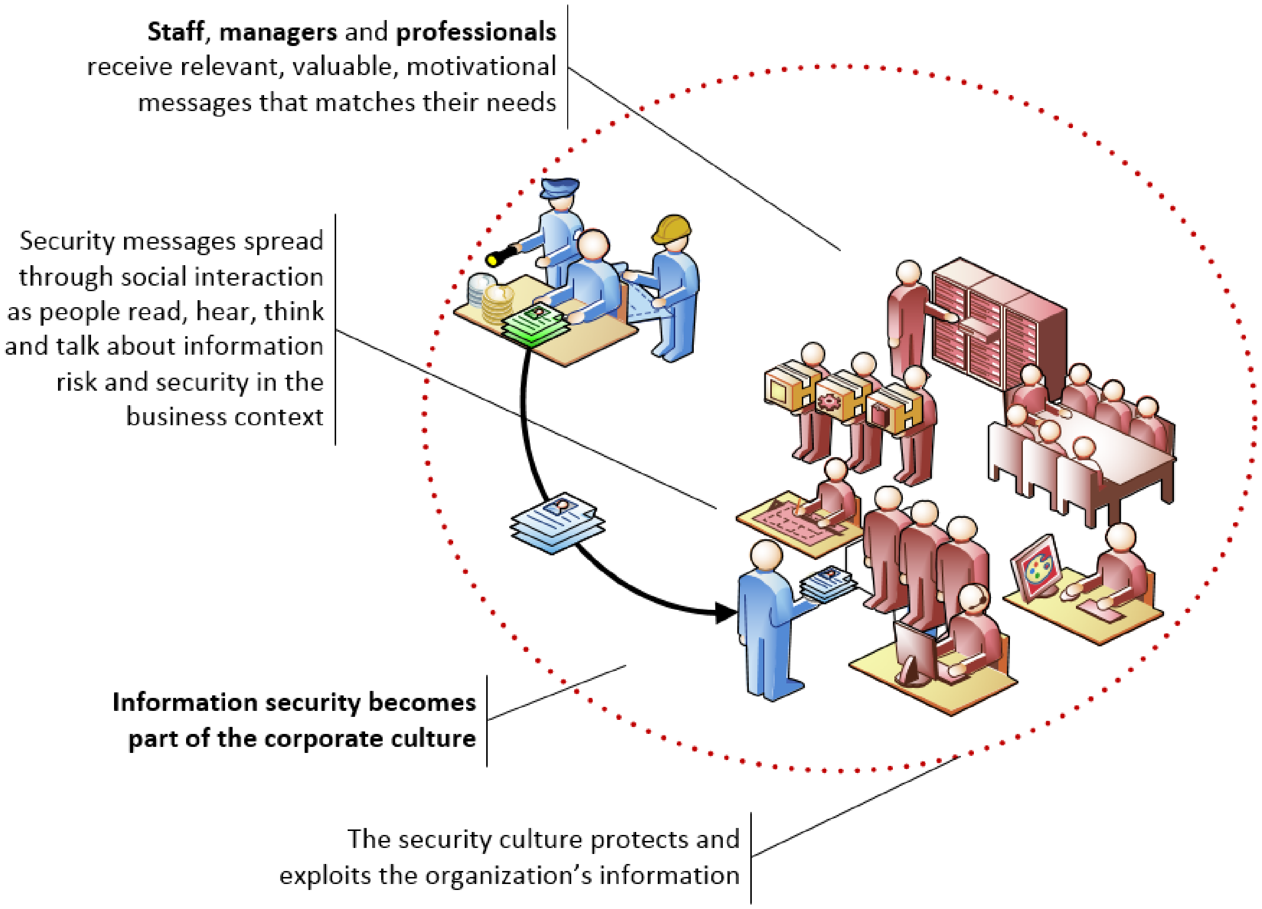
Awareness program overview

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 here) makes the point that raising security awareness is not an end in itself but an important a step on the way to the ultimate objectives: reducing information risks and costs, increasing assurance and enabling the business to prosper.


