Global Information Assurance Certification Paper

Implementing BS7799 Part 2 in an IT organisation.
A Case Study

GSEC Practical Assignment. Version 1.4b

Marc Vaughan

Table of Content

1. Management Summary.

This case study documents the experiences of a large global Enterprise Organisation on its move to becoming BS7799 accredited.

As modern businesses are leveraging the Internet as a means of communicating with suppliers, partners and customers, IT security is becoming an important consideration.

With a variety of guidelines and standards currently available which allow Organisations to improve their security, this paper aims at providing some real life experience of a successful BS7799 implementation. Hopefully, some of the points will provide guidance for any others that wish to take the BS7799 certification path.

2 Introduction

British Standard 7799 (BS7799) was developed as a framework for security best practice. Its roots developed from the British Government's Department of Trade and Industry and in 1989 the 'Users Code of Practice' was published. This was further developed into 'a Code of Practice for Information Security Management' and published in 1995 as BS7799 Part 1.

BS7799 Part 1 is a Code of Practice and provides a security framework that should be meaningful and practical from an end user perspective. In October 1999 BS7799 Part 1 was proposed as an ISO standard and in October 2000 became ISO17799.

It has now become a de facto standard within Britain, Europe and Australia / New Zealand (AS/NZS4444). Also, over the last few years, it has spread internationally and now covers some 24 Countries across the globe (see table below).

Region	Number of Certificates	Region	Number of Certificates
Australia	**1**	Italy	**3**
Austria	**1**	Japan	**17**
Brazil	**2**	Korea	**9**
China	**3**	Norway	**6**
Egypt	**1**	Singapore	**6**
Finland	**5**	Spain	**1**
Germany	**6**	Sweden	**4**
Greece	**2**	Taiwan	**3**
Hong Kong	**6**	UAE	**1**
Hungary	**2**	UK	**74**
Iceland	**1**	USA	**3**
India	**7**		
Ireland	**3**		

Extract from http://www.xisec. com/

A second BS7799 Code of Practice was developed in February 1998, BS7799 Part 2, which provided a certification process against key controls and security measures. BS7799 Part 2 has recently been revamped and released as BS7799-2:2002 (September 2002).

Part 2 details precisely what an Organisation must do in order to become successfully certified.

An Organisation can happy adopt and abide by the BS7799 Part 1 but what makes them take the roller coaster ride to becoming certified? The disadvantages (cost, lack of understanding, complacency once certified) can be outweighed by the following advantages:-

- Providing a common framework for Organisations to develop and implement security management.
- Allow businesses to become certified against a common security framework / benchmark.
- Raise security awareness within the Organisation.
- Allow organisations to quickly implement security best practice methods.
- Reassure customers that the Organisation takes security seriously in as much that their security practices have been independently reviewed and certified.
- Help to promote inter-company trading.
- Allow an Organisation to measure their existing security against the ISO17799 standard.

The remainder of this paper details the real life experiences of an IT Organisation going through BS7799 Part 2 certification.

3 Background

In order for IT Security to be effective in any Organisation, regardless of size, a corporate stance must be clearly communicated (Wong, K & Watt, S, 1990).

An essential part of achieving this is through IT security occupying a defined position within the company infrastructure. Unless senior management clearly define IT security as a serious issue individual training programs and audits are likely to prove of little value.

Although good security practices existed within the Organisation, there was no consolidation or overall strategy, which meant that each department took a different approach and view on what was right (or wrong). Hence IT security did not occupy a defined position within the company infrastructure.

Sound security technologies had been implemented. Firewalls had been deployed to protect the organisation from 3rd party network connections and the Internet. Anti virus software had been installed on every workstation,

server and Internet gateway to provide 'security in depth' for viral infections. Physical security was strong owing to the fact that all doors had swipe card access and camera protection provided to key sites such as the Communication and Computer rooms. A perimeter fence existing around the site. Remote user access to the Network was secured by using various VPN technologies and all file server data was backed up on a regular basis.

These technologies provided a degree of protection from Confidentiality, Integrity and Availability threats to the organisation.

However these security measures had 'evolved' within the organisation due to a lack of strategic direction, no clear security policies and procedures, roles and responsibilities and management support. They had been implemented with good intentions but not thought through. This led to various issues such as:

- Lack of understanding and importance in deploying security measures. If senior management were not interested then why should the systems administrator care?
- Security Incidents were not handled with the merit that they required. There was no formal process for reporting incidents and then dealing with the incident as it progressed. No formal review of the incident took place after the event as a learning exercise.
- Staff awareness of security was low. People would talk openly to third parties over the phone about the IT infrastructure, passwords were weak and confidential information was left on desks or printers.
- IT projects did not include security as part of the project requirements, leading to poorly designed application or network infrastructure.
- Communication of security was poor. There was a lack of documentation.
- It was difficult to obtain ownership for a security requirement. No one wanted to take responsibility.

As most of the challenges faced within the organisation could be addressed by a best practice framework it was decided that BS7799 part 1 and 2 should be implemented.

4 On the road to BS7799 Certification

IT security is not a 'one size fits all' solution, as is evident in the approach of BS7799 where companies choose which controls are relevant to their operating environment. Owing to different cultures of organisations of differing sizes all infrastructure, including IT security, is also likely to differ markedly between Organisations whilst sharing some basic similarities. This point is important to bear in mind, as common sense must prevail when defining an acceptable level of security for an Organisation.

Therefore the first steps to BS7799 certification is to obtain a 'starting point' or base line where the level of acceptable risk within the organisation can be defined. This also gives IT security a visible positioning within the organisations infrastructure.

4.1 Baseline Positioning or Risk Assessment

Baseline Security - The security level adopted by the IT organisation for its own security and from a point of view of good 'due diligence' (Cazemier, J Overbeek, P & Peters, L:1999)

Carrying out a risk assessment is the best approach for providing a baseline of the IT organisations IT security infrastructure.

Risk assessment is a very important part of the computer security process. You cannot protect yourself if you do not know what you are protecting yourself against! After you know your risks, you can then plan the policies and techniques that you need to implement to reduce those risks (Garfinkel, S & Spafford, G:1996)

The risk assessment was undertaken to give a clear understanding of the organisation's security benchmark and also to identify key areas against an applicability statement. The key areas are defined from the ten BS7799 sections. Each key area was marked against the following criteria;

(i) Not applicable. Key areas are not relevant to the organisation.
(ii) Accept the risk. Risk is known and accepted by the organisation
(iii) Compliant. The correct levels of security have been taken.
(iv) Out Standing. Risk has been identified and accepted but measures are required to address the risk.

Once the risk assessment had been completed, it was easy to tell what had already been addressed, what was not applicable to the operation of the organisation and, more importantly, what was lacking. From the risk assessment a Statement of Applicability document was defined.

It quickly became apparent that a major area for improvement was not down to the implementation of technologies but in defining good policies and procedures that were clear, concise and easy to understand.

Following the risk assessment a Statement of Applicability (SOA) could be defined.

4.2. Statement of Applicability.

Having defined the SOA meant that the Organisation could now see the 'wheat from the chaff'' and focus on the areas of security that required improvements. This was a tremendous help and meant that the organisation had a clear starting point and clear direction to take in addressing some of the

areas defined in the BS7799 security framework. It set the scene for the work to follow.

5 Areas of Improvement During BS7799 Certification.

During the BS7799 certification process various areas had to be address to bring the organisation to an acceptable level that would ensure a successful outcome.

During the risk assessment stage and the development of the 'Statement of Applicability, areas for improvement were clearly identified. Some of these were technology biased, identifying the need for Intrusion detection Systems (both Network and Host IDS) and Strong Authentication (in the form of something you have and something you know – i.e. token-based technology). However the majority were procedural.

Following the identification of the level of unacceptable risk within the organisation the following important areas of improvement were addressed.

5..1 Improvements to the Corporate Security Policy.

Although a corporate security policy existed, this was updated and reissued by the Board to provide the management focus. It also provided the guidance required and was the foundation for the rest of the security initiatives to come.

5..2 Development of a Staff Training Plan.

There was a general awareness of security within the organisation but not at a consistent level. One person would feel that opening an email attachment from an unknown source was acceptable while other thought it was highly risky.

A security awareness-training plan was developed to ensure that a consistent message was present to all staff in the organisation.

5..3 Central Documentation.

Very little documentation existed within the organisation or if it did it was located in many different areas. A central repository for security documentation was developed.

All security policies and procedures had to be documented and clearly defined. This addressed the issues of awareness, communication and the uncertainty of security ownership within the organisation.

5..4 Creating a Task Force.

To ensure that security had a consolidated approach a task force was create to provide ownership for security within the organisation. The task force comprised of a representative from all department and functions within the organisation.

Representatives included application designers, NT and UNIX support, Account Management, Networks, Help Desk, Personnel department, desktop support and various senior managers.

By creating the task force it provided a synergy between the departments, provided a strategic direction and also ownership for any projects born from the group.

6 Obtaining BS7799 Certification. What has it meant?

Although there are ten key controls within the BS7799 model (the key controls are defined as either legislatively required or considered fundamental building blocks) the main areas that have had the biggest impact and contributed immensely to a successful certification are detailed below.

6.1 Management buy in

By its very nature obtaining a certification has an appeal to management. This had a great benefit as it immediately provided the focus required.

In the past small expenditures on security were difficult to justify. Now much of this is automatically accounted for. One example of this change is that, in the past, laptops were provided with no real security. Now any new purchase of a laptop automatically includes software protections and a Kensington lock to physically securing the device to the desk.
These days getting a budget for security requirements seems a little easier!

6.2 Roles and Responsibilities.

Before the advent of BS7799 within the organisation there were no clear Roles and Responsibilities for security requirements. If an incident occurred there was no clear owner for the problem, no co-ordination and no formal reporting.

Roles and responsibilities have been defined. Senior management now own the security policy, the help desk is the focal point for reporting incidents, ownership for change management has been defined etc.

This has produced better working practices within the organisation (not just in the security arena).

6.3 Staff Awareness Program

This was a major quick win in the BS7799 process and had the most impact on security. It also had the least cost to implement.

During the risk assessment it was quickly highlighted that there was a major lack in security awareness within the staff of the organisation.

Simple things such as weak passwords, not locking the screen on the PC while away from the desk, not visibly wearing security passes and leaving confidential material on the desk was prevalent.

As social engineering is the easiest way to subvert the technical security measures already in place, this was a major focus area for improvement.

All staff (including the directors and VP) have now undergone a security awareness program which was arranged through the personnel / training department (this was key to ensuring full attendance). Subjects covered were the need for strong passwords, Internet usage, email policies, wearing of ID passes etc.

Also all new starters now get the security awareness program as part of their induction into the organisation.

Another requirement of BS7799 is to ensure that at regular periods all staff has a refresher awareness presentation. This now happens at least once a year.

Following the staff awareness there has been a dramatic culture shift and security is in the foremost of people's minds.

6.4 Documentation of Policy and Procedures

A lot of good practices existing within the organisation but unfortunately most of these were not documented. Long term members of staff had grown into these practices. The difficulty was proving that these policy and procedures existed, leading to difficulties in enforcement.

Work was carried out to ensure that all policies and procedures were, updated if they already existed, and documented if they did not.

The key to success here was to ensure that these were visible to all staff. The documents have been posted on the Intranet and all senior managers responsible for a department have had hard copies to be kept within their area for reference.

The Organisation's security policy has been signed off by the Board and issued out as a high level document.

Tackling these areas not only addressed most of the key controls but also covered a vast amount of other 'none' key elements to BS7799. It is fair to say that by addressing the formal documentation of the policies and procedures and staff awareness went a long way to ensuring certification.

7 A change in Culture

There maybe some criticism on the costs and merits of becoming BS7799 certified but having gone through the process, there have been some clear benefits.

There has been a clear culture change with regards to security. Before BS7799 security had a bad image, something that put barriers in the way.

Now security is thought about on a day to day basis and actively included at the development stage of projects. In the long term this should reduce the cost of security as applications are built in with security measure, network connections are secured and operating systems are hardened before production of a service (and not after!)

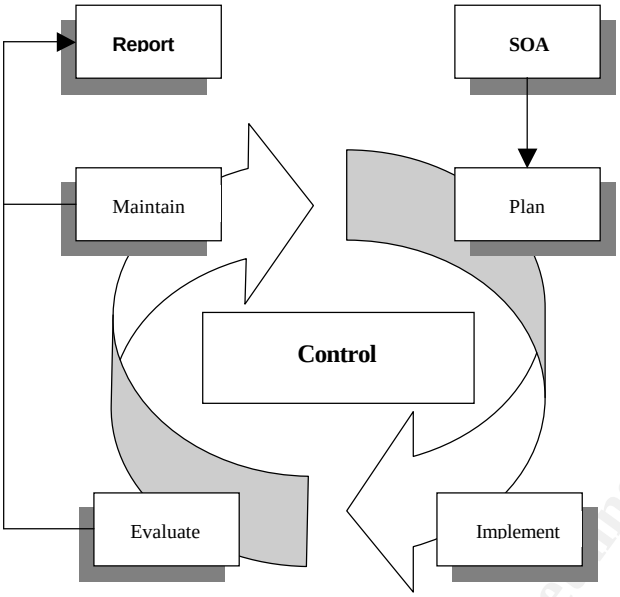
This culture change is also 'rippling' out to other organisations within the Enterprise since certification. Questions are now asked as to whether it can or should be done rather than it is being done.

8 Next Steps.

Since the IT organisation has become BS7799 certified, there are plans to implement the standards and obtain certification in other business units over the next few years. This will enforce the commitment to IT security on a global basis.

However the most important on going point is to ensure that the policies and procedures which have been put in place are continually reviewed to ensure that they meet the ever-changing world of IT security.

The process below has been adopted to ensure an effective security management. The model has been taken from the CCTA IT Infrastructure Library.



Below are some indications as to what the relevant boxes refer to in the review process.

Plan – Policy statements, Service level agreements, 3rd party contracts.
Implement – Create awareness, Personnel security, physical security, network security and incident handling.
Evaluate – internal audits, external audits, self-assessment and security incidents.
Maintain – learn and improve.
All policies and procedures are now regularly reviewed to ensure that they are still relevant and up-to-date.

9 Recommendations

Having gone through BS7799 certification some of the following points may be worthwhile considering. From experience these made an important difference to the success of our certification. Even if you do not wish to become certified they will certainly help with improving the security awareness within your organisation.

(a). Obtain senior management buy in of security and the BS7799 framework. This is imperative to ensure success.

(b). Start small. Don't bite off more than you can chew. Pick a key business unit, function or department if you are medium to large enterprise – do not be tempted to expand your horizons hurriedly.

(c) Carry out a risk assessment and produce a Statement of Applicability that is relevant to your organisation.

(d). If possible carry out periodic dummy audits to see were you stand. Carry out a gap analysis and produce a plan of action to address the gap.

(e). Good practice can be achieved through small expenditure. Staff awareness programs, in house training and a workable security policy does not have to prove expensive.

(f). Document your policies and procedures. You may have some good security practices by default but if you have not documented them then they will not mean much to an auditor. You may have to prove what you say you are doing!

(g). Clearly defined roles and responsibilities and, again, document. For example, make sure it is clear what role the help desk play in the event of a security incident, who owns your security policy, who is responsible for patching web server's etc.

(h). Finally, ensure that you have a review process in place and that it is carried out on a regular basis. Policies and procedures that are no longer relevant are no longer useful and maybe confusing – weed them out and discard.

10 Conclusion

Effective security management depends on accurate risk analysis so that the knowledge of the impact of risk and the costs of avoidance is understood. Without it, the tendency is either to ignore the risk in the hope that they will never happen, or expend disproportionate amounts of time and money on avoiding the risks of minor potential impact. Risks are an inevitable feature of life, but only manageable risks should be permitted. Security management is concerned with those activities that are required to maintain the risk at manageable proportions (Cazemier, J Overbeek, P & Peters, L:1999).

Undertaking BS7799 goes a long way in fulfilling some of the important points made in the above quote. Organisations would certainly benefit by applying the security best practice framework of ISO1799 Part. However by taking the extra decision to achieving certification of BS7799 Part 2 appears to consolidate security awareness and shift cultural views on security.

The BS7799 standard is a first step towards internationally recognised baseline security standards, against which organisation can certify themselves. Any improvements of an Organisation's computer security can only be benificial.

11 References

Internet

- http://www.iso17799resource.com/index.xalter
IS017799 Awareness / Understanding

- http://www.all.net/books/audit/bs7799.html
Summary of Controls used in BS7799.
Fred Cohen and Associates

- http://www.c-cure.org/faqs.htm
BS7799 Frequently Asked Questions

- http://www.securityauditor.net/iso17799/
ISO17799 Compliance and Positioning

- http://emea.bsi-global.com/InformationSecurity/Overview/index.xalter
Information Security
BSI Group

Literature

- Practical Unix and Internet Security, 2nd Edition.
- Simson Garfinkel & Gene Spafford. 1996 isbn 1-56592-148-8

- CCTA IT Infrastructure Library, Security Management.
Jacques Cazemier, Paul Overbeek & Louk Peters. 1999 isbn 0 11 330014 X

- Managing Information Security: A none technical management guide.
S Watt & K Wong. 1990