Review of Availability of Advice on Security for Small/Medium Sized Organisations

March 2010

Authors:

David Lacey

Barry E. James

Executive Summary

Small and medium sized enterprises (SMEs) face a growing range of information security threats. Few SMEs, however, apply sufficient controls to safeguard their sensitive information. For reasons outlined below they are inclined to regard security as “someone else’s problem”. The result is a growing risk of security breaches of sensitive business or customer data, as well as an exposure for many larger organisations that subcontract work to SMEs.

SMEs have little or no access to security know-how and skills, and typically seek to avoid unnecessary overheads. Persuading SMEs to address the risks and improve their security is a challenging task, demanding compelling arguments and clear, simple and appropriate advice and standards. Effective guidance needs to be based on consideration of SME business drivers and decision making processes, which differ from those of large enterprises.

Security advice is available through a range of public web sites. Unfortunately, it is rarely appropriate, complete, or held in places that SMEs would think to look. Most guidance is adapted from big company practices which are not suited to SMEs. Guidance for large enterprises tends to focus on policy, governance and comprehensive standards. Advice to SMEs, however, needs to convey arguments that will have an impact on the bottom line, as well as simple measures that address the most serious risks.

Three essential measures are required to remedy this problem. Firstly, SMEs must know where to go to find appropriate advice. Secondly, the advice provided must be compelling and relevant to their circumstances. Finally, they must see a clear route for taking further action. The conclusion of this project is that there is substantial scope for improvement in each of these areas, and the report makes a number of recommendations on how these gaps can be tackled.

Purpose and scope of this report

This report sets out the findings, conclusion and recommendations of a research project to identify and assess the needs of small and medium sized organisations (SMEs) for advice on information security, especially concerning the safeguarding of personal information, and how these needs are currently being met, or could be better met, by public sources of security guidance.

In particular, the report includes an analysis of:

- How the circumstances and needs of SMEs differ from large organisations.
- How to gain engagement and communicate in a compelling way with SMEs.
- How far these needs are being met by existing, publicly available guidance.
- How this advice might be better framed, presented and communicated.
- What further action and guidance is needed to fill gaps and compel SMEs to implement better security measures to safeguard information assets and the data rights of citizens.

These findings and recommendations are based on research, interviews and workshops with selected SMEs, representative SME bodies, leading IT and Security institutes, recognised experts in the field, and current suppliers of security guidance (including industry bodies, government authorities and law enforcement agencies). They also take account of the views of large customers of SMEs, who face potential security risks from contracting out services to small companies, and who are applying growing, commercial pressure for higher security standards across their supply chains.

The timing of this report is significant as many SMEs are now moving towards Internet based ‘cloud computing’ services, which offer new business risks and security opportunities for securing sensitive information. Many research and security institutes are currently studying this area and several guidelines have recently been published. No significant educational material is currently available to cover this area. Existing security advice will need to be adapted to take account of this new dimension. Delivering appropriate and accessible advice on this subject to SMEs, who will be the major consumers of these services, will be both crucial and challenging.

Problem statement

Threats to the security and privacy of information are a concern to organisations of all sizes. There is substantial evidence[1], however, that many SMEs do not implement sufficient security and privacy protection to safeguard their potentially valuable, critical or sensitive information. Most are uninformed about legal and compliance obligations, and they lack the insight or motivation needed even to implement simple, inexpensive measures, such as instilling a more responsible security culture. The vast majority of SMEs regard security as 'somebody else's problem', or at least wish that this was so, and seek to minimise their commitment and involvement. This last point has been a consistent view expressed by all SME bodies and experts consulted.

This endemic attitude has been encouraged by sales pitches for new technology which promote the business benefits, but rarely mention difficult areas such as security which might impede the sale. Allied to this are a range of factors and obstacles which SMEs face, including unfamiliarity, more pressing priorities, tight constraints on money and resources, and a general desire to ignore anything that is not directly involved with business survival and growth. Many SMEs find security complex, technical and confusing, and will be sceptical about the business case. They lack the knowledge, expertise and experience to identify and manage the risks, and cannot call on in-house specialists. Even where budget is available, SMEs face the difficulty of identifying and procuring reliable and trustworthy specialist support.

The level of complacency amongst SMEs is a growing concern both to large business customers and to individual consumers. Yet during a series of recent SME focus groups conducted by the Business Crime Reduction Centre in support of a Technology Strategy Board research project, typical comments included: "It will never happen to us"; "Why would someone want to target our business and computer systems?"; "The business has nothing that a hacker would want to steal"; and "What is the threat? I cannot see it!"

Most directors lack the time and inclination to engage with the issues and the possible remedies. Marketing managers and business advisers view security products and advice as a 'grudge purchase' because owners, directors and managers don't 'own' the security problem. They are unwilling to expend valuable time or money unless compelled to act. Instead, they seek to avoid the issue or pass it on to their IT suppliers. When faced with security demands or regulatory compliance requirements from large customers, the natural inclination is to see if they can charge extra for security overheads.

Part of the problem rests with large business customers who aim to drive down their costs by contracting out work to small companies but provide little or no guidance or

---

[1] This evidence is largely anecdotal, gathered from consultants to SMEs, business crime reduction units and SME focus groups assembled for research projects.

facilities. Several large customer security managers expressed concern that their business managers employed SMEs with inadequate security but felt unable and unwilling to intervene. One SME operating in the information security market confided that they were surprised that business customers preferred to pass them highly sensitive information to load on their equipment, rather than provide secure facilities to view and process it.

A growing body of guidance is available to larger organisations through institutes, standards groups and private security circles. Much of this is developed by experts from a corporate background and not directly applicable to SMEs. Very little guidance has been developed specifically for SMEs, despite the fact that they represent a major part of the UK information economy. The result is that there remains a low awareness of security requirements amongst SMEs, even in sectors that handle sensitive, personal information, such as the legal profession.

The scope for improvement is large and a major national concern. SMEs represent an important sector of the British and European economies. They are a major source of entrepreneurial skills, innovation and employment. More than 4 million micro businesses exist in the UK, the vast majority of which rely heavily on information systems to run their business operations. Across the European Union, SMEs provide around 65 million jobs and represent 99% of all enterprises.

Much more is at stake than the risk of some small enterprises failing. The weak security posture of SMEs in handing sensitive information is the ‘soft underbelly’ of government and industry for acts of espionage, terrorism, fraud and criminal theft of information. SMEs carry out many activities on behalf of larger organisations, often involving privileged access to sensitive information or critical business services. Some SMEs handle surprisingly large amounts of sensitive personal data, and a number have been the source of large data breaches.

The problem space also extends to security vendors and their customers, as the lack of security interest, awareness and technical skills amongst SMEs discourages the wider deployment of privacy-enhancing technologies, reducing sales opportunities for security vendors and inhibiting the emergence of low-cost, affordable solutions. Most security products are aimed almost exclusively at the corporate sector, especially financial services or central government markets. Price points reflect the deep pockets of large organisations that are compelled to purchase them to meet mandatory regulations. Solutions are driven by security specialists to meet policies set at board level. When vendors are planning or marketing a security product, it is understandable to chase such ‘low hanging fruit’.

