Global Information Assurance Certification Paper

Information Security Management Systems in Small & Medium Sized Enterprises

Anna Smears
GSEC v1.4b
Option 1
December 16th, 2003.

Abstract:

This paper raises the issue of security management for Small and Medium Sized Enterprises (SME). In Europe, small business accounts for 99% of the market share, yet, effort has been concentrated on large business, because large business provides around 50% of the turnover. SME's are becoming more technology dependent, and we must ensure that there is adequate and re levant advice to ensure protection of this sector, and thus the future of our economies. This paper explores these issues, and presents a simple process definition that could be relevant for S ME's to implement the foundations of their security management systems.

Table of Contents

Introduction

Traditionally, the philosophy of business was to base business cases upon a tangible need. Need had to be demonstrated visibly, and the potential gain from supplying that need. Initially, security was put aside, as no potential gain could be proven, and the intangible threat of lost revenue was not understood by the decision makers. Buy-in to security happened after the demonstration of damage that successful attacks caused. The Love bug virus in 2000 caused huge financial loses [1], and we have seen this loss repeated numerous times with Code Red and Sobig viruses etc.

Now, businesses are becoming more security aware, in that they know they need to spend more on security, however, many still lack any understanding of the problem.

There are various sources of advice, such as the British Standards Publishing Limited (BSPL) BS ISO/IEC 17799:2000 BS 7799:2000 [2], Cordis' Information Technology Security Manual [3], the NSA/CSS Infosec guides [4], and the ISF Information Security Forum [5], to name just some, but who is catering for our small businesses.

In the UK, The Small Business Service, an executive agency of the Department of Trade and Industry, published the following statistics in the 2002 National Statistics Press release [6]. The vast majority of UK enterprises (99.1 %) were small (0 to 49) employees. Only 27,000 were medium sized (49 to 250 employees), and 7,000 were large (250 or more employees.) With small businesses accounting for over 99% of the business market, should we not be targeting these companies with advice on security that is practical to their needs? Undertaking compliance with the BS ISO/IEC Security standard is a considerable undertaking, and there are few small businesses that would be able to attempt this. It could be argued that business should aim to apply the relevant parts of the standard, but is this really a viable option? Small business does not often possess enough profit to be spending money on expensive consultants to analyse their risk categories. We should be advocating good security practice, but must ensure that it is in a form that these small businesses can also apply.

---

[1] Sherter, Alain. "Love's Labour Is Banking's Loss. Bank Technology News.
URL: http://www.banktechnews.com/btn/articles/btnjun00-6.shtml

[2] British Standards Publishing Limited (BSPL) BS ISO/IEC 17799:2000 0 BS 7799:2000. British Standards Institution, London, UK

[3] Commission of the European Communities, Information Technology Security Evaluation Manual (ITSEM) V1.0, Brussels Luxembourg 1992, 1993.
URL: http://www.cordis.lu/infosec/src/down.htm

[4] NSA/CSS INFOSEC
URL: http://www.nsa.gov/isso/index.html

[5] ISF Information Security Forum
URL: http://www.securityforum.org/html/frameset.htm

[6] DTI News Release, National Statistics, August 2003, UK
URL: http://www.sbs.gov.uk/content/statistics/pressreleasesmestats.pdf

According to SME Techweb [7], an EU initiative called 'The Sixth Framework Programme' is aiming to aid technological development in SME's. " SMEs are the basis of future European competitiveness and job creation. They represent 99.8% of all EU enterprises and two-thirds of all employment. SMEs form a dynamic and heterogeneous group, and face many challenges in the European single market and in global markets. To survive and grow, SMEs must constantly innovate, which means either developing new technologies themselves or gaining access to technology developed by others."

The European Commission's Sixth Framework programme is specifically targeting SME's to develop their technology. If a concentrated effort is being made to encourage SME's to develop their technology, this means that these companies will become more technology dependent in order to operate. Security needs to be implemented alongside this technology development.

A simpler message to the smaller, less technical businesses could gain support from furthering their understanding, and by making them realise that security can play a part in their enterprise. The author suggests that all companies will be technology dependent at some point in the future, and would it not be good advice to educate these companies now to ensure security becomes part of their everyday practice.