Staff, managers and professionals receive relevant, valuable, motivational messages that matches their needs
Security messages spread through social interaction as people read, hear, think and talk about information risk and security in the business context
Information security becomes part of the corporate culture
The security culture protects and exploits the organization's information

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.

Target awareness audiences

While security awareness programs have traditionally addressed just IT users or 'everyone' (without distinction or focus), it makes more sense address distinct audiences with different awareness requirements, backgrounds, perspectives and information needs. We recognize three main target audiences, namely:

1) workers in general;
2) managers; and
3) professional specialists.

These audiences are explained further in Appendix A.

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 below.

Metrics derived from measurement techniques such as surveys 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.

Awareness program content

Information security topics

An innovative feature of our proposed approach is that we will concentrate on a different information security topic each month. An indicative list of topics is presented in Appendix B although the list is not cast-in-stone. The topics will vary according to the evolving awareness needs of the organization, plus the ever-changing information risks, compliance requirements *etc*. We will incorporate new topics as they come up, and the program as a whole will gradually mature as time goes on.

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

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, contractors, consultants, temps, interns *etc*. ('workers');
- Relevant laws, regulations and best practice standards (*e.g*. privacy laws, industry regulations and ISO/IEC 27001) will be cited;
- Straightforward plain English guidelines and procedures will advise employees on how to comply with the corporate policies, standards, laws *etc*. in practice;
- 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 and near-misses are an important element of the awareness program since people commonly underestimate or discount information risks;
- Technical details on specific information risks plus advice on incorporating appropriate controls into applications, procedures *etc*. will help technologists build and maintain secure IT systems;
- Briefings on emerging information risks associated with new technologies, systems, business relationships, market conditions *etc*. will keep everyone up to date;
- Realistic case studies and presentations will make the topics more relevant, stimulating thought, discussion and learning.

Sources of awareness materials

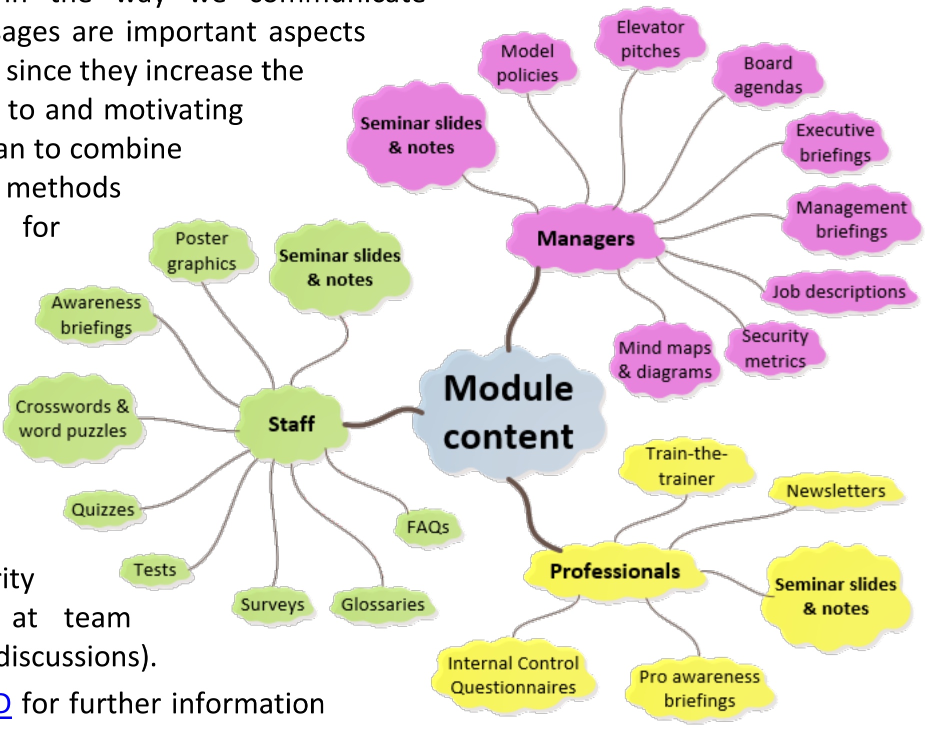
Awareness materials (content) will be obtained from:

- Internal corporate resources such as information security awareness and training materials developed previously, plus information security policies, standards, guidelines *etc*. (some of which may belong to other departments Site/Building Security, HR and Legal);
- NoticeBored, a security awareness subscription service from security awareness specialist IsecT Ltd. NoticeBored delivers high quality awareness content in the form of seminar presentations, newsletters, posters, briefing papers, checklists, quizzes *etc*. The NoticeBored materials are supplied electronically for editing and inclusion in our awareness program with little effort on our part (to be covered by a license agreement with IsecT Ltd.);
- Public information on the Internet *e.g.* news stories about information security and privacy breaches, virus updates, Microsoft, IBM and SANS security briefings *etc*. (subject to copyright restrictions);
- Materials published by the government, industry bodies and others *e.g.* laws and regulations, information security surveys, guidelines and booklets on privacy (these may also be subject to copyright restrictions);
- Where necessary, of course, we will create our own supplementary awareness content from scratch.

Security awareness methods

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 workers. We therefore plan to combine communication methods traditionally used for awareness programs (posters, newsletters *etc.*) with modern electronic methods (*e.g.* intranet, email, SMS/text messaging) and other innovative ideas (*e.g.* facilitated information security seminars, presentations at team meetings and board-level discussions).



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

Information Security's intranet website – the Security Zone

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

Through the *Security Zone*, current information security policies, standards, procedures and guidelines will be made available in one place to all workers. Definitive versions of approved policies *etc*. will be available instantly throughout the organization.

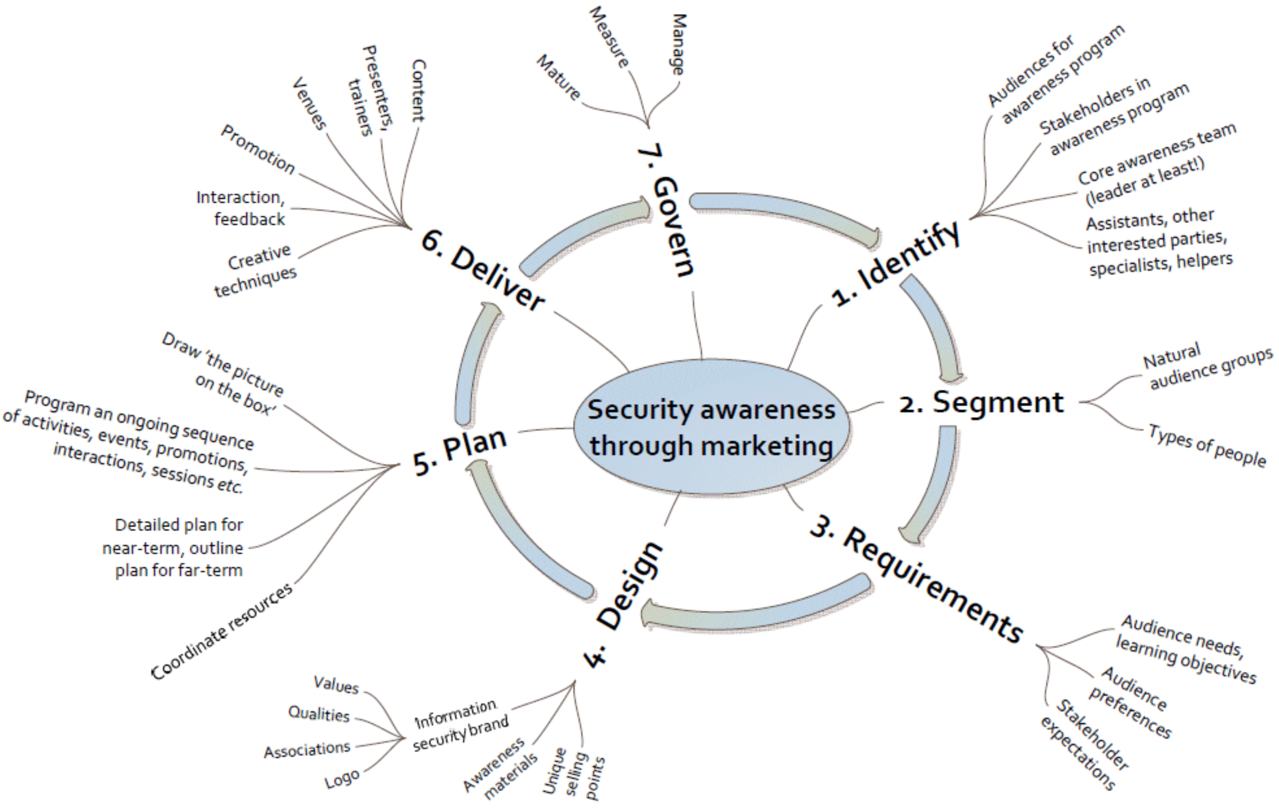
Fresh awareness materials will be added to the *Security Zone* every month, highlighting a succession of topics. The engaging stream of new materials, news stories, quizzes, competitions and so forth is designed to interest, inform and motivate the audiences. We aim to get workers to visit the *Security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

In time, we may extend the *Security Zone* using other social media such as blogs, wikis *etc*.

Branding and marketing

Whereas the awareness program will use various communications methods over the long term, individual elements will be linked 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. Workers will soon form conceptual links between the awareness materials and the overt security messages, as well as gaining a deeper appreciation of the underlying information security goals and less obvious messages. In time, information security will become an accepted part of the daily routine - business as usual, 'the way we do things here'.


Security awareness through marketing
1. Identify
Audiences for awareness program
Stakeholders in awareness program
Core awareness team (leader at least!)
Assistants, other interested parties, specialists, helpers
2. Segment
Natural audience groups
Types of people
3. Requirements
Audience needs, learning objectives
Audience preferences
Stakeholder expectations
4. Design
Information security brand
Values
Qualities
Associations
Logo
Awareness materials
Unique selling points
5. Plan
Draw 'the picture on the box'
Program an ongoing sequence of activities, events, promotions, interactions, sessions etc.
Detailed plan for near-term, outline plan for far-term
Coordinate resources
6. Deliver
Promotion
Venues
Presenters, trainers
Content
Interaction, feedback
Creative techniques
7. Govern
Mature
Measure
Manage

New employee orientation/induction training

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

We cannot safely assume that newcomers are sufficiently security-aware. While they *may* know about some of 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 is also an opportunity for newcomers to meet our information risk and security professionals, establishing social links soon after they start work.

We will establish a standardized security orientation/induction course that can be delivered to all new workers, cover the basics such as:

- General security compliance obligations;
- Where to find security policies and advice (introducing the *Security Zone*);
- Choosing strong passwords and keeping them secret;
- Heads-up on common social engineering techniques such as phishing and grooming;
- 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 Help Desk.

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

Security awareness program management

Program governance

The organization's Security Forum will act as the senior management body overseeing and steering the awareness program as a whole. Once or twice a year, the Information Security Awareness Manager will review the status of the awareness program, deliver progress reports and metrics to the Forum to demonstrate the effectiveness of the program, and discuss future directions.

Information Security Awareness Manager (ISAM)

We propose to manage the program within the Information Security 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 risk, security, privacy, governance, compliance and IT experts including information security professionals, security administrators and other contacts throughout the organization;
- Corporate Communications, HR and Training functions who routinely communicate with workers;

- Legal department will of course be consulted on legal matters and, along with HR, may wish to advise on appropriate forms of words for the more formal materials such as policies.

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, competitions and a glossary will be made available to all workers 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 or supplementary awareness content). Existing security awareness materials and activities that are already in progress will gradually be absorbed into and superseded by the new program.
- Deliver the awareness materials – through a range of 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. Interactivity will be a major 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. Progress reports containing key statistical information will be presented to the Security Forum, and more detailed operational metrics will be used to manage and improve the program month-by-month.

Monitoring and measuring the awareness program

The awareness program will be monitored and 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).

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 (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)	The *Security Zone* will provide on-line quizzes, surveys *etc.* to test workers' knowledge. Evaluation scores and feedback comments from those attending awareness activities, presentations *etc.*, will be collected, collated and analyzed systematically. Website statistics from the *Security Zone* will demonstrate the popularity of the site as a whole and in detail. Occasional surveys or structured interviews may be used to assess knowledge and gather feedback comments and suggestions on the awareness program.
Business value (outcome)	The most compelling result is the hardest to measure. Indicators include generalized reductions in information security incidents, and specific reductions linked to monthly awareness topics.	Various, some depending on the topic *e.g.* the trend of virus incidents should fall but the number of associated Help Desk calls should rise after the awareness program covers the "malware" topic

Cost benefit analysis

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

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

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 or impact of information security incidents, reducing costs both directly (*e.g.* data and systems 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 arise here**];
- Facilitate disciplinary or legal action against people who deliberately break the information security rules (ignorance will no longer be a reasonable defense).

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 workers 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 in due course for the program itself.

Appendix A – Target audiences

Group	Reason for grouping	Members
All workers	Prime targets for the awareness program are the people who use our IT systems and handle corporate and personal information – in other words, practically everyone. 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. Demonstrable awareness of the organization's information security rules is vital if we are to take disciplinary or legal action following a breach.	Practically all our employees plus contractors, consultants *etc*. on our premises. Membership includes everyone in the two remaining groups.
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 themselves understand and comply with their information security obligations). Furthermore, managerial oversight is itself an important class of information security controls, hence managers need to be aware of their governance responsibilities including monitoring, guiding and supporting their subordinates.	Senior to junior management, from the executives and board members to team leaders and supervisors (depending on topic)
Specialists	This group is largely ignored by traditional security awareness activities yet we expect them to understand, promote, implement, operate and often manage many 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 information technologists to incorporate appropriate technical controls in IT systems they build and operate, and make use of controls in systems they use.	IT professionals and "power users", plus specialists and advisors on risk, security, governance, compliance, privacy *etc*.

Appendix B – Indicative awareness topics

1. **Accountability and responsibility** - examines, explains and contrasts these two commonly misunderstood concepts that are fundamental to information security, governance and compliance;
2. **Apps** - about integrating information security into the application development/acquisition lifecycle, and mobile apps;
3. **Authentication and identity management** - from choosing strong passwords to biometrics, identity theft, access control and federated identities;
4. **Best practices** - discovering, evaluating and adopting best practices in information security can be a short-cut to excellence;
5. **Bugs!** - security vulnerabilities created by errors or flaws in program specification, design, coding or configuration by software development professionals and end-users;
6. **Business continuity** - covers business impact analysis, resilience, disaster recovery and contingency to maintain critical business activities;
7. **Business relationships** - securing the information element of 'third party' relationships between organizations is more involved than it may appear, given the number of relationships, their dynamics, and the wide variety of situations where information is placed at risk;
8. **BYOD (B**ring **Y**our **O**wn **D**evice**)** - using personal tablets, laptops, smartphones *etc*. for work purposes may suit the business but presents information risk and security challenges;
9. **Change management** - covers the intersection between change management and information security management, taking in risk management, compliance, patching, testing, configuration and version management, and more;
10. **Cloud computing** - covers the information security aspects of cloud computing;
11. **Compliance** - fulfilling obligations under information security-related laws, regulations, standards, contracts *etc.* plus internal corporate policies, procedures and guidelines;
12. **Computing on the go** - securing portable ICT devices such as laptops, USB memory sticks, PDAs, smartphones and all manner of boys' toys*;*
13. **Cryptography** - a fun, lightweight introduction to the rather heavy topic of encryption and other cryptographic applications;
14. **Cybersecurity** - a heavy-duty but gripping module lifts the cover on *extreme* cyber-risks relating to cyberweapons and cyberwar;
15. **Cybertage** - 'sabotage in cyberspace' concerns the use of information and IT systems as weapons to commit sabotage, and sabotage *of* information and IT assets;
16. **Database security** - securing large collections of valuable data against hackers, corruption, loss *etc.;*

17. **Digital forensics** - forensic investigation of data relating to and arising from information security incidents;
18. **Email** - security aspects of email plus other electronic person-to-person chat tools such as Skype, IM, Twitter, blogs and more;
19. **Fraud** - taking advantage of victims through deception and coercion;
20. **Governance** - roles, structures and reporting lines for the information security function and its relationships with others such as risk management, IT audit and general business management;
21. **Hacking** - tips to counteract hackers, crackers, industrial spies, insider threats, scammers, criminals and other adversaries exploiting network, software, hardware, physical and human vulnerabilities;
22. **History of security** - looks at the evolution of information security techniques and technologies through the ages;
23. **Hi-tech infosec** - risks and controls involving IT, systems and networks, and high-technology;
24. **Human error** - explores the human side of information integrity including booboos, blunders and gaffes;
25. **Human factors** - the human side of information security - security culture, awareness, policies and more;
26. **Identity theft** - stealing and faking credentials, phishing, impersonation and fraud;
27. **Incident management** - the cyclical process for identifying, reacting to, containing, resolving and learning from information security incidents;
28. **Industrial information security** - information risks and security controls relating to industrial IT systems controlling factory machines, equipment and plant, microcontrollers and critical national/corporate infrastructures;
29. **Information protection** - obligations to protect information assets, plus information classification and baseline security controls;
30. **Information Security 101** - a general, multi-topic starter module covering the basics of information security for new employee orientation sessions and to accompany the launch or re-launch of security awareness programs;
31. **Information risk management** - processes to identify, examine and treat the full spectrum of information risks, in the context of corporate risk management as a whole and information security specifically;
32. **Insider threats** - security threats arising from employees on the payroll and third party employees working for/within the organization in a similar capacity (‘workers’ we call them);
33. **Internet security** - from web surfing to eBusiness apps, social media and cloud computing, this module covers one of the hottest and riskiest areas of information security;
34. **IoT (the *Internet of Things*) security** - also known as the Internet of Threats;

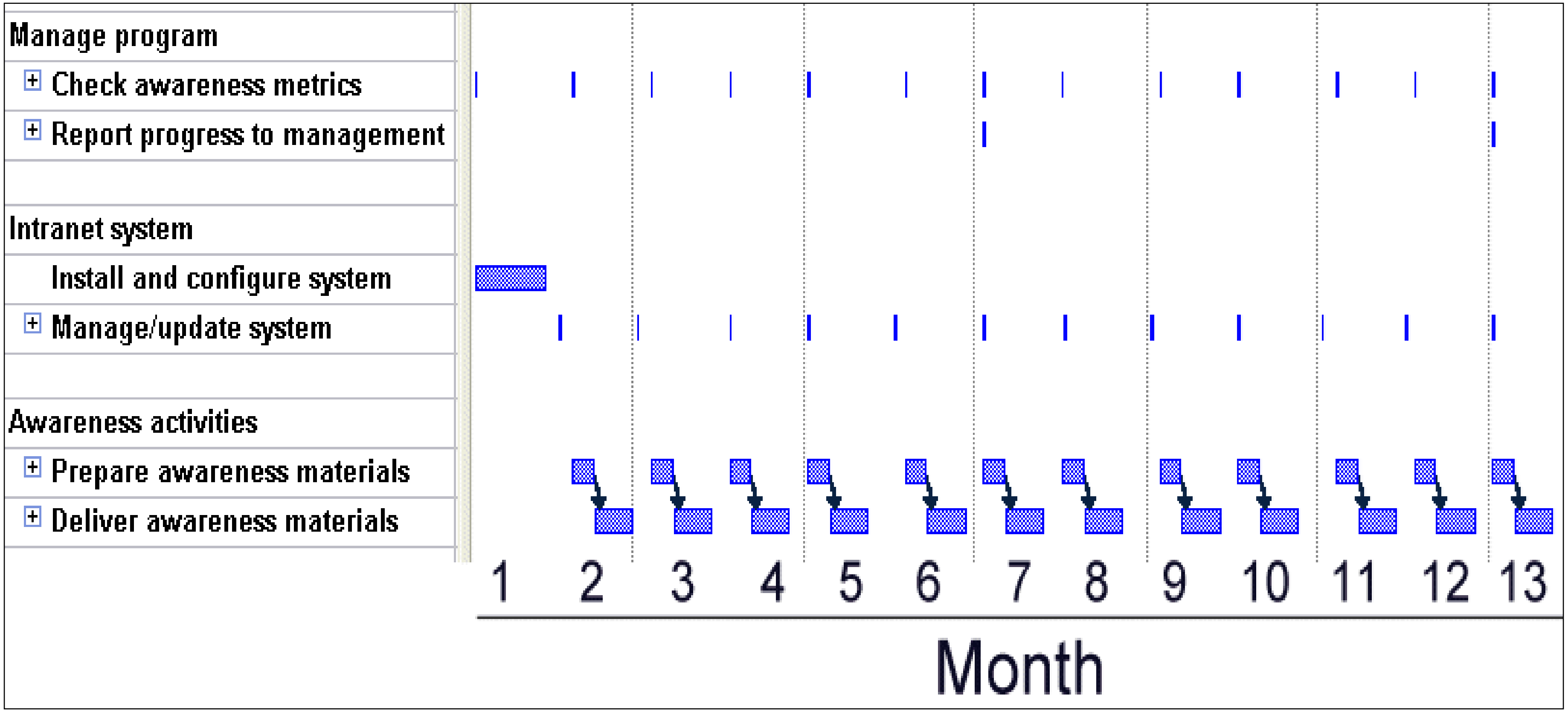
35. **IPR (I**ntellectual **P**roperty **R**ights) - protecting our own rights and interests while also respecting others';
36. **IT auditing** - understand what makes IT auditors tick, what they do, and how to work with them more effectively;
37. **Knowledge** - protecting intangible information assets and intellectual property;
38. **Learning from information security incidents** - improving security in response to incidents that involve the organization or third parties;
39. **Lo-tech infosec** - concerns those important parts of information security that lie beyond IT-security or cybersecurity;
40. **Malware** - viruses, worms, Trojans, keyloggers, spyware, rootkits, APTs/Advanced Persistent Threats, multifunctional and embedded malware, and ransomware are such significant threats that we will update this awareness module annually with fresh, topical content;
41. **Network security** - all manner of information security issues arising from networking, internetworking, communications, liaisons, collaboration and social interaction, VOIP, VPNs, IoT, BYOD, mobile working ...;
42. **Office security** - the average workplace faces a range of information security risks ranging from intruders, thefts, fires and floods to bugs and a variety of office IT security issues;
43. **Oversight** - a unique security awareness module covering both 'oversights' (casual errors, accidents and omissions) and 'overseeing' things (an integrity control);
44. **Passwords** - concerns credentials used for identification and authentication of people, including passwords, passphrases, two-factor authentication, biometrics and so forth;
45. **Permissions** - including but extending well beyond rights and privileges;
46. **Phishing** - aside from touching on phishing in several other modules (such as email, credentials, identification and authentication, social engineering, malware, fraud and identity theft), we dedicated an entire awareness module to the topic, reflecting its significance;
47. **Privacy** - protecting personal information, respecting individuals' privacy rights and expectations;
48. **Physical security** - protecting information assets (including people) against physical threats such as unauthorized or inappropriate physical access, fires, floods, and various workplace hazards;
49. **Portable devices** - security of laptops and other portable/mobile ICT devices, touching on BYOD and home working/teleworking;
50. **Secure-by-design** - making information security an integral part of systems and processes from the outset, including security architecture and the concept of fail-safe/fail-secure design;

51. **Social engineering** - the only practical way to tackle this growing threat is to ensure employees are well aware of the issue, motivating and guiding them to think critically and so resist attacks;
52. **Social media** - covers the information security and privacy hazards associated with Linkedin, Facebook, blogging *etc*.;
53. **Social *in*security** combines social engineering with the security aspects of social networking and social media, including 419 and lonely hearts scams, spear phishing, inappropriate online disclosures and insider threats;
54. **Surveillance** - increasingly common in public, corporate and personal domains, surveillance is both a valuable form of monitoring control and a privacy/human rights concern depending on your perspective;
55. **Survivability** - tackles the *extreme* end of risk management, incident management and business continuity when major incidents occur;
56. **Tools and techniques** supporting/enabling information risk and security;
57. **Trade secrets** - a spectrum of activities from legitimate market research and competitive intelligence through to unethical if not illegal industrial espionage and information warfare;
58. **Trust and ethics** - trustworthiness depend on the trusted party's ethics, making this an important - if unusual - information security awareness topic.

Note: this is not a definitive list of planned awareness topics so much as an indicative outline. These are the monthly topics that have been covered previously by the NoticeBored service. The actual awareness topics we cover in future will reflect current and emerging information security risks and issues, new technologies, recent incidents, compliance obligations *etc*. Topics listed separately above may be combined and supplemented, or split up to cover certain aspects in more depth. The beauty of the monthly, rolling approach is that we can respond rapidly to the organization's evolving information risks and security awareness needs/

Aside from the specific subject matter, the awareness materials as a whole will constantly reinforce fundamental concepts such as confidentiality, integrity, availability, risk, control, governance, compliance, privacy, ethics *etc*. The very fact that the organization is willing to invest in the program is itself a sign of the importance of information security to management.

Appendix C – Outline program plan



Appendix D – Communications methods

There are *many* different ways to get the information security messages across. We would like to use a wide range of communications methods and vehicles, *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 approaches. The following list 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 Security Zone from other relevant intranet sites. We will solicit feedback from users and may incorporate social media functions 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, cascaded internally through the organization structure. There will also be a regular information risk and security column in the company 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 or conference. Avoiding 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 or 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).
- **Departmental contacts**: we will establish an internal corporate social network of departmental information security champions or ambassadors to disseminate key information security messages and channel feedback comments from staff back to Information Security. 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.
- **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 where necessary for their roles and responsibilities. Wherever possible, we will use internal training resources to contain the costs, and we will collaborate with HR to analyze training needs.
- 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 as appropriate (*e.g.* integrating advice on information risk assessment and security architecture into 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. We 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 such as **signs and passes** will be updated to incorporate relevant messages *e.g*. warning notices saying "Since this is a secure facility, you are subject to random spot-checks by Security"; similar security messages will be printed on the rear of the standard staff and visitor passes. We will liaise directly with site security/facilities management on these materials to ensure appropriateness and consistency across the 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 rewards).
- **Reference materials** – information security videos, books, journals, interactive presentations, Computer Based Training and other resources will be made available through the *Security Zone* and library, promoted in the awareness newsletters, training courses, presentations *etc*.
- Appropriate security awareness messages may be incorporated into system login banners, desktop backgrounds, screensavers, application messages, help text, email signatures *etc*.
- **Voicemail broadcasts and SMS/text messaging** may also be used on occasion, particularly to communicate messages relating to phone security or urgent alerts.
- A **suggestion scheme** may be introduced once the awareness program is established to solicit improvement suggestions, feedback and fresh ideas.
- **Collaboration with specialists** in Privacy, Risk Management, HR, Legal/Compliance, Site Security and Audit 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 and value of information security.