Persuading key decision makers in SMEs to modify their attitudes and behaviour, especially in a *sustainable* way, is a challenging task. The most important and first hurdle is to change the perception and attitude of SME directors. Unless security advice is welcome, compelling and linked to business drivers and personal interest, it

will have no impact. Given the resource constraints that SMEs work within, such advice needs to be highly selective, presented in the most appropriate form and clearly signposted through the most accessible and authoritative channels.

Achieving a change in attitudes and behaviour also demands more than just good communication of security and privacy requirements. It requires attention to financial, operational and psychological drivers and barriers to change. SMEs need to be *persuaded* to apply security measures, not just informed about security, or 'sold' the problem.

SMEs can be made legally or contractually responsible for implementing privacy safeguards, but compliance cannot be guaranteed merely by cascading security standards that have been designed primarily for larger organisations. One reason for this is the lack of awareness amongst SMEs of the relevance and implications of current compliance requirements. Another is the different mindset and operational style of SMEs, where employees are rarely obliged and less inclined to consult company policies (even if they exist) and have limited, if any, access to professional expertise and resources.

Because the failings in SMEs are hard to address, many people have assumed that little can be done to improve security in this sector. An effective intervention in the SME sector, however, can have a significant impact on the national security and privacy compliance posture, because the majority of jobs are provided by this sector and this offers a major opportunity to influence the attitudes of the population as a whole. But the solutions required are different from those designed for large organisations. Guidance for SMEs needs to be based not only on knowledge of the subject area, but also a sound understanding of the factors that underpin their business instincts and behaviour.

What is an SME?

The acronym SME is an internationally recognised abbreviation for 'small and medium sized enterprises'. SMEs are an important sector of the economy, representing more than 99% of all enterprises in the UK and Europe, and responsible for employing the majority of the national workforce.

The European Commission defines three categories of SME: micro, small and medium. These are differentiated by size of headcount, turnover and balance sheet. For the purposes of the suitability of security advice and countermeasures, the most significant of these criteria is headcount, as this is the primary influence on organisation structure, working methods, culture and IT services. In fact micro enterprises of less than ten staff have markedly different security needs from small enterprises of less than 50 staff and medium enterprises of up to 250 staff.

Decisions are made differently in the SME sector than in the corporate world or in central government. Policy is a foreign concept to most SMEs, especially towards

the base of the pyramid. If policy documents are demanded by investors or customers, they tend to be quickly created and filed away without further action. Since the owners, the board and the management are often the same individuals, decision making is less formal and more difficult to influence. Time away from the ‘coalface’ is strictly limited and often regarded as unproductive.

There are several other relevant characteristics of SMEs that serve to shape their approach to security. The first is industry sector, which affects the sensitivity the information involved, as well as the associated security threats and compliance requirements. Clearly an engineering company has a markedly different security risk profile from a private clinic handling sensitive patient records on high profile individuals.

A second major influence is age and operational maturity, which generally influences the levels of established procedures and prior incident experience. Many security controls need to be embedded in established management systems and operating procedures. This is harder for a start up company, but on the other hand a new enterprise it is more likely to have newer IT operating systems with greater security potential.

Other characteristics that are likely to influence the approach taken to security include ownership structure, investment sources and management style. The personal views of the directors and the values and strategies adopted also have a significant impact. These criteria are useful for identifying common characteristics amongst SMEs.

Addressing the SME sector

Addressing the SME sector as a whole is a major challenge, as it is essentially a large collection of interrelated markets serving consumers, other SMEs and, increasingly, the larger corporate sector. Most marketing initiatives select and research a target market, and adapt their promotional material and communications plans accordingly. A more targeted approach will be more complex but far more effective for promoting information security advice. There are identifiable opportunities for taking such a strategy forward.

Towards the top end of the sector, many medium companies begin to have similar security needs to large enterprises, but with identifiable differences. This makes it easier to craft common approaches and messages. These organisations are also more likely to take regulatory compliance seriously and to assign security responsibility to a named person or small team, at least on part-time basis. They have fewer resources and less stamina than larger enterprises, however, when it comes to facing up to major security challenges.

Diversity is greatest at the micro end of the sector, which presents challenges for outreach, but there are groups that can be more easily targeted. Start-up companies,

for example, are a strand worth singling out for special attention, as they can be most easily targeted through grant funding and other forms of support, and typically have aspirations to grow. But many micro companies, such as IFAs and plumbers for example, are destined to stay small and will be less inclined to emulate practices from larger organisations or to adopt maturity models that offer a longer term path to more professional governance processes. In fact, relatively few companies make the transition from micro through small, to medium enterprise, and this is usually a slow process, often with lengthy stops along the way.

Professional firms, such as lawyers, accountants and IFAs, are also a useful strand to target as they are more likely to be motivated by security threats and related business opportunities, and are obliged to be seen to be acting professionally. They can also be targeted through industry sector or regulatory bodies (such as the SRA). Such channels are a useful focus for engagement as they are generally familiar with corporate governance processes and capable of supporting initiatives to enhance security awareness, compliance and audit.

The insurance industry is well placed to address security as risks and risk assessment processes underpin their core business, though they have been generally slow to recognise security risks and the associated commercial opportunities. Many SMEs are cost-sensitive but require insurance, such as solicitor's cover, to meet mandatory compliance requirements. Insurers are also in a position to demand evidence of security or self-certification as a condition of cover, which can serve as a powerful motivator for clients to identify and address security risks, and perhaps enable reduced premiums in some circumstances.

The impact of enterprise size on security

The most important differentiator for the design of security advice is the size of the enterprise. Complexity and efficiency of business operations change substantially with the size of an enterprise, and this has a major impact on structure, priorities and working methods. A one-person operation is relatively efficient, with no staff management and communication overheads. As the company grows, the level of productivity initially falls as communications overheads grow and responsibilities overlap, then rises as the work becomes structured, specialised and increasingly anonymous. The number of relationships grows slowly at first, but the rate of this growth is exponential and increases with size. All of this dictates the speed and the way that decisions are made. In companies of less than 50 staff, personal relationships dominate and most decisions will be made by managing directors and their immediate associates.

Up to a level of around 150 staff, relationships are manageable and efforts can be easily aligned. Beyond this point, the group becomes large and complex. It is forced to split into units and an anonymous culture will set in. Start up companies often begin as a partnership, then grow to family, then a tribe, and ultimately to a faceless

community. At each stage there is a change in culture, structure and working methods. In particular, the need for policies, procedures, committees, controls and audits grows with size. Governance mechanisms and documentation dominate the information security solution space in large organisations.

Security priorities and countermeasures change with enterprise size. Many control objectives are the same, but the urgency and affordability of countermeasures will be different. Security advice, standards and recommended solutions need to be tiered to take account of this. Figure 1 below illustrates this point.

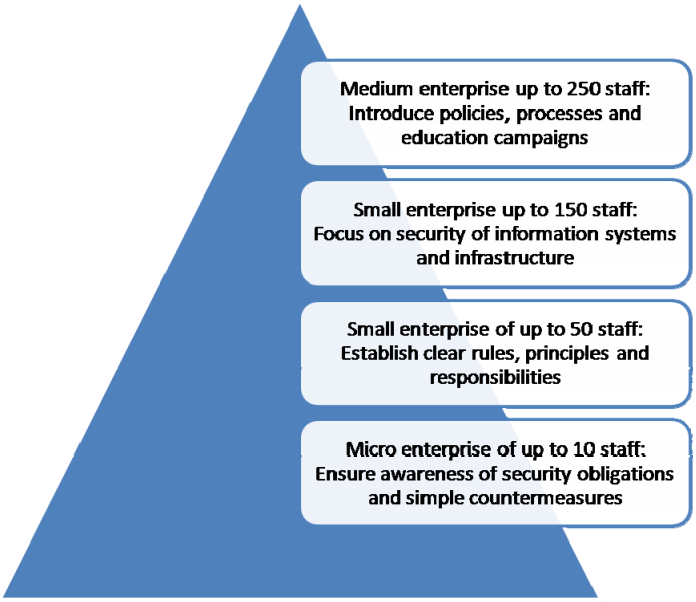

Figure 1 – The impact of enterprise size on security priorities

Most of the leading standards and management frameworks for information security were originally developed by or for large organisations[2]. The consequences of this can be seen in their presentation, which generally have a strong emphasis on policy, organisation and compliance requirements. They are not suitable for SMEs who have a different perspective and attitude, responding primarily to practical drivers such as sales opportunities, rather than policy requirements.

Drivers and blockers for security

Security drivers

Large businesses are driven by policies and strategy set by the executive board, and delivered by executive management. In large companies, security programmes are developed in an environment with a long term, proactive focus. Decisions and working practices are shaped by corporate policy and governance processes.

---

[2] An example is the international standard ISO/IEC 27002, the content of which was originally developed by, and for, large organisations, such as Shell, BT and Unilever.

Managers often compete for the maximum staff and budget available. Professional security managers are employed, often in large numbers. Major decisions affecting the enterprise are made by committees, rather than individuals. Strategies and programmes can stretch over several years. Regulatory compliance is a major driver of change.

In marked contrast, small companies are characterised by a predominantly short term, 'just in time' focus, in which costs are minimised, cash flow is carefully managed, and changes driven primarily by customer demands, and the need to win and retain business. The smaller the business, the more they are obliged to 'chase the money' rather than be driven by a set corporate strategy. Professional security managers are rarely employed and decisions are often made quickly by business managers on the basis of short term needs and priorities. Regulatory compliance is rarely a driver for change, unless there is an immediate, identified threat to the business. Figure 2 below illustrates the primary drivers of small companies.

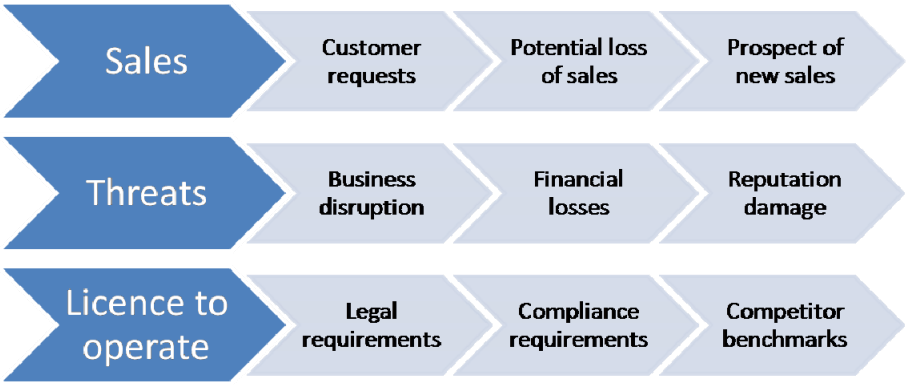

Figure 2 – Security drivers for small companies

Specific drivers for implementing security in SMEs are likely to include the following.

- Demands by customers.
- A perceived threat of losing an important customer.
- A realistic prospect of gaining new business.
- Recognition that it is part of the perceived 'license to operate' within the sector.
- Visible and externally auditable regulatory compliance requirements.
- The desire to avoiding a potential loss.
- The potential for reputation damage, from a major security breach for example.

A relatively new and potentially powerful driver is growing pressure from larger customer organisations to address the need for security in contracts with suppliers who need access to personal information. This trend is reinforced by mandatory

guidance from supervisory bodies such as the Financial Services Agency and the Office of Government Commerce[3].

Security blockers

At the same time, there are a number of blockers and constraints for implementing security, including issues such as the following.

- Insufficient time, desire and priority to understand or address the need for security.
- Ignorance of what needs to be done.
- Lack of cash or credit, especially following a recession.
- No expertise or suitable resources available.
- A 'just in time', short term focus.
- Perception that security is an unnecessary overhead.
- An aversion to paperwork, policies and procedures.
- A perception that security is something for techies, not business people.
- A feeling that the enterprise is too small to be affected.
- Operating in an environment that demands and accepts a high tolerance of risks.

Education and awareness campaigns and material need to focus on engagement with the target audience and promoting the drivers and explaining how the blockers and constraints can be overcome. Blockers such as ignorance and a shortage of management time and expertise are easier to overcome than an absence of money and a shortage of management time and resources.

Presentation of security advice should reflect this, with priority given to measures on which decisions can be reached quickly and which have fewer obstacles to implementation, as illustrated in Figure 3.

[3] The FSA warns that "Firms have an obligation to look after customer data even when the process has been outsourced to a third party, including mail shot providers and couriers". OGC has set mandatory requirements for government contracts involving personal or other confidential information. These requirements include the need for staff vetting as well as controls to safeguard the confidentiality, integrity and availability of the data. The Data Protection Act 1998 also stipulates that the data controller remains responsible for the personal data when the processing is outsourced.

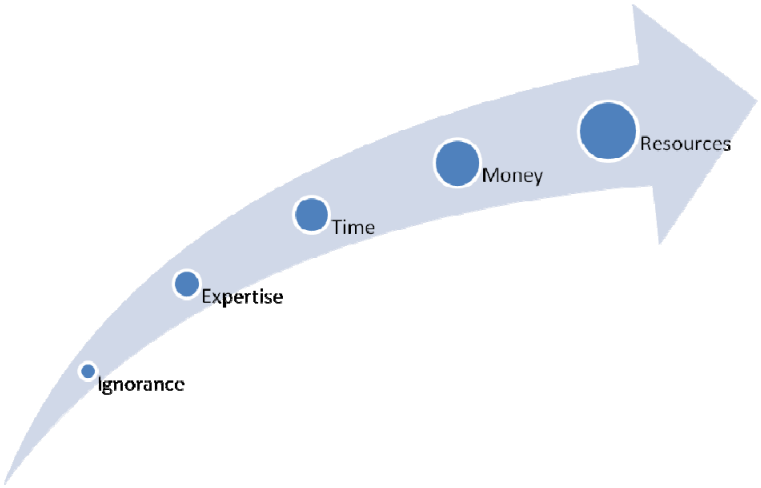

Figure 3 - Smaller obstacles should be tackled first

Mental models of security

Every director and employee has a personal perception of information security that helps shape their attitudes and behaviour. Some of these mental models are positive ones, such as the thought of gaining the trust of customers and business partners. Emphasising such an image will help convey the business-enabling qualities of security. Other mental models are more sinister, such as the thought of criminals or spies. Such images might help to scare a complacent director into paying more attention to security. Some models are negative ones, which might discourage a director from listening further. Examples of these might be a perception of information security as a bureaucratic demand, for yet more documentation, which should be avoided, or a highly technical matter that should be left to their computer suppliers. Figure 4 below illustrates some common images associated with information security.

Figure 4 - Common images associated with information security

The most common mental model, and the one that is most used for education campaigns and awareness materials is that of physical security items such as safes, padlocks, chains, locks and keys. The disadvantage of this image is that it carries a suggestion of expensive countermeasures and restrictions on access to information. A more positive image would be one that represents an important business benefit and enabler, such as the handshake illustrated above. Images should aim to convey the importance of trust, reliability and responsibility, rather than aiming to instil fear into a business director, who is likely to have a relatively high risk tolerance.

Slogans and titles can also have a major impact on perception and attitude. Phrases such as “Get Safe Online” can convey a subtle an underlying message that the Internet is, or can easily be made, secure. Most current guidance also mixes subjects such as safety, privacy, security, assurance and crime prevention, which share common strands and solutions, but can have very different drivers. Guidance that emphasises a single issue, such as crime or child safety, will not be taken up by companies who face a different set of drivers. Such advice would have greater impact with more SMEs if it were also to mention other common drivers.

Security advice requirements of SMEs

General requirements

SMEs require a range of advice and solutions, from simple tips on relatively low cost policy and awareness measures to more sophisticated, technology solutions that require specialist external advice. Unlike large organisations - where advice received can be specifically tailored to the organisation by corporate centre specialists - advice aimed at SMEs needs to be designed for direct presentation to the target audience, or for easy adaption, with a minimum of tailoring.

In particular, guidance delivered to SMEs must be clear, succinct and compelling, and provide a clear path for decision making and action enabling managers without technical training or security experience to:

- Appreciate the importance of security and privacy protection.
- Grasp the implications of increasing customer and compliance expectations.
- Be motivated to instil a healthy security and privacy culture.
- Place a value on personal information.
- Understand the root causes of data breaches.
- Identify and assess security risks to data and their impact.
- Understand the range of protective measures available.
- Appreciate the costs and benefits of privacy protection.
- Build security and privacy controls into new systems and processes.
- Specify security and privacy in contracts with suppliers.
- Understand when and how to obtain specialist external support.

These requirements are not dissimilar from those of large organisations, but awareness materials aimed at SMEs need to be presented in a simple fashion that provides the minimum essential information alongside compelling arguments that strike a chord with business managers. This requires careful consideration of the business drivers, constraints and priorities of SMEs, as well as the most appropriate analogies and 'mental models' to communicate key concepts.

Effective security privacy protection encompasses a broad range of measures implemented through people, process and technology. The range of interventions required includes the need for policy, process improvements and technical measures, as well as measures to enhance attitude, awareness and motivation. In particular it needs to include measures that contribute to sustainable improvements in culture and practice.

As discussed earlier, security priorities and capabilities vary with the size of the enterprise. Ideally the presentation of material should be tiered to reflect this, as illustrated in Figure 5 below. It should be noted that there is a clear hierarchy of needs, building from simple, basic measures to sophisticated countermeasures and initiatives.

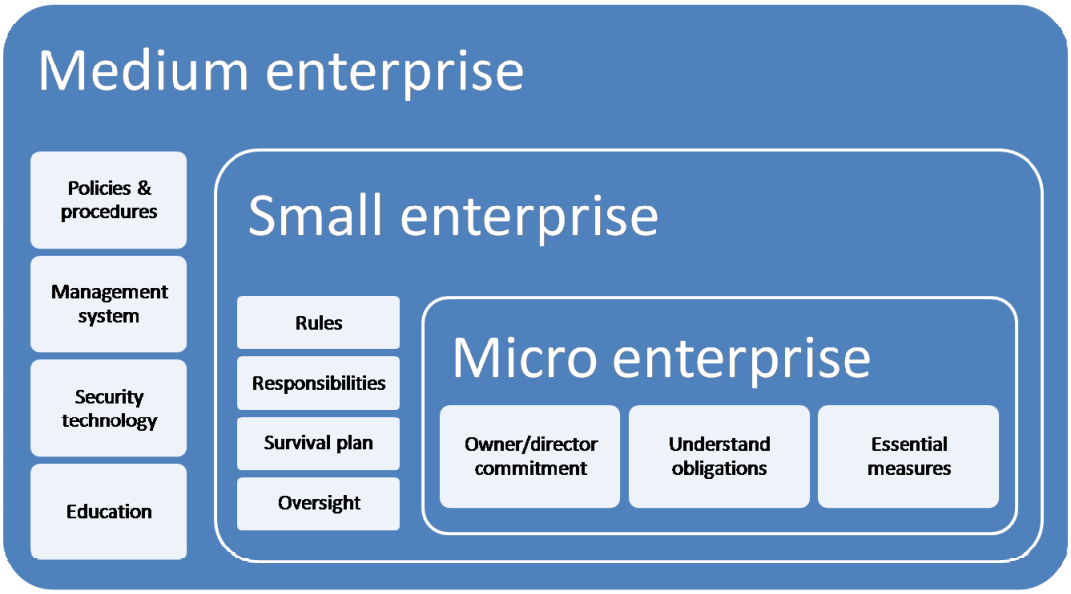

Figure 5 - Illustration of how security advice can be tiered to reflect enterprise size

Changing attitudes and behaviour

Initiatives to improve the security posture of organisations need to go beyond good communications of key facts. They also need to include arguments to shape *attitudes*, as well as incentives to influence actual *behaviour*. All three components must be present to guarantee that the advice presented will be positively received and acted on.

Communicating knowledge is a relatively easy task, though it does require an appreciation of the mindset of the audience and a degree of ‘stickiness’ to ensure the recipients pay attention and that messages are understood and remembered. Effective techniques include the use of analogies (motoring is a popular theme for security) which enable people to relate new concepts to familiar experiences. Questions are also useful devices to reinforce communications as they encourage the recipient to think more about the subject.

Changing attitudes is harder. It cannot be done by simply arguing the facts, but requires a process of self-discovery, through a learning experience such as reading a story, watching a film or engaging in a discussion. Case studies are powerful vehicles for changing attitudes. Opportunities also arise when an incident occurs within a related business.

Achieving an actual change in behaviour is generally the hardest challenge of all. It requires careful consideration of the type of behaviours to be encouraged (or discouraged) and identification of incentives to help leverage them. Motivators might be threats or rewards. But simple cues and reminders are also important.

Channels of advice
A number of different channels of advice are needed to enable the maximum impact with the broadest range of enterprises. These include the following.

- Internet web sites
- Leaflets and booklets
- Local support through SME circles and business crime reduction units
- Seminars, webcasts and training from IT and security vendors
- Helpdesk telephone support

Each channel offers different strengths and weaknesses:

Internet sites are the primary source of information, providing a ‘24 x7’ source of advice to wherever you happen to be located. Identifying suitable, reliable and up-to-date information is a major challenge, however, without advice on where to look.

Leaflets and booklets are useful for handing out at exhibitions, and help to whet the appetite of those reading them, but they are a ‘push’ rather than a ‘pull’ mechanism, and their general, high level content rarely convey sufficient information to enable an enterprise to take action.

Direct local support is often the most effective source of advice, but can only be done on a highly selective basis and is largely ‘preaching to the converted’. There is a need, and therefore an opportunity, to provide advice to SMEs following a security incident, which is likely to have a much bigger business impact on a small enterprise than a large organisation.

Seminars and webcasts from vendors are a growing source of free, up-to-date, expert advice but they lack independence, and can be hard for SMEs to find out about. Advice on where to look and what to expect is a pre-requisite for exploiting this source.

Telephone support is offered by several regional agencies, but it is only as good as the expertise, experience and information available to the operators. This is, however, a source that, if suitably equipped, can deliver the essential support needed to help find further relevant, authoritative and reliable sources of specialist advice and support.

Presentation of information

These messages need to be prioritised and structured to aid communications. An example of a useful structure that would provide efficient navigation for an SME seeking security advice is given in Figure 6 below.

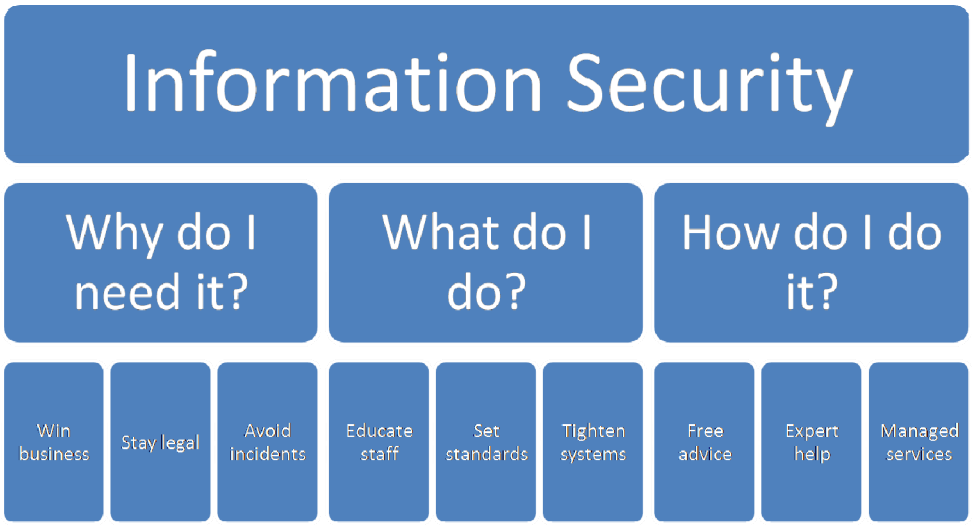

Figure 6 – An example of an efficient structure for SME security guidance

Sources of public advice

Evaluation criteria

The project team identified and examined a wide range of sources providing guidance specifically or partially aimed at SMEs. This encompassed Internet sites, publications and local support organisations, as well as national initiatives, such as ISAF and WARPs (see below) to help coordinate information awareness. Because of the very large and diverse amount of information and sources available, it was only practical to carry out a detailed evaluation of material published by the most significant sources of advice, which were primarily public Internet sites.

Major sources of security advice were analysed to assess their suitability for SMEs. The criteria used for evaluating each source were the following.

- Relevance to SMEs: how well it focuses on small enterprise needs, as opposed to big company practice
- Appropriateness of scope and coverage: is the information complete? (no important items missing)
- Correctness of advice
- Up-to-date, and likely to stay that way
- Quality of material
- Presentation of information

Internet sites
Detailed reviews were carried out of the following Internet sites, which were selected primarily for their significant amount of content, or because they are logical starting places for SME organisations to look when seeking information.

Jointly sponsored sites:

- Get Safe Online

Central Government sites:

- CPNI (General security advice, not aimed at SMEs)
- BIS Information Security Business Advice

Business crime reduction sites:

- BCRC
- e-Crime Wales

IT/Security vendor sites:

- Microsoft Small Business Centre - Security Guidance Centre

SME business advisory sites:

- MYCCI “Bob’s business”
- Federation of Small Businesses (FSB)
- Business Link: IT & e-commerce advice

The purpose and background of sites, together with some general comments on their suitability are summarised below. An overall analysis of the findings is also given, together with a comparison for the relative coverage and suitability of more specific advice for a range of individual subject areas.

Get Safe Online
Get Safe Online is a UK national initiative to teach citizens about computer security and internet privacy. It was launched in October 2005 with the backing of several government departments, and the support and sponsorship of a number of private sector companies. The campaign's centre point is its website where people can go to

get information about internet safety, how to protect themselves online, and other practical advice. Amongst other things the site offers a ten minute guide for beginners, as well as more technical information and guidance for businesses and home users. Get Safe Online is widely supported and promoted by government security agencies and leading institutes as the major national source of security advice. The major focus is on criminal threats to citizens, though the site also gives advice to small businesses. Navigation is the main problem for SMEs, as there is a lot of material on many different subjects. A small company would find some of the advice helpful, but might be deterred by the wide range of subjects and the opening set of guidance which overemphasises the importance of planning and documentation, and refers the reader to an old and excessively detailed IETC guideline. There is a leaflet aimed specifically at small enterprises, but it is a high level one, designed to whet the appetite rather than deliver prescriptive advice. Get Safe Online is an important, established source of guidance and well supported across government, industry and academia. A Google search on this title attracts close to 100 million Google search hits. As such it is a national asset that merits further support and investment.

Reference: http://www.getsafeonline.org

Centre for the protection of national infrastructure (CPNI)
CPNI is the government authority that provides protective security advice to businesses and organisations across the national infrastructure. The advice aims to reduce the vulnerability of the national infrastructure to terrorism and other threats, keeping the UK's essential services safer. Although not specifically aimed at SMEs, CPNI provides integrated security advice, combining information, personnel and physical, to the businesses and organisations which make up the national infrastructure. Its advisers cover a range of security disciplines and are experienced in providing advice to national organisations. There is plenty of detailed, independent and authoritative security advice of the CPNI website, though it is not primarily designed for small organisations. SMEs can however find useful information on major security threats, risk management, business continuity and physical security. It is also one of the few sites that publish detailed advice on personnel security.

Reference: http://www.cpni.gov.uk

BIS Information Security Business Advice
The Department for Business, Innovation and Skills (BIS) creates the policy critical to grow the economy, from higher education, skills and science to innovation, enterprise and business, including the strategy to help businesses create the jobs of the future. BIS is therefore a major stakeholder in the task of building the information security capability of SMEs, and has, over the years, sponsored and published a range of guidelines for organisations of all sizes. BIS is a natural source of advice for small companies seeking security advice and it provides a wide range of publications on a variety of issues, including information security, cyber trust and crime

prevention, though few of these are suitable for SMEs and many are out of date. In partnership with Mid Yorkshire Chamber of Commerce & Industry (MYCCI), BIS has also helped to produce an interactive e-learning package (see below). BIS has just announced that it intends to invest £4.3 million in combating fraudsters, criminals and rogue traders who use the internet and email to con consumers. It intends to form a new, specialist cyber enforcement team and provide extra funding for trading standards. There are no publicised plans, however, to invest in security advice for SMEs.

Reference: http://www.bis.gov.uk/policies/business-sectors/information-security/business-advice

Business Crime Reduction Centre

The Business Crime Reduction Centre (BCRC) is an initiative which is designed to help SMEs in the South Yorkshire area tackle problems caused by crime. Amongst a range of advice and services to local companies, it provides advice and support, including training, on electronic crime and fraud threats. The range of advice and content is similar to Get Safe Online, though it is easier to navigate, and the material is presented in a more dynamic way, as illustrated for example by the relatively 'punchy' leaflet "E-Crime - What your business needs to know". The site contains advice on other aspects of crime and security, such as metals theft and retail crime, which will be of interest to many SMEs. The BCRC site is a better starting point for SMEs than Get Safe Online for SMEs, though it is constrained by a primary focus on the criminal threat, and limited technical information.

Reference: http://www.bcrc-uk.org

e-Crime Wales

e-Crime Wales is a partnership of organisations and agencies committed to equipping Welsh businesses with the knowledge and tools to be aware, vigilant, informed and ultimately safe from the destructive effects of e-Crime. Such crime is estimated to costs Welsh businesses around £294 million every year, through direct financial or intellectual property theft, disruption of communications or damage to business-critical data. The partnership brings together police forces, specialist public sector organisations and expert commercial businesses, distributing knowledge and intelligence to enable online business to be conducted safely and securely. The advice published is very suitable for SMEs and reflects a good understanding of the roles and decision making processes in organisations, both with and without IT specialists. Advice is wide ranging, but focused and accessible, though there is a tendency to sacrifice depth of coverage for brevity. The "12 Steps to Information Security" document is expressly aimed at non-technical staff in businesses with more than one PC but no IT department, and is engaging, well written and appropriate to its audience.

Reference: http://www.ecrimewales.com

Microsoft Small Business Centre - Security Guidance Centre
Microsoft provide a range of free technical advice to SMEs on their Small Business Centre, including a self-contained Security Guidance Centre site, which includes a range of guidance on information security, data protection and fraud prevention. This site has a lot of useful, practical advice put together specifically for small business users. It is not as comprehensive as other sites in coverage, but it addresses many subjects in depth. Other vendors produce similar security guidance, but the Microsoft site has broader coverage and more relevance for small business users. As a leading supplier it is also an obvious place for small business users to look for advice.

Reference: http://www.microsoft.com/smallbusiness/security.aspx

Mid Yorkshire Chamber of Commerce & Industry
British Chambers of Commerce are an important business support network and an obvious source and place to look for advice. They deliver advice to members on many areas of compliance, but provide little leadership or advice in the area of information security. One exception is an initiative undertaken several years ago by the Mid Yorkshire Chamber of Commerce & Industry, in partnership with the Department for Business, Innovation and Skills, to produce an interactive, e-learning package. The result, “Bob’s Business”, is intended to be a practical and appealing guide to information security for staff in smaller businesses. This package is a rare example of an attempt to provide accessible material that staff can use directly, without the need for further tailoring. The principle and objectives are commendable, though the execution leaves something to be desired, as the presentation is slow, the coverage incomplete, and many people will find the tone a little condescending. The site requires registration of users, but follows a bad practice in sending an unprotected email to the user displaying the secret password.

http://www.bobs-business.co.uk/

Federation of Small Businesses (FSB)
The Federation of Small Businesses is the UK's largest campaigning pressure group promoting and protecting the interests of the self-employed and owners of small firms. Formed in 1974, it now has 215,000 members across 33 regions and 230 branches. The FSB also delivers a wide range of business services to its members, and is a natural starting point for SMEs to look for guidance on information security. Surprisingly, the FSB Internet site provides little advice on information security, other than a one-page guideline on “How Secure is my Broadband?” Unfortunately, this advice is not well suited to SMEs as it commences with a recommendation to draw up a security policy and then introduces a range of technical terms without explaining the nature of the risks, nor the business drivers for security. It would be better to signpost the way to more appropriate sources of security advice.

Reference: http://www.fsb.org.uk/it/broadband-security

Business Link: IT & e-commerce advice

Business Link is a free business advice and support service, available online and through local advisers. It aims to help businesses save time and money by providing instant access to clear, simple, and trustworthy information. The advice provided is developed in partnership with subject experts within government and relevant business-support organisations to help enterprises comply with regulations and improve their performance. It is therefore a logical first place for many SMEs to look for advice on information security advice. Business Link's IT & e-commerce web pages provide a range of guidance on data protection, risk management and IT security. The material is limited in both scope and detail but it provides a useful starting point for SMEs. It is one of the few sites that highlight the need for data protection, though in common with other sites it provides no information on other compliance requirements such as the Payment Card Industry (PCI) Data Security Standard.

Reference: http://www.businesslink.gov.uk

Other relevant awareness initiatives

Information Security Awareness Forum

The Information Security Awareness Forum (ISAF) was founded by the UK Chapter of the Information Systems Security Association in 2008, following a number of highly publicised data breaches. Its objective is to create a co-ordinated cross-industry and cross-institution approach for delivering security awareness to large corporations, SMEs and individuals. It is composed of industry bodies and professional organisations with a specific interest in promoting security awareness. The forum aims to co-ordinate the work of other organisations, rather than publishing its own awareness materials. ISAF maintains a web site at www.theisaf.org, the main objective of which is to provide information about the forum, its members, and links to other sites. For advice to SMEs, the web site directs readers to Get Safe Online and the Business Crime Reduction Centre. ISAF has also published a series of directors' guides on board responsibilities, governance and risk management. IT also promotes an information security awareness week once a year, and encourages a series of security themes, one for each month of the year.

Publications and educational material for purchase

There is a small but growing industry selling security publications, educational material and e-learning packages. British and international standards include an extensive portfolio of information security codes of practice and guidelines. Many of these are designed to be adapted to companies of all sizes, but are unsuitable for SMEs because of their length, price and focus on documentation, rather than solutions. Some vendor solutions also include thousands of pages of security policies and procedures that can be cut down and tailored to help organisations achieve ISO 27001 compliance. These packages are expensive, however, and their

content is based on big company requirements. Adapting documentation designed for large organisations is an unsatisfactory basis for SME security. Such material is unlikely to be absorbed and applied, though its possession can tick some compliance boxes. Security for SMEs is far better built upwards from a basis of simple rules and procedures that are compelling and can be easily assimilated by company staff. Educational material, such as that provided by The Security Company, a leading vendor of security awareness material for in-house use by customers, is more appropriate, as it is designed to explain security requirements in a simple way to company staff. The price of such a solution, however, is considerably above the budgets of SMEs.

Reference: http://www.i-wareness.com

Information security clubs and circles

There is a growing number of professional information security circles, institutes and clubs operating across the UK and internationally, who provide, or have the capability of developing, information security advice. Institutes and local circles tend to focus on the professional development of individuals, though some provide advice on public policy issues to citizens. Private clubs catering for corporate membership, such as the Information Security Forum (ISF), produce a large portfolio of information security guidance (some of which is published as a sample), but membership is expensive and the primary focus is on the large organisation needs. Institutes such as the UK Chapter of the Information Systems Security Association (ISSA), however, offer very good value in providing free expert advice to members in return for a modest annual subscription.

Reference: http://www.securityforum.org and http://www.issa-uk.org

Warning, advice and reporting points (WARPs)

For several years, the Centre for the Protection of the National Infrastructure (CPNI) has been promoting information sharing about security threats and incidents through a national network of warning, advice and reporting points (WARPs). WARPs provide three core services to members: firstly a filtered warning service where members receive only the security information they need, selected via an online tick-list; secondly an advice brokering service, where members can learn from other members' initiatives and experience, perhaps through a bulletin board; and thirdly a trusted sharing service, where reports are anonymised so that members can learn from each other's incidents, without fear of embarrassment or recrimination. There is certainly a strong need for local engagement, mutual support and information sharing. Many SMEs, however, are concerned about potential competition, and reluctant to share experiences with local companies in similar markets. Support networks will need to de-emphasise the concept of incident sharing in order to gain interest and engagement within the SME sector.

Overall findings of evaluation of public sources of advice

The detailed analysis of the major sources of information security advice shows a large number of gaps and overlaps. Annex A illustrates the coverage of individual subject areas on the major public Internet sites, based on searches for guidance on the following topics.

Security drivers: threats such as identity theft, online fraud, espionage, malware, equipment/media theft and disasters; as well as compliance requirements such as data protection and payment card security standards.

Governance: essential processes such as planning, policy, risk management, business continuity, audit & review and supplier selection.

Countermeasures: such as physical security, email security, anti-virus, firewalls, critical updates, access control, data encryption, end-point security, wireless security and guidance on staff education.

Annex B illustrates the suitability of this guidance for SMEs, based on a simple traffic light system.

These assessments are necessarily subjective, as most of the published advice is not consistently structured or packaged, and not well signposted. It is difficult therefore to be definitive as to what comprises an adequate or partial coverage of the subject area. (Individual members of the project team found it hard to agree on these assessments.) The ratings should be interpreted as a general indication of which subject areas are well covered, which are not fully addressed, and how appropriate the range of information is for an SME audience.

The overall findings indicate that much of the information and advice available is incomplete or fails to address the mindset, circumstances and business drivers of SME organisations. As such, most guidance is unlikely to gain their engagement, and persuade them to take action. There are exceptions. e-Crime Wales displays a good understanding of SMEs and presents the arguments and information in an engaging manner. Similarly, BCRC addresses the SME sector well, following up reported incidents and encouraging introducing a ‘prevention’ dimension as far as possible.

In general however, much of the advice available is unbalanced, unsuitable and hard both to locate and navigate. Many sites have too great an emphasis on crime prevention, big company thinking and older style countermeasures. There are items of essential advice missing from all sites, and there is very limited prescriptive guidance published that explains how to go about an important task.

Conclusions of this research review

There are major challenges in motivating SMEs to adopt security measures. The starting point is to appreciate the differences in mindset, priorities and circumstances. Most educational initiatives fail to do this (though there are one or two notable exceptions). The next step is to ensure that the motivators and benefits of security from an SME perspective are clearly conveyed. Relatively little effort has been applied to this essential step.

SMEs face many of the same security risks as large organisations, but their needs for guidance are different. Advice needs to be selective, compelling and easy to grasp, and with a clear route for further action. Most existing public sources of advice fail to achieve this. Too much material is derived from big company standards, with excessive focus on policy, documentation and governance, rather than simple practical measures.

There are notable exceptions, such as the two regional crime reduction sites, but these sites are heavily focused on crime prevention, and miss some key areas relevant to protecting sensitive data, such as espionage, data encryption and the Payment Card Industry (PCI) Data Security Standard. The lack of knowledge amongst SME retailers about PCI requirements is a concern. No organisation seems to have taken the trouble to inform them. Banks are applying supply chain pressures to remedy this, but it seems likely that many small retailers will remain unprepared and uninformed.

None of the sources of advice reviewed have comprehensive coverage of the subject area. There are gaps in individual sites, as well as inconsistencies in terminology and scope across sites. Weak areas include important measures such as data encryption, compliance, critical updates, and how to identify a suitable supplier. The latter point will become an increasing concern as ‘cloud computing’ services gain wider adoption. Current cloud services provide no guarantee of security, and it is impossible for SMEs to judge the degree of risk involved. (Larger organisations can conduct their own due diligence.)

Most security advice is in the form of online documents that are never updated. Many individual items are out of date, with a few dating back ten years or more. This is a consequence of awareness materials being developed as an ad hoc initiative or project, rather than aiming to provide a long term, sustainable service. Old advice can be misleading and should either be regularly revised or removed.

Funding and resources for security awareness generally is a major shortcoming. Given the degree of public debate surrounding the subject, there are surprisingly few programmes or initiatives addressing the subject, and the quality and slow progress in building portfolios of guidance reflects a general lack of investment in professional communications services. Where funding has been provided in the past, substantial

improvements in the quality and quantity of advice have been achieved. But there remains a lot more room for improvement.

Bodies, such as ISAF who are currently coordinating national efforts in this field also have no funding, relying entirely on the voluntary, part-time support of members. This might be adequate for overseeing the general direction of a relatively mature field, but information security awareness is an immature subject, lacking experience, skills and best practices.

Advice is not available in the places that SMEs would normally look to find it. Most would look to Business Link, Chambers of Commerce, or the Federation of Small Businesses for advice, but advice is very limited on these sites. Ideally, they should signpost the way to other sites containing more comprehensive information.

Navigation within individual web sites to find a particular piece of information is also a major challenge, especially where SME security advice is a sub-set of a more general collection of advice. e-Crime Wales is a notable exception with a good, clear, simple design. But, in general, more effort needs to be applied to efficient web site design.

Although Internet sites provide the primary channel for obtaining security advice, there are other channels of advice, as well as opportunities for supporting SMEs. The level of local support varies widely across the country, reflecting the level of initiative and investment provided by regional development agencies and business crime reduction units. Some provide specialist telephone advice and training, but others are poorly served. SMEs can be relatively hard to reach for educational campaigns, but opportunities can be generated when security incidents are reported to the police, or through sector-specific “meet the buyer” exhibitions.

Supply chain pressure from big customer organisations is a small but growing driver. Unfortunately, it encourages demands for the adoption of standards and practices that were not originally designed for small companies. The absence of a simple SME security standard and certification process, perhaps including a self-certification mechanism, is a major barrier for SMEs wishing to implement security.

Recommendations for further action

There are a number of recommendations identified in the course of the study that would substantially improve the availability, quality and effectiveness of information security advice to SMEs, as well as their level of interest and engagement in information security. Many of these are outside the scope of the ICO’s responsibilities and capabilities, but can be pursued through national institutes and bodies such as the Information Security Advisory Forum (ISAF).

Firstly, there is a need for a single, well-designed and complete high-level structure for online advice for SMEs, to enable them to navigate Internet sites seamlessly and

find the key items of information they require. Figure 6 in this report provides a useful starting point for this. This would be a relatively straightforward task for a body such as ISAF to address.

Secondly, there is a need to provide a suitably designed ‘signpost’ to security advice in places that SMEs are likely to look, such as the web sites maintained by Business Link, Chambers of Commerce, the Federation of Small Businesses, etc.

Thirdly, there is a need for simple, compelling guidance that highlights the key drivers and benefits of security that are most likely to appeal to and motivate SMEs to take action. Such guidance should take account of the mindset and circumstances of SMEs, as well as the psychological motivators that will maximise buy-in by SME directors.

Fourthly, there is a need to fill gaps in the material available, especially concerning compliance requirements such as PCI, how to conduct an audit or review, and advice on the security of emerging services such as ‘cloud computing’ that are likely to be widely taken up by SMEs.

Fifthly, there is a need to encourage and support networks amongst the SME communities that provide advice on where to go for further, reliable, specialist advice and support. It is also important to gain local engagement through ‘thought leaders’ and advisers operating within the sector, to help overcome the widespread perception of business owners and directors that privacy and information security are ‘someone else’s problem’. The current model of warning, advice and reporting points (WARPs) is not suited to the SME sector, as small enterprises are reluctant to share sensitive incident information.

Sixthly, there is a need for a simple security standard and certification process for SMEs, perhaps including, or starting with, a self-certification mechanism. Ideally, the requirements should be tiered in a hierarchical fashion geared to company size and governance style, in a similar fashion to the PCI Data Security Standard. Figure 5 in this report provides a suggestion on how this might be structured.

Finally, there is a need for further research into the decision making processes within the different strata, strands and markets within the SME sector, as surprisingly little published information is available on this subject, and a deeper understanding of the underlying influencing factors behind SME decisions would significantly improve the effectiveness of communications.

Acknowledgements

This report was prepared by David Lacey and Barry James on behalf of the Information Commissioner's Office. The research work was supported by many experts and stakeholders from large and small organisations. In particular, we are especially grateful to the following people who all provided valuable advice, without which the project could not have been completed.

Sarah Bradley	Help Ahoy
Mike Briercliffe	Briercliffe Associates
Les Fraser	ISSA-UK
Geoff Harris	ISSA-UK
Dr David King	ISAF
Paul Maloney	Technology Mgt. and Consultancy Ltd
Dr Stephen Marsh	Cabinet Office
David Ransom	Business Crime Reduction Centre
Dominic Storey	Sourcefire
Claire Taylor	Technology Mgt. and Consultancy Ltd
Gareth Venables	Yorkshire Forward
Emma Warren	Portfolio Directors
Howard Wright	Insight4Forsight

Annex A - Coverage of subject areas by sources of security advice

	Subject areas	Get Safe Online	CPNI	BIS	BCRC	e-Crime Wales	Microsoft	MYCCI	FSB	Business Link
Security drivers	Identity theft	●		●	●	●	○	○		●
	Online fraud	●		●	●	●		○		●
	Espionage		●			○	○			○
	Malware	●		●	●	●	●	○		○
	Equipment/Media Theft	●		○	●	○		○		
	Disasters			●	●	○				●
	Data Protection	●		●	●	○				●
	Payment Card Security									
Governance	Planning	○	○		○		●			
	Policy	●		●	●	○	●			○
	Risk Management	○	●	○		○				●
	Business Continuity	○	●	●	●	○				●
	Audit & Review									
	Selecting a Supplier	●		●		●				
Countermeasures	Physical Security	●	●	●	●	○				
	Email Security	●		●	●	○	●			
	Anti-virus	●		●	●	○	●		○	○
	Firewalls	●		○		○	●		○	
	Critical Updates	●		○		○				
	Access Control	●		●	○	○	●			○
	Data Encryption	●					●			
	End-point Security	●		○						
	Wireless Security	●		○	●	●				●
	Staff Education	●						○		○

○ significant partial coverage ● relatively complete coverage

Annex B - Suitability of security educational material for SMEs

Subject areas		Get Safe Online	CPNI	BIS	BCRC	e-Crime Wales	Microsoft	MYCCI	FSB	Business Link
Security drivers	Identity theft	●		●	●	●	●	●		●
	Online fraud	●		●	●	●		●		●
	Espionage		●			●	●			●
	Malware	●		●	●	●	●	●		●
	Equipment/Media Theft	●	●	●	●	●		●		
	Disasters			●	●	●				●
	Data Protection	●		●	●	●				●
	Payment Card Security									
Governance	Planning	●	●		●		●			
	Policy	●		●	●	●	●			●
	Risk Management	●	●	●		●				●
	Business Continuity	●	●	●	●	●				●
	Audit & Review									
	Selecting a Supplier	●		●		●				
Countermeasures	Physical Security	●	●	●	●	●				
	Email Security	●		●	●	●	●			
	Anti-virus	●		●	●	●	●		●	●
	Firewalls	●		●		●	●		●	
	Critical Updates	●		●		●				
	Access Control	●		●	●	●	●			●
	Data Encryption	●					●			
	End-point Security	●		●						
	Wireless Security	●		●	●	●				●
	Staff Education	●						●		●

● partially suitable coverage ● appropriate coverage