This paper aims to improve communication with this sector of the market by offering some practical solutions that any company, no matter how small can assess and apply if relevant. It is good practice to get every company thinking about security in some fashion. A company of 5 employees is not going to sit and plan security according to the standard BS ISO/IEC 17799:2000 BS 7799:2000.

[7] CORDIS, European Commission SME Techweb, 2002 National Statistics Press Release. URL: http://sme.cordis.lu/idea/1background.cfm#1

Where security sits in an organisation?

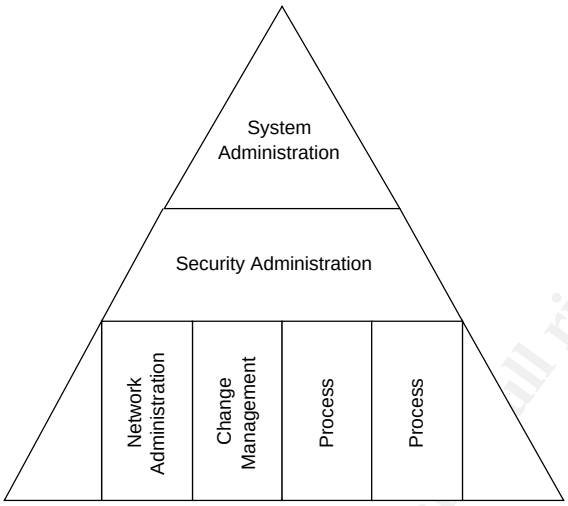

Figure 1 Relationship of security practice within the operations of an organisation[8]

As Microsoft has the largest percentage share of the SME market, this paper concentrates on the security perspective that Microsoft has to offer. Microsoft has illustrated where security should sit within an IT administrative model (see above). System administration denotes what type of security model is observed, whether it is centralised, or a distributed model that delegates control to its branches. Below system administration the operations of IT can be divided into processes, such as network administration, and change management, etc. These processes will vary according to the company operations. Security administration sits above all these operational processes, as security plays a part in each.

For example, network administration covers the handling of the physical components that make up the organisation's network, such as servers, routers, switches, and firewalls. Network administrators must ensure that such items as firewalls are correctly configured in order to ensure security, and to prevent unauthorised access.

Change management deals with the controlled change of the environment. Any change to the environment must be assessed for the impact that these changes produce, including the affect upon security. Changes should be tested and introduced in a controlled fashion. These are illustrations of how security affects system administration operations.

[8] Microsoft security Administration Operations Guide, April 2001.
URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/maintain/opsguide/secadmog.asp

There are a number of other operational processes of which security plays an important role, such as storage management, configuration management, and financial management, to name some common to most medium to large sized companies. A member of the security team should be involved in the coordination of any changes that occur to the infrastructure. Configuration management deals with keeping track of the versions of internal software; this will include critical patch updates. A member of the security team will be instrumental in identifying updates to be made. Security is involved in financial management. Due to the lack of realisation that security is more than just one core process that makes up the system administration model, but in fact permeates all other processes, there is often an underestimated assessment of the cost of security, which in turn can impact the integrity of the information system.

The message that Microsoft has to offer is a valuable one, but possibly needs to be scaled down for the smaller SME's. It is still presenting security in terms of a large Information Security Management Systems (ISMS), and is thus not really catering for a business sector in which it is predominant. Microsoft does not seem to have a Security Administration Operations Guide for its SME market.

Microsoft has made a number of statements regarding their position on security; "the need for heightened security in our increasingly connected world has elevated security to the top of Microsoft's agenda." [9]

Microsoft also states its aims for the future; " We need to make it automatic for customers to get the benefits of fixes. Eventually, our software should be so fundamentally secure that customers never even worry about it." [10]

It is pleasing to know that Microsoft is aiming so high, however, we should not be placing our faith in such 'vision' statements. For this to happen, security professionals would have had to gain the upper hand. This is currently not the case, as recently demonstrated by the MSBlaster virus. Why should we expect this to be the case in the future, when we have no evidence that this will happen? Microsoft have to place faith in their offerings, however, it would not be good planning on our part to become complacent. We need to provide SME's with education now, and try to increase their self-reliance to implement security.

