Communicating Information Security to SMEs

Michael Barwise

The problem of communicating the security message to small and medium enterprises (SMEs) has been widely aired. However little progress seems to have been made to date, largely because two major issues have remained unaddressed.

Clarity of Definition
Firstly: what is an SME? This is a broad economic classification which encompasses a wide variety scales and business structures. It is therefore probably not the optimum descriptor for the information security context, where solutions are critically dependent on scale and structure. From the information security perspective, SMEs can basically be divided into four categories;

[case 1] businesses that do not use information technologies
[case 2] businesses that use information technologies but do not employ any technical support staff
[case 3] businesses that use information technologies and employ IT support staff, but only staff without specific security expertise
[case 4] businesses that use information technologies and employ IT support staff with specific security expertise

Each of these categories will potentially require different guidance, both in terms of content and presentation, although the first two categories are probably where the main effort must be expended.

Clarity of Business Requirement
Secondly, there is still a tendency to start discussions of information security from descriptions of technical threats and the deployment of product-based solutions, rather than from the business requirement for sound information management. This excessive technocentrism can only be addressed by re-appraising the way we approach security as a discipline. Rather than *ab initio* emphasising technical threats and solutions: viruses; worms; hackers; firewalls; network security; intrusion detection *et al*, we should first be stressing the business requirement for information robustness in terms of privacy, integrity, availability, recoverability, authenticity and so on prior to considering technical issues. Only once these business requirements have been established can technologies be effectively deployed. Security technologies are the solutions: they do not define the problems. We must establish what the problems really are before attempting to solve them, and where resources are limited (as they always are) the most important problems must take precedence.

The needs of SMEs

Combining these two approaches, it is possible to outline the requirements for communicating information security effectively across the spectrum of SMEs. However, the following notes are not exhaustive, but are intended to trigger further discussion and development. In particular, the four categories of SME are not absolutes. They are merely easily identifiable key points on a continuum that has numerous additional parameters such as business turnover, profitability, human resources, and, most importantly, prior awareness of the business implications of insecurity.

Case 1
The first and most important point (which is largely obfuscated by BS7799 and particularly by DPA 1998 in the light of the Durant case[i]) is that even if a business uses no IT and does everything on paper, it will still have a requirement for information security. People leak, lose and corrupt business information to a much greater extent than computers do, and even technical breaches of computer systems and detriments to electronic data are mostly facilitated or caused by acts or omissions of people acting in good faith.[ii] So basic guidance on how to create and maintain sound business processes supporting the management of business information (including statutory obligations) must be expressed in sufficient detail that it can be directly acted upon by the smallest and least technologised business right down to the microbusiness and sole trader. Currently, this information can only be obtained *in toto* by recourse to numerous disparate sources which are difficult to identify and, often, to understand. A single body of clearly expressed standard guidance would prove much more effective.

Case 2
The second category of SME, that uses IT but has no support staff, requires somewhat more varied information in support of the larger volume and complexity of information processed and the

increased exposure resulting from using IT (particularly Internet connectivity). However, the owners and managers of this scale of business generally and quite reasonably have little time or patience for technical discussions. What they need most is guidance on how to locate, validate and control the use of affordable external IT and security consultancy. For example, these SMEs need objective factual information about the levels and relevance of qualifications, memberships and registrations held by consultants, coupled with guidance on contractual matters, including professional indemnity, terms of service, insurance.

Despite their characteristic impatience with technical detail, there is still considerable resistance among this category of SME to the use of external consultants, often because the cost seems *prima facie* difficult to justify. In reality, however, a case 2 SME not professionally involved with IT will be ill-equipped to go it alone in securing their information. Even if basic technical guidance is provided, there is a high probability of attaining a sense of security that is substantially greater than the reality. It can be pointed out that the most expensive component of corporate security consultancy is not the technical component but the business requirements analysis. It is therefore demonstrably cost-effective to perform this in-house and buy in the technical expertise, particularly as the latter is only required on an occasional basis. However, merely providing such information will not suffice: a culture change must be brought about, as the generally preferred option is still to place corporate information security in the hands of total novices (even if they *are* the Directors). This naive policy is not generally applied to accounts or manufacturing processes, because they are seen as significant contributors to business viability. Information security, on the other hand, is still largely seen as a nuisance factor of limited business significance. This attitude must be changed before we can make any real progress in the technical direction.

