ISSA UK

Information Systems Security Association

ISSA-UK 5173

Information Security for Small and Medium Sized Enterprises

March 2011

OVERVIEW

Purpose

This paper, prepared by a working group of the ISSA (UK), sets out recommendations on information security controls for small and medium enterprises (SMEs). There are already several sources of educational advice for SMEs, but none currently aims to set a standard for information security. This document is intended to serve primarily as a reference document for helping to determine an appropriate level of security for SMEs. It is hoped that others will build on this work and develop interpretation guidelines for specific sectors or circumstances, as well as appropriate educational materials.

Introduction

SMEs are the engine of the global economy, creating employment and generating innovation and wealth. They are also attractive suppliers to larger organizations, having lower administrative overheads and faster approval processes, and can therefore respond quickly and efficiently to changing business requirements. The Achilles heel, however, is that SMEs lack the knowledge and resources needed to protect computer systems to the security standards expected by large customers, such as banks, oil companies and government ministries.

This weakness would not matter if security incidents were confined to bigger companies. Unfortunately they are not. Small enterprises are just as likely to be hit by computer viruses, laptop losses, identity theft, and failures or disasters. But they are less likely to implement security measures, whether through lack of understanding, an absence of suitable resources or simply a desire to save money. Because of this exposure, many large organizations expect suppliers to demonstrate an equivalent security standard to their own. Some supervisory bodies, such as the Financial Services Authority, the NHS, and the Office of Government Commerce, now require that contracts with third party contractors include security conditions. And while few are aware of it, every small business that processes credit and debit cards is required to comply with the Payment Card Industry Data Security Standard or face substantial risk.

Information security has therefore become a requirement for every business, small and large. It is not a matter of cybercrime, but of providing sustainable business operations and remaining competitive. In these scenarios, an online retailer who has insufficient safeguards on their customer credit data, or a local management agency whose sales lead leaves for the competition, is actually exposed more than large business. A local business which suffers an incident, even one as simple as website unavailability or the loss of a day's worth of order records, can damage business partnerships and endanger future prospects long after the actual incident.

Smaller companies, however, operate differently to big ones. They do not employ the type of formal control mechanisms found in large organizations, such as corporate policies, steering committees, full-time security managers and internal auditors. The concept of an information security management system, as required by ISO/IEC 27001, is not something that resonates with a smaller enterprise. Big company standards can be adapted for smaller enterprises, but this requires a process of risk assessment, something that small enterprises are not usually equipped or motivated to carry out when dealing with matters of information security. This particularly applies to startups and micro enterprises, some of the most innovative and potentially lucrative areas of the economy.

To be effective in an SME environment, security standards need to take account of the limited resources and options available. They need to avoid inappropriate bureaucracy, and be expressed in language that is engaging, compelling and likely to resonate with the mindset of a typical small company. This guidance sets out to achieve this goal, in order to encourage a greater level of adoption of information security measures by SMEs.

What this document is

This document attempts to start addressing the SME security challenge. This first part answers the basic questions of what the problem is, why current efforts are insufficient, and how the ISSA-5173 standard attempts to address it. Following this, on page 7, the standard is presented. As mentioned throughout this document, the concepts of scope and applicability are essential, so it is not recommended that to skip straight to reading the standard without understanding how to apply it. The standard must be tailored to the context of the business environment.

It is worth mentioning that this is not a set of prescriptive guidance that must be implemented for security. In the highly individual world of the small business, there is no such thing. As such, the ISSA-5173 working group is committed to developing guidance for each principle in the standard and releasing it as supplementary work. This is to be used selectively to help understand the control points, not as prescriptive requirements.

Instead, this standard sets out to provide a single point of clear, non-technical guidance specifically tailored to be accessible to the SME owner/manager. In addition to the above points, research[1] has shown that there is a marked absence of information security guidance available for the small business. What information exists is difficult to find and highly technical in nature, which, lacking specialist advice, increases the adoption cost of information security to a level that is not tolerable for most SMEs. As this guidance is normally oriented both for enterprise environments and for information security practitioners, this is not unexpected.

Therefore, this standard sets forth a hierarchy of three categories of control, each detailing the basic principles of information security a micro, small, or medium enterprise should pursue. Each principle is designed to minimize the administrative burden often

[1] Lacey, D. & James, B. (2010). Review of Availability of Advice on Security for Small/Medium Sized Organisations. Retrieved 14/01, 2010, from http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/review_availability_of_%20security_advice_for_sme.pdf

associated with information security, focusing on the business processes that will best provide information security as opposed to bureaucracy.

What is an SME?

Definitions vary slightly as to what constitutes an SME. The criteria can be revenue or headcount. But the most important consideration from a security perspective is the number of employees. For a 'micro business', staff numbers are generally measured in single figures, for a 'small enterprise' they will amount to several dozen, and for a 'medium organization' they can run into several hundred. The important point to note is that the methods used to govern a group of people vary with its size. In particular, the way that work is organized is different for a handful of individuals than for a large community. This is because the number of relationships within an organization grows exponentially with its size, which influences the speed and nature of decision making. In small enterprises, personal relationships will dominate. In larger ones, formal processes are needed.

Why should SMEs implement information security?

Many SMEs rely on information systems, both electronic and paper based, for essential business activities such as advertising services, capturing orders, processing payments and maintaining accounts. Good information security ensures accurate, reliable and uninterrupted operations. It prevents damaging losses from theft of equipment or data. It reduces time wasted in dealing with incidents, such as computer viruses. And it helps speed up the recovery time from equipment failures. With large customers and regulators increasingly demanding better security in supply chains, a good approach to security can help win and retain business. It is already a mandatory requirement for companies that handle sensitive data (concerning customers, employees or citizens) and for retailers that process credit cards. In the longer time, it is likely to become a key part of a company's 'license to operate' in all sectors that place a value on good information security.

What types of security measures are appropriate?

SMEs cannot be expected to embrace protective measures that are expensive, bureaucratic or demand specialist skills. Security recommendations need to be quick, simple and cheap to apply and maintain. Otherwise they will be ignored or fall into disuse. Small enterprises operate with a higher degree of improvisation. They do not employ committees for decision making or consult written policies for guidance. A good understanding of information security principles and a commitment to apply them are preferable than a hefty tome of documented policies. Physical, technical or administrative safeguards must be easy to operate and require no specialist skills or knowledge, though a small amount of outside expertise can often be beneficial to help select and install the most appropriate controls.

Larger SMEs require a degree of formal organization, but this will certainly not be as extensive as the comprehensive management systems found in large organizations. As the number of employees grows and activities become more structured, there is a greater need for defined security roles, responsibilities and oversight. Similarly, as the supporting infrastructure becomes more extensive and complex, there will be a need for better planning and stricter standards. The need for formal policies, procedures, committees,

controls and audits grows with the size of the organization. Such controls, however, will be regarded as a distractive overhead in small to medium sized organizations.

Finding the right balance between smart improvisation and strict adherence to formal processes is a difficult balance for any SME, especially one that aspires to grow. Priorities and controls will therefore need to change with enterprise size. Control objectives might remain largely the same, but their urgency and affordability will vary. Information security advice, standards and solutions should therefore be tiered to take account of such differences. Figure 1 illustrates this concept.

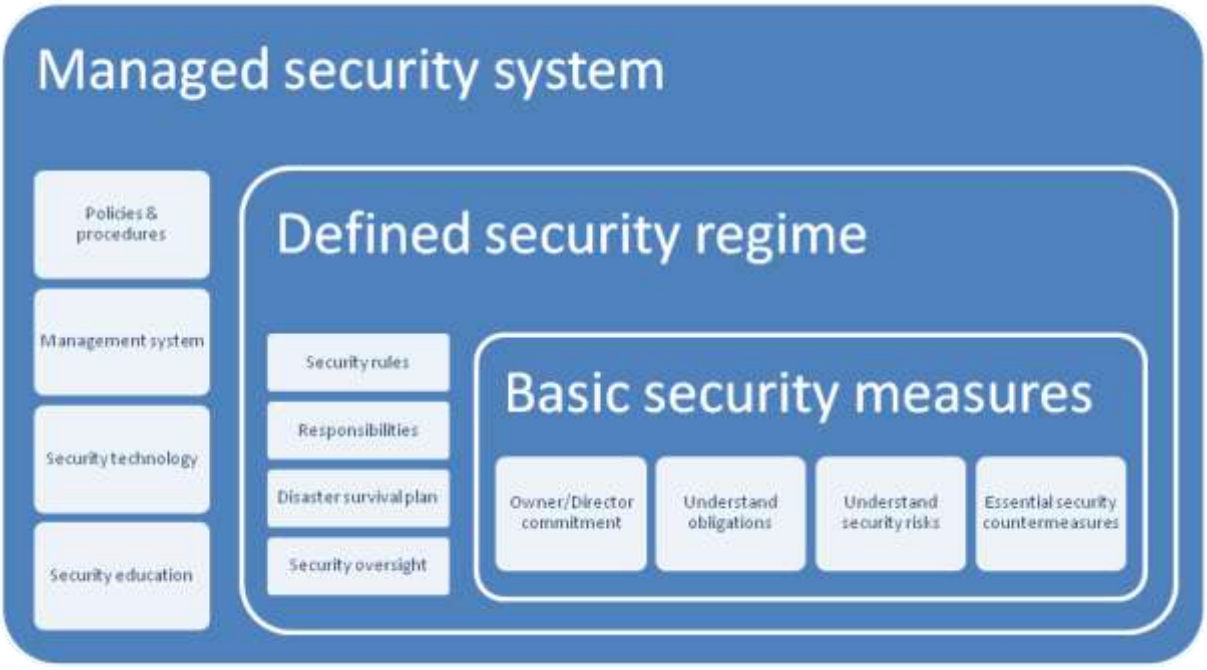

Figure 1 - An example of how security controls can be prioritized

This standard sets out a typical hierarchy of security controls that are considered to be both appropriate and affordable. In practice, some SMEs will require a higher level of security, depending on security risks, compliance requirements and customer expectations. Where possible, such additional considerations are pointed to in the descriptions. The precise requirements can, however, only be established through a professional assessment of risks, requirements and feasible solutions.

The ideal solution is for SMEs to obtain external, specialist advice in order to help then strike the right balance. It is recognised, however, that few SMEs are willing and able to invest in such support, and that there is a general shortage of skilled practitioners who are able to deliver such support. This document is intended, therefore, to provide useful advice to those SMEs who do not wish to employ external advisers, as well as indicating those areas where specialist support will be most beneficial. The standard and its related guidance does not propose to replace or replicate existing resources of use to SMEs. Instead, as few resources exist that are both accessible and understandable, it seeks to provide direction to existing informational resources where appropriate.

Compatibility with large organization standards

International security standards, such as ISO/IEC 27001, have been widely adopted by large public and private organisations across the world. The ISO standard sets out more than 130 individual security controls grouped into 11 key areas. Not all controls have to be implemented, as they can be selected on the basis of a professional risk assessment. A small or medium sized enterprise will find that such a standard contains many controls that are not relevant or appropriate to their circumstances, but might occasionally be required by a large customer or business partner to demonstrate their level of compliance. The controls set out above provide a good start to meeting the key requirements of ISO/IEC 27001, but enterprises will need to carry out a formal risk assessment and 'gap analysis' to establish their level of compliance. ISSA-UK is considering the development of a guideline to help indicate the relevance of each of the ISO/IEC 27001 controls for small companies. This guideline would be published as a separate document, subject to appropriate approvals.

Feedback

The ISSA-UK 5173 Working Group encourages other organizations to build on this standard and develop complementary guides and initiatives. In particular, further work is needed to develop materials such as:

- Educational material
- Getting started guides
- Interpretation guidance
- Implementation guidelines
- Sector specific guidance
- Country specific guidance
- Purchasing guides
- Topical checklists

While a full discussion of the project roadmap is beyond the scope of this overview, the aim is to develop a platform that makes guidance available to SMEs across all sectors, internationally. As such, ISSA-UK welcomes feedback on this standard, information on related guidance and ideas for initiatives to encourage SMEs to apply information security.

THE STANDARD

How to read this standard

This standard is organised into three categories, micro, small, and medium, each of which is comprised of four principles of information security that are relevant for SMEs. The categories are roughly analogous to the size of the SME, either in terms of staff size or revenue. Figure 1, above, displays this graphically.

This document was designed with the understanding that SMEs are highly unique entities. The context and scope of each business is the final determining factor for how much effort needs to be placed into information security measures, and organisation size is only one measure by which this can be assessed. Other factors need to be taken into account, such as the industry the SME is in, the level of proprietary or personal information that needs to be protected, regulatory exposure, and contractual requirements. While specialist advice can be sought, this is a business decision, and as such the decision to decide which principles apply to each individual SME, and how to apply them, lies squarely with the owner and/or managing director.

While the decision of what level of control is the prerogative of the business owner, it is also the case that the business owner is responsible for the security of their business operations. SMEs have a responsibility to their business partners and customers to operate in a safe, secure manner. This is a legal responsibility in many countries, due to various measures such as the Data Protection Act, and due to regulations such as PCI. This standard aims to provide accessible guidance that can be tuned to ensure SMEs meet their responsibility and, therefore, sustain their business.

1. Basic security measures

Basic security measures are those expected to be implemented by all enterprises, regardless of size or sector. In many cases, they will need to be augmented with additional measures in order to mitigate particular security risks or to meet specific regulatory compliance requirements.

1.1 Owner/Director commitment

The enterprise's commitment to information security should be promoted through a written undertaking or pledge. Such a document reinforces the commitment of management to information security, and helps communicate it to staff and stakeholders. It can take the form of a formal security policy or a simple statement, signed by the owner or

[2] Summarised: http://creativecommons.org/licenses/by-sa/3.0/
Full legal code: http://creativecommons.org/licenses/by-sa/3.0/legalcode

managing director, stating that the enterprise will aim to apply its best endeavours to safeguard sensitive data and critical business systems from security threats.

1.2 Understanding obligations

Managers and staff responsible for handling sensitive business information or controlling essential business systems must have a good, up-to-date understanding of relevant legal, regulatory and commercial requirements. Within the UK, examples of this include the Data Protection Act, Computer Misuse Act, and for retailers who process payment cards, the Payment Card Industry Data Security Standard (PCI DSS). It is also important to ensure that relevant employees are aware of any security requirements associated with commercial agreements with customers and business partners, as well as the requirements of regulators and trade associations.

1.3 Responding to security risks

Directors and managers need to understand and address the information security risks to their business assets and activities. Regular reviews should be carried out of existing and emerging security threats, such as theft of data or equipment, fire or floods, equipment failures, computer viruses or computer hacking. Consideration should also be given to the vulnerability of systems, equipment and premises to specific security threats, and the measures required to reduce the level of risk.

A range of specialist technical services are available to scan Internet-connected computers for known exposures. It is essential, however, to seek professional advice and ensure that any services or products used are appropriate and genuine, as some advertised products can be sources of malware infection.

1.4 Essential security countermeasures

Enterprises should ensure there are appropriate security measures in place to protect equipment and data from theft, damage or unauthorised access. These should include the following.

- Physical security measures for premises, such as secure entrances, intruder alarms and lockable cabinets for sensitive or valuable assets.
- Procedural controls, such as choosing appropriate passwords, not sharing login accounts, taking regular back-up copies and locking away papers and laptops when offices are vacated.
- Technical measures such as firewalls, anti-virus software, event logs and back-up storage devices. It is also particularly important to ensure critical security updates to software are promptly applied.

Many losses occur outside the office or when working in shared environments. It is important therefore to ensure that mobile devices and data are adequately protected from loss by physical security and/or data encryption.

2. Defined security regime

A defined security regime introduces additional measures that will be needed in small to medium sized enterprises to ensure that key security measures are operated consistently and efficiently, with minimal risk of misunderstandings, mistakes or duplication of effort.

2.1 Security rules

A clear list of Do's and Don'ts should be maintained to ensure that employees understand and remember to follow the essential rules needed to safeguard sensitive data and critical business services. Examples might include: "Don't share customer data with outside parties", "Lock away laptops and sensitive data when the office is vacated", or "Take regular back-up copies of data". These rules should be periodically reviewed and updated by senior management.

2.2 Security responsibilities

Individual responsibilities should be assigned for safeguarding important assets, including premises, equipment, systems and data, as well as for carrying out specific security activities, such as taking back-up copies or managing access rights to business systems and data. Deputies should be assigned for key tasks to ensure they are carried out during leave or absences. Responsibilities of partners and suppliers (e.g. software developers and service providers) should also be defined and included in contractual agreements.

2.3 Disaster survival plan

Business activities can be seriously disrupted by unpredictable hazards such fire, flooding, hacking or equipment failures. It is important to identify alternative working arrangements, such as fallback sites or systems, and to make appropriate preparations for such an event, such as drawing up a simple plan and keeping up-to-date back-up copies of essential data and software at a secure, alternative location.

2,4 Security oversight

Experience shows that, in busy working environments, security rules and procedures can easily be overlooked. Examples of this might include staff failing to take back-up copies, change passwords, or to apply critical security updates to software. An appropriate set of checks should therefore be established to ensure employees have correctly discharged their responsibilities.

3. Managed security system

A managed security system introduces additional governance measures, appropriate to larger SMEs or those with greater risks, which enable a more comprehensive set of security measures and activities to be managed efficiently. It also provides a higher degree of assurance that security policies and controls have been implemented.

3.1 Policies & procedures

A large number of ad hoc security rules and practices can be difficult to communicate and manage effectively. Formal security policies and procedures, setting out policies, responsibilities and control objectives in a structured manner are easier for staff to consult

and for managers to oversee. Procedures for key processes, such as management of access rights, issuing equipment and taking back-up copies, need to be documented as a structured set of guidance, with appropriate responsibilities assigned for updating and review.

3.2 Management system

Experience in large organisations has shown that the most effective and efficient means of managing security requirements and activities is through a 'process approach' similar to the models widely used for business process improvement. This approach encourages security activities to be planned, implemented, checked and continuously improved on a proactive, strategic basis. The adoption of such a management system requires the establishment of clear security objectives, a structured programme of security activities and a formal board to review progress against targets.

3.3 Security technology

SMEs should consider the use of specialist security technology to safeguard sensitive data and critical business systems, and to help prevent or detect potential security incidents. Examples of security technologies that are becoming increasingly essential for everyday business use include 'strong authentication' devices for secure, remote connections by home users or travelling staff, 'hard disk encryption' systems to safeguard the data on laptops, and 'intrusion prevention systems' to detect and block incoming network attacks.

3.4 Security education

Security is everyone's responsibility within a modern enterprise, so all employees need to be educated, and regularly updated and reminded of the range of security threats to business data and systems, as well as their responsibilities for reducing the risks to an acceptable level. Security education should begin with an appropriate induction session for all new staff and should be maintained through regular briefings and bulletins.