Microsoft does state that it has a range of tools to implement security [11], but it is generally accepted that this range is limited. Windows Update informs of critical updates, and Software Update Services (SUS) can be used by larger companies to provide updates. Microsoft Baseline Security Analyzer (MBSA) is also a useful tool, but this is where the range ends.

[9] Microsoft Security 2003 Marketing Booklet. US, 2003.
[10] Bill Gates, Chairman and CEO, Microsoft 2002. Microsoft Security 2003 Marketing Booklet. US, 2003
[11] Microsoft Security 2003 Marketing Booklet. US, 2003.

Processes

Recently, whilst reviewing the security of an organisation, I found it difficult to make recommendations for such things as server hardening, as it was apparent that there were no operational processes in place to maintain the 'secured' servers. Security threats are dynamic, and ongoing maintenance of the systems is required to keep them up-to-date. It is for this reason that this paper is offering some security suggestions for SME's to consider when creating the fundamentals of a security organisation. The importance of the process can only be assessed by a risk analysis, and some of the processes will not be relevant to all companies; this will depend on their technological infrastructure.

A risk assessment table is provided in the prioritising section. If a small company refuses to seek external advice, the following descriptions aim to provide some understanding of the processes involved. Some risk assessment is required in order to prioritise work, as a security organisation is not built all at once.

Configuration Management

Configuration management can be applied to all areas of business, and it is important to define the scope and objectives of the process. It should be responsible for identifying, controlling and tracking all components of the IT environment. In terms of providing for the hardening of the infrastructure, it is suggested that the configuration management process should cater for the following as a minimum:

- Establishing and maintaining baseline configurations
- Document all changes to the IT environment
- Control assets by knowing what is held by the organisation.

Configuration management should also provide status accounting, and review changes to ensure product integrity. Configuration management applies to all companies, and can be implemented on a small scale.

In terms of security there are three areas suggested here where configuration management should be implemented, in order to provide structure to the following functions.

Patch management

As technology evolves, attackers develop new methods to exploit security vulnerabilities, which can then impact business operations. Security patch management is the process of identifying updates that a company should make to its servers, and the assessment of how and when these patch updates occur. A system needs to be implemented to ensure that the stability of the environment is maintained. Patch management is a primary line of defence available to organisations that are interested in protecting themselves from these threats.

Companies can apply service packs and hot fixes along with 'best practice'. Microsoft recommend that hot fixes are only applied to your environment if pertinent, for example, if there are no web servers, then hot fixes for web servers should not be implemented. The quantity of hot fixes released requires that a management process is in place to control any changes.

Once a process is defined, and the environment has been brought up to a baseline, maintenance of this baseline will reduce the number of successful attacks on business operations.

Build management

Medium sized companies may want to introduce a standardisation of builds for a number of reasons. It saves time building and rebuilding servers, and ensures that servers are built to a known state. In terms of security, this is important, as a standard build that has addressed known security risks, removes the threat of the environment being compromised due to human error during the build.

A Build Management process can be integral to a defence-in-depth strategy. Rebuilding servers that have been compromised, to restore their integrity, increases the cost of ownership, and impacts business operations. A standard build reduces the time required to restore normal operation. By concentrating on repeatable builds, change control, and audits, servers can be treated as replaceable whenever they drift from a known good state.

There are a number of benefits of a build management process. Quick diagnosis of problem servers, and recovery using standard builds is facilitated. System maintenance is simplified, thus increasing the system administrator's span of control.

Services Management

In order to maintain the integrity of server builds, all servers should have their roles defined. Examples of this categorisation are web servers, mail servers, files servers, and application servers. Each server should have all services that it is running documented, in order to assist in the management of these servers. An example of this would be that the web servers have the following services running: IIS, etc. Categorisation of these roles and services will ensure that servers are built according to a defined procedure (where they differ from the standard build), an example of this, is that all servers running IIS should have the IIS Lockdown tool applied to them.

