



NOTICEBORED

Seven steps to security awareness

By Dr Gary Hinson CISSP CISA CISM MBA, CEO of IsecT Ltd.

Last updated: September 1st 2005

Introduction

Are you maybe thinking about running a security awareness program but are not quite sure where to start? This paper offers some pragmatic hints and tips on applying the seven key steps of a typical IT procurement process to the selection and launch of an awareness program, based on our experience at being the 'driver' of the process and the 'driven'.

We have done our level best to make this a useful generic paper, not one that is specific to NoticeBored, but leave it to your judgment to adapt the paper to your individual circumstances.

Like others on the NoticeBored website, this paper is a work-in-progress. Thanks to the wonders of the web, we will revise it from time to time when further inspiration strikes. If you have a question or suggestion relating to this, please do [get in touch](#). We'd love to hear from you, especially if we've overlooked something important to you.

1. Specify your requirements

The first step is to think carefully about what you are really trying to achieve through security awareness. Until your objectives are clear, you will have problems planning and organizing the awareness program, let alone evaluating and choosing the products and services you may need in the first place.

Here are some rhetorical questions to ask yourself for a start:

- Do you have an information security awareness program already running, or is this an entirely new concept for the organization? If not information security, are there other awareness programs running that might act as role models?
- Does/should the program involve awareness, training and education, or only one of these?
- What topics does/should the program cover? Are other aspects of information security important to your organization?
- How often does/should the program address individuals? Is that frequent enough to keep information security on their agenda?
- Does/should the program go into sufficient depth to provide useful advice and guidance where appropriate, or it is only meant to give a superficial overview?
- Does/should the program apply to all employees from their first to their last day at work? Does/should it extend to third parties working in a similar capacity to employees e.g. consultants, contractors and other associates working on site?

NOTICEBORED

Now try dreaming a bit - picture yourself in the future - try to imagine how things will be when your awareness program is running smoothly. You might like to consider some more complex issues such as:

1. Do you simply want to make people "aware" of security, or do you in fact want them to behave differently as a result of being aware? Awareness is worthwhile in itself but, we suggest, is usually not the ultimate goal, and therefore your program plan needs to continue beyond simply raising awareness.
2. Who are you trying to reach with your awareness campaign? Are all those people alike or are there in fact separate audience groups with different information needs? In your management hierarchy, do the superiors for your target audience/s understand and support what you are doing or do you need to tackle them too? Are there particular teams with more specific requirements (such as IT Operations and IT Help Desk people)?
3. Are you looking for generalized security awareness, or specific training in particular problem areas, or both? What kinds of things do you want to make people aware of? Is this a fixed list of topics or a dynamic list that will change over the coming months and years? Answering this question will tell you whether it is feasible to cover the whole planned syllabus in one hit or whether you need to think long term to avoid information overload
4. ... which leads on to: Do you plan to run the awareness campaign on an ongoing basis or are you looking for a one-off fire-and-forget or similar short term initiative to address a specific issue? Both approaches are valid in the right circumstances, sometimes a combination approach is needed.
5. Do you have a culture of security in your organization already, or are you constantly fighting to get anyone to take security seriously? In other words, how mature is your organization on security? If security is already pretty well ingrained in the organization, its people and its processes (like, for example, in most banks) you will have an easier time promoting information security awareness than if it's an entirely alien concept. Do you have a comprehensive set of information security policies in place already, for instance, and are they maintained up-to-date, or will your program need to develop these as well as promoting them? Be realistic in your planning about the time and effort it will probably take to reach your goal: remember, it's better to under-promise and over-perform than *vice versa*!
6. Will the campaign be funded and run as a business or IT-led activity? Who will run it, and what qualifications/experience do they have in information security and security awareness/training/education to equip them for the task? If, as is quite often the case, it's your baby, then maybe you could do with some additional training or consultancy assistance to get things off the ground. A little bit of concentrated assistance in the planning and initiation stage can help avoid a lot of wasted effort and aggravation later.

[NIST Special Publication 800-50](#) is an excellent source of unbiased advice on security awareness. If the six issues above have got you thinking, check out SP 800-50 to broaden your horizons and deepen your analysis.

2. Prepare a plan and checklist

Awareness programs do not run themselves, especially as many organizations start from a fairly negative position. It will take concerted effort to overcome that inertia, get the organization up to speed on information security, and then keep it rolling. In other words, you need to design the program, develop a plan to establish the program and then manage it effectively in order to deliver the projected benefits.

If you have a lot of ground to cover (e.g. "the whole of information security"!), we would definitely recommend planning to cover it in discrete sections or chunks spread out over time, and wherever possible framing those chunks in terms that make sense to your target audience/s. Take, for example, the virus problem: anyone who uses an IT system should have a basic understanding of viruses. In explaining about viruses, you may want to mention issues such as configuration

NOTICEBORED

management, network/systems access and so on, but you need not go into depth on all of these at the same time. It's perfectly acceptable to say "We will tell you more about this later" or even "Call the Help Desk or the Information Security Manager for more information".

An ideal way of crystallizing your thoughts from step 1 above in parallel with developing your plan is to prepare a product evaluation checklist containing:

- Rows for each of the criteria that are important to you;
- Columns for the criteria and their weightings (e.g. 3 = essential, 2 = important, 1 = nice-to-have), and then further columns for comments and scores against each of the products you are evaluating.

As you work through the checklist, you will in effect be defining and refining your requirements for the program, making it easier to develop an associated plan. That's why we treat these two activities as one step.

3. Secure funding and management support

Getting your senior management on board with the whole idea of an awareness campaign is, I humbly suggest, by far the most important thing you can achieve in the next few months and will pay big dividends in the long run. How you actually achieve this is down to you: we can only hint at things that have worked for us and our clients.

Depending on the corporation, you may or may not need to make a strong financial case for the investment - some senior managers respond better to gut feel than raw numbers. Our [generic business case](#) paper may be a useful straw-man if you need to persuade your management to fund and support the awareness campaign (by all means [call us](#) for the editable MS Word version of the paper if that will save time). It includes some hints on financial modeling for risk reduction projects like yours.

Work with your CIO or IT Director, for sure, and ideally other influential managers who have an interest in seeing the awareness program succeed. You will often find friends in functions such as Internal Audit, Compliance, Facilities, Risk Management, HR and Finance. Time spent privately and patiently explaining your plans to these stakeholders will help (a) refine your plan; (b) identify any concerns; (c) deflect criticism and (d) line them up to support your program, and do so overtly during the critical early phases of delivery.

By the way, it's often worthwhile getting *explicit* management support for information security during this process, meaning at least one strong quote from a senior manager which unequivocally mandates compliance with the organization's information security policies and associated requirements. You may need to draft the statement for the CEO in practice but her signature on the bottom will add weight to your awareness program way beyond its apparent value. Believe me, clout works!

During step 3, do not be afraid to continue refining your plan and requirements. All the time, you are thinking about it and learning about the possibilities. Don't waste that brain energy!

4. Identify and shortlist possible solutions

Now you are in a good position to go looking for what you might need. Start by looking within your own organization for suitable resources, for example in your IT, HR, Internal/Corporate Communications and Training and Development functions. Take advice from colleagues running other internal awareness/training/educational programs (such as Health and Safety or IT training). Simply asking your colleagues for advice is worthwhile as it may help get their support for delivering the program later on, whereas not asking them may inadvertently set them against it.

When it comes to finding public free and commercial offerings, Google is your friend! Search for terms such as "security awareness", "information security awareness", "security awareness posters" and so forth. Check out the industry magazines and professional societies for help and advice. Join the [Security Awareness Forum](#) on Yahoo and check out the archives. Pretty soon,

NOTICEBORED

you will have amassed a list of interesting products and services. Be systematic about the way you gather the information and you will make the remaining steps easier.

Now go through your list of internal and external resources and home-in on those parts which you think may suit your needs. By all means discard the others but be careful - it is easy to overlook useful resources that are badly marketed, incompletely described or simply unknown (often because they are new). If you have the time and energy, it may be safer to shortlist most if not all potential suppliers at this stage and trim the list later. There is no harm in contacting companies for initial information at this stage but be wary of overt sales pitches: the next step in the process works best if you approach it objectively on your terms, not theirs.

5. Evaluate potential solutions

For commercial offerings, this is the conventional tendering sub-process:

- You prepare a formal Request For Proposals containing your requirements derived from your dreaming, planning and evaluation criteria (which you probably do not want to disclose);
- You send the RFP to potential bidders (without identifying who is being invited to bid), along with a deadline to respond;
- You receive questions from some bidders, and respond quickly to all bidders without disclosing who originated the questions;
- When the deadline expires, you reject any further bids/proposals and start systematically evaluating and scoring them using the checklist written earlier (we suggest a percentage score against each criterion);
- Focus on the essential requirements first - you may be able to exclude some bidders immediately if they simply do not satisfy your essential needs;
- Don't neglect any additional offers made by the bidders - sometimes, they will suggest useful, valuable ideas you had overlooked, and they can help reach a final decision if the scores are close between a number of offers;
- Look at the quality of the bids/proposals as well as any sample awareness systems or materials sent for evaluation - these are all valid indicators of the professionalism and quality of the bidders;
- Do the math: final score for each bidder = (sum of (score for each criterion x weighting for that criterion)) divided by maximum possible score x 100 percent.

Your Procurement people should be falling over themselves to help you with the tendering process, especially if there are substantial sums of money involved. They will want to ensure that the process is fair, objective and entirely above-board. This is *their* profession: take their advice!

For in-house and free offerings, the shortlisting, evaluation and assessment process is similar. It is entirely possible that you may wish to take advantage of commercial and free awareness materials, for example, and combine them with internal resources. It's your choice.

6. Select and procure chosen solutions

The end result of step 5 is usually but not always a single winning bidder. Sometimes you may have selected different bidders for separate parts of your requirement, sometimes you will have been unable to decide between a few bidders. Step 6 generally involves a bit of negotiation with the suppliers, perhaps some clarification of the price, the terms of the offer, and another hard look at what they offered. Finally you make the decision, prepare the Purchase Order, sign the contract and move swiftly along. This is known as *doing the business*.

NOTICEBORED

7. Implement and launch the awareness program

Let the fun commence! Whilst the previous 6 steps may perhaps have seemed a rather bureaucratic and pointless diversion, you may well find the opposite in practice. Just as with a software development project, time spent deciding the requirements, designing the solution and testing the system pays off in the end with a smoother and more effective implementation.

You have a well-written plan and the necessary resources to deliver it. Now is the time to call on the support of your internal colleagues and chosen suppliers to build and deliver the awareness program of your dreams.

Conclusion

In this paper, we have given a flavor of what is normally involved in launching a security awareness program. Your mileage may well vary but we hope this helps turn a somewhat confusing process into a straightforward set of steps. Good luck!

About NoticeBored

NoticeBored is IsecT Ltd's innovative security awareness product line:

- **NoticeBored Classic** is our content-only service. Every month, we prepare and deliver a fresh package of high quality security awareness materials on each information security topic. The materials comprise presentations, briefings, newsletters, posters, mind-maps, case studies, policies, white papers, screensavers, awareness surveys *etc.* in industry-standard editable file formats (e.g. Rich Text Format, PowerPoint & JPG).
- **NoticeBored Plus** is a Java application that serves your information security policies, standards, procedures and other awareness materials on the corporate intranet. ISO 17799 policy templates are provided along with tools to create, manage and deploy the materials and facilities for creating online lessons and tests linked to the policies. We also deliver the monthly NoticeBored Classic materials free-of-charge to NoticeBored Plus subscribers, forming a comprehensive security policy and awareness solution unmatched by our competitors.

Please visit www.NoticeBored.com or else call IsecT on +44 1428 727 900 for more information.