To effect this change, SMEs will need a clear exposition of the nature of business information hazards in terms of privacy, integrity, authenticity, availability, recoverability *et cetera*, and the concomitant potential financial losses. Management needs to be able to reliably estimate such losses, so that an inevitably limited IT support and security budget can be allocated to best effect. The technical solutions offered by a contracted technical consultancy must be guided by clearly established business priorities, so the SME must be equipped by a common body of knowledge to make the necessary decisions. It must also not be forgotten that in this category of SME, a considerable contribution the IT and security consultancy will be made by general housekeeping, not necessarily directly recognisable as "security services", so guidance on such housekeeping is as necessary as that on more esoteric hazards. We might envisage a television campaign emphasising these points, possibly on similar lines to a recent and striking advertisement depicting a couple showing a potential burglar the weak points in their home security.

Finally, a basic description of the general nature of technical hazards and solutions in layman's terms would prove useful, so that management will be able to vet and approve the consultant's offered solutions from a cost-benefit perspective. A good example of a simple but effective graphical representation has been offered recently by Symantec.[iii] Note, though, that this technical guidance comes last in the requirements list, and cannot hope to be exhaustive if it is to be accessible to such a readership. Attempts to impart non-product-specific technical guidance at more detailed levels ("DIY security manuals") have so far failed, largely because the issues are inherently sufficiently complex to preclude simplification to the desired level. For example, network-layer firewall configuration requires some understanding of data packets, Internet addressing, protocols and port allocations, plus the critical matter of what threats such a firewall will *not* protect against. None of this can be adequately imparted to a complete novice in a few short pithy sentences. Nevertheless, it is a highly dangerous exercise to deploy a firewall without this prerequisite knowledge, as without it there is no way to validate the firewall's real contribution to security, even supposing step-by-step configuration instructions can be followed without error. One of the author's past SME clients had deployed a firewall that permitted all traffic in both directions before they called him in to explain what was going wrong!

There is a possibility that more could be achieved than at present by encouraging product vendors themselves at the low cost end of the market to offer conceptual technical guidance in addition to configuration notes with their products. Cisco, for example, have for a long time offered such guidance at the high end of the market, albeit with the assumption of considerable technical expertise on the part of their readership. But the task of providing such information for a completely non-technical readership would be substantially more arduous, and by no means easy to make proof against potentially hazardous misunderstanding by the uninitiated.

Case 3

Where an SME employs IT support staff without security expertise, the two basic alternatives are to employ security consultants in collaboration with their own internal IT support staff, or to train some of the IT support staff to take on security responsibilities internally, thereby becoming a case 4 SME. Each of these strategies will need to be supported by a different body of information.

When employing external security consultants, the case 3 SME can generally leave technical communication with the consultants to their internal IT staff. It will be less necessary in this case to provide management with technical guidance . However, it must still be made clear that allowing IT staff to mediate with consultants does not absolve management from participating in security strategy and planning. The same need for, and processes of, prioritisation as in case 2 must be applied, but the chain of communication is longer and the politics are potentially more complicated. These SMEs therefore need the same guidance for management as case 2 SMEs with the addition of emphasis on the need for good internal and communication and for management participation in security decision-making.

Where a case 3 SME decides to train internal IT staff to fulfil the security role, it will in the first place need guidance on the nature of the required training. All too often staff are merely sent on product training courses after security solutions have been implemented, and these courses tend not to impart much understanding of the principles involved. The costs and benefits of employing internal security staff must be objectively communicated, and recommendations made concerning the minimum range and depth of expertise to be aimed at.

In either case, all the information required by case 1 and case 2 SME must also be provided.

Case 4

Case 4 is the easiest to communicate, as this is where most has already been done. These SMEs are in much the same position in respect of security management as larger corporations, except that infrastructures will be smaller in scale and fewer resources will be available for security. We may expect the same security problems associated with multiple sites and complex business processes. As this is the scale at which there is most extant technical information available, the primary need is for guidance on where and how to obtain it.

In order to fulfil the potential demand for small-scale information security consultancy, we must also consider standards, training and guidance for the consultancies themselves, most of which are indeed also SMEs. This is an issue of importance, and deserves significant attention in its own right. Space does not permit it to be properly addressed here, but in principle three messages must be communicated: first, the need for all IT consultants to be security aware; second, the benefits to both consultants and their clients of offering security services; and third, the need to communicate security issues in terms the client can understand.

A Change of Emphasis

A lot of enthusiasm has been expressed for “DIY” technical security guidance, and such guidance has been attempted. However experience has shown that only very general concepts can effectively imparted to the uninitiated, due to their lack of basic prerequisite knowledge of technical principles. Effectively all proposals of this kind have so far been proffered by those who already possess, and probably take for granted, that knowledge of principles. From such a position it is extremely difficult to put oneself in the condition of the complete novice: to realise how substantial is the effort required to achieve an adequate level of technical competence. This competence must be adequate not only to carry out, but most essentially to validate the adequacy of, the selection, technical deployment and maintenance of security products. The harsh reality is that these technical decisions are still best left to experts. One might envisage a time when security products have been improved to the point where this no longer applies, but unfortunately that time has not yet arrived.

The most effective contribution of business management is, then, the specifying of business information security priorities to carefully selected competent technical experts, who will carry out the technical tasks in accordance with the provided specification. To this end, certain basic principles must be communicated to business management, some of which have so far generally been overlooked in the SME security arena. These include:

[1] the business must define its security priorities in terms of the relative values of its information assets. It must therefore have and maintain accurate knowledge of its information assets and their values.

[2] in order to establish security priorities, business decision makers must be equipped to consider the nature and implications of detriments to business information in terms of confidentiality, integrity, authenticity, availability, recoverability (and possibly ownership and other attributes, depending on the nature of the business), and be able to use this awareness to direct technical deployments.

[3] all decisions must be properly documented and supported by evidence. Both the decision and the evidence must be validated impartially prior to implementation.

[4] all proposals must include realistic assessment of ability to fulfil continuing support requirements.

[5] individual security provisions must be co-ordinated so that they contribute to a coherent whole defined by the business priorities.

[6] all implementations must be adequately tested prior to deployment.

[7] all security staff and consultants must be adequately validated as trustworthy and competent.

These principles must be imparted to senior management, together with their importance as a groundwork for decision making on security priorities and the management of deployments. Then, having gained the attention of the audience, clear guidance must be offered on how to realise these principles reliably and economically.

Conclusions

Why this emphasis on business information security prioritisation? Put simply, it is no longer the case (if it ever really was) that a business can secure its information with any justifiable confidence by simply having obvious core products such as anti-virus and network-layer firewalls installed at some notional perimeter. They may be necessary, but they are not sufficient, particularly as the concept of the perimeter is eroded by ever more complex electronic information sharing between small businesses and their clients, and indeed between small businesses and Government agencies.

Clearly, there is no more dangerous condition than that of false confidence in inadequate security. Therefore the greatest need in communicating security to SMEs is to enable them to robustly and reliably determine their security requirements in the light of the value of their business information assets, and to select and manage expert technical assistance. Only then can an SME be confident that truly appropriate security measures are being implemented for them by those technically competent to do so. Despite the considerable resistance this approach has encountered (not least from the SME community), it is in reality the optimum way to ensure a real level of security in which justifiable confidence can be held. Although ultimately security solutions are technical, their selection, deployment and configuration depend on business needs. Business management should ideally concentrate on that part of the problem they know best: the business and its business security needs. This point has not until now been sufficiently emphasised, and, not surprisingly perhaps, little progress has so far been made towards improving the reality of information security for a vast community of SMEs and microbusinesses, the vulnerability of which is likely to increasingly impact on the security of critical IT infrastructures up to the national level.

Submission to EURIM on behalf of the BCS, November 2004

[i] Michael John Durant v Financial Services Authority [2003] EWCA Civ 1746 *and*
The Information Commissioner. The ‘Durant’ Case and its impact on the interpretation of the Data Protection Act 1998, V1.0

[ii] for example: Computer Weekly 02/11/04, p1.”Inland Revenue deletes tax records in database gaffe”

[iii] Symantec. 2004. Prevent Unwanted Access by Intruders. ISBN 91-631-5906-6