User Management

User management encompasses all aspects of how users and their accounts are managed. User management processes are required to maintain and secure an area of the environment that is in constant flux; users' passwords change on a regular basis, new users are added, users leave, users require new access rights, distribution lists change. It is necessary to have a simple management system that details these threads of the user management process, and scales well to allow for growth, whilst maintaining the security of the environment. Examples of processes that should be covered in this category are:

- New account creation (including which type of account)
- Account amendment, (when members of staff change job within the organisation)
- Account deletion, or disabling
- Restriction of user environments
- Access controls (to resources, NTFS permissions, Group membership)
- Password controls (creation, teaching of how to create good passwords, re-setting of passwords
- Re-activation of locked accounts
- Description of appropriate use of facilities
- Description of roles and responsibilities

Domain Security Policy Management

The domain security policy is set by a number of factors, such as pass word length, duration etc, and by selecting these a domain security policy is set in place.

However, other factors to consider, and to bring under the domain security umbrella, are the administrative aspects. Some exam ples of this are:

- Administrative and special access should be kept to a minimum, and use of the administrator account should be audited.
- A dummy administrator account should be created
- A definition of what resources users have permission to access.
- What auditing should take place, and who should monitor this

A process should cover all aspects of administration, and determine how the domain security policy is reviewed, and how security policy settings are changed. Documented guidelines would aid this process. This will ensure that decisions affecting the domain policy are properly planned.

Back-up Management

Back-up management ensures that a company can minimise damage to data, should any of the live data be compromised in any way. A process for ba ckup management should cover the following as a minimum:

- Details of what back-ups are taken as standard procedure.
- Details of any non-standard back-ups required.
- Who is responsible for ensuring that all servers are backed -up.
- Who is responsible for determ ining which servers are to be backed up.
- A restore process to ensure the integrity of the back -ups.
- Regular testing of the restore process.
- Documentation on the back-up and restore procedure.
- Back-up management is responsible for the security of any off -site back-ups, and the transportation of these off -site back-ups between sites.

The strategy should cover the design process, and current back -ups taking place. The strategy should cover how the backup for each server is determined, and who's responsibil ity it is to ensure that the server is added to the back up process. Definition of procedure is recommended to ensure that there are no gaps within the backup strategy.

The level of security required for data needs to be determined. If considered to be of a sensitive nature, the co mpany should consider where back-ups are stored (off-site?), and how the transportation of tapes occurs between sites.

Physical Management

Physical management covers a number of aspects from allowing access to the building , to restricted areas within the building, to the protection of all hardware. This process should define:

- Appropriate use of facilities and equipment
- What levels of access are required for use of the facilities and equipment, and how this access will be granted

Prioritising

In order to prioritise work, each security risk needs to be assesse d. Industry suggests the following categorisation as an aid to assessing security risk.

High risk: These are flaws that are serious enough to allow a cracker to access and take control of computer systems.

Medium risk: These risks permit either a disruption for external users or unauthorised access for internal users.

Low risk: There is no industry standard definition for low risks, as they are more generic in nat ure, and are not considered to pose an immediate threat.

The following matrix can be used to prioritise work. The impact will vary depending on what the business currently has in place. Companies will have to prioritise their work depending upon the imp act, and the probability of realisation. It will indicate the areas of sec urity administration that need planning and implementation in order to provide a secure framework for the environment.

Risk Description	Priority Order	Impact	Probability that ris k is rea lised
Configuration Management			
Patch Management			
Build Management			
User Management			
Services Management			
Domain Security Policy Management			
Backup Management			
Physical Management			

For any operationally technology dependent companies, it is critical that there is a thorough assessment of any changes to the security of the servers in a test environment before any changes are made to the production environment. The test environment should mimic the production environment as closely as possible.

Testing is necessary to establish that the environment is still functional after the changes are made, but it is also essential to ensure the level of security is as intended. All changes should be thoroughly validated.

Future Development

Whilst researching this paper, I found that some banking institutions are providing basic security guidance for Internet banking users. Although of a basic level, their guidance is relevant, and very simply put. HSBC Bank plc has the following offerings, and describes it as the 'Four Golden rules' [12]. According to HSBC Bank, these four rules offer the most protection for the least effort, and encompass the following:

Security Updates and Patches
Anti-virus software
Personal Firewalls
Password Advice

This simplicity of message clearly defines measures that everyone can take, and HSBC Bank has ensured that this information is targeted correctly, in order to hit a large percentage of their users; it is a useful example of how information should be understandable by its readers.

It would be valuable to provide some kind of assessment tool for the SME market. This tool would contain a number of questions, and could even be based upon a security standard such as BS ISO/IEC 17799:2000 BS 7799:2000. Companies could answer the questions, and the data could be correlated to provide output, suggesting areas that may be of relevance to that company. It would be important to emphasise that outside technical help is advised, but where this is not going to be taken, the following measures may be suitable to implement, and would improve security. There would be certain areas where reference to outside help would be the only recommendation. This offering should form part of a non-profit making initiative. It should essentially provide small companies with the 'what to do' in the same way that BSI and other such organisations equip large companies.

[12] HSBC Bank plc
URL: http://www.hsbc.com/public/groupsite/internetsec/home/index.htm

For the configuration management such questions as below, would be asked:

What is the status of an inventory sy stem in your organisation?

If there is an inventory system, what does it track?

In terms of user management, the following would be applicable:

Have security roles and responsibilities been outlined in your job descriptions?

Is screening conducted for job applicants?

These are only a brief example of the type of questions that could form part of the security assessment tool. If pertinent information is sought, the output should prove to be of value.

In making these recommendations, we must make sure that we are targeting the correct market, otherwise, some SME's may think they are addressing security adequately when they are not.

Conclusion

The Internet changed the way information is stored, accessed, and shared. Companies are implementing a more o pen and distributed information model, and consequently need to manage the associated security risks. Security breaches and network downtime can cost organisations considerable loss of revenue, and can cause incalcul able damage to the image of the organis ation. Security is a continuous process, requiring constant monitoring and adaptation of the protection shield to accommodate system growth and changes in the environment. Process definition is required in order to manage the constant adaptation of our systems.

For some time now it has been accepted that Information security is characterised around the preservation of the following three concepts:

- Confidentiality: protecting sensitive information from unauthorised disclosure.
- Integrity: safeguarding th e accuracy and completeness of information/data.
- Availability: ensuring that information and associated services are available to users when required.

The author feels that a forth concept should be introduced – communication, and should now be brought into focus. Business is waking up to the security threat, but now it is time to stop just scaring companies to act, but also gain understanding. When a need is understood implicitly, security professionals won't have to spend so much time shouting.

Unless communication is facilitated with these companies, and they are able to implement measures quickly, the SME business sector will at some point be seriously affected by security breaches. This impact will affect the productivity of our economies. It is in our own best interest to co ncentrate more effort upon the SME section of the market to ensure future development and prosperity. Attacks will look for vulnerabilities in all areas, and if we leave some holes open, then these holes will be attacked.

References:

Sherter, Alain. "Love's Labour Is Banking's Loss. Bank Technology News.
URL: http://www.banktechnews.com/btn/articles/btnjun00_-6.shtml

British Standards Publishing Limited (BSPL) BS ISO/IEC 17799:2000 BS 7799:2000. British Standards Institution, London, UK.

Commission of the European Communities, Information Technology Security Evaluation Manual (ITSEM) V1.0, Brussels Luxembourg 1992, 1993 .
URL: http://www.cordis.lu/infosec/src/down.htm

NSA/CSS INFOSEC
URL: http://www.nsa.gov/isso/index.html

ISF Information Security Forum
URL: http://www.securityforum.org/html/frameset.htm

DTI News Release, National Statistics, August 2003, UK
URL: http://www.sbs.gov.uk/content/statistics/pressreleasesmestats.pdf

CORDIS, European Commission SME Techweb, 2002 National Statistics Press Release.
URL: http://sme.cordis.lu/idea/1background.cfm#1

Microsoft Security Administration Operations Guide, April 2001.
URL:
http://www.microsoft.com/technet/treeview/d efault.as p?url=/technet/prodtechn ol/windows2000serv/maintain/opsguide/secadmog.asp

Microsoft Security 2003 Marketing Booklet. US, 2003.

HSBC Bank p lc
URL: http://www.hsbc.c om/public/groupsite/internetsec/home/index.htm

Last Updated: July 24th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor