Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Building and Implementing an Information Security Policy

This paper describe a process of building and, implementing an Information Security Policy, identifying the important decisions regarding content, compliance, implementation, monitoring and active support, that have to be made in order to achieve an information security policy that is usable; a policy that lives and evolves as your organization infrastructure and operational requirements change and a policy that is understood and supported by management and colleagues.

Copyright SANS Institute
Author Retains Full Rights

AD

Streamline IT security environments and compliance processes.

Transforming IT Management.

Martyn Elmy-Liddiard.
GIAC Security Essentials Certification (GSEC) Version 1.4
Option 1 – Research on Topics in Information Security

Building and Implementing an Information Security Policy.

Introduction:

The purpose of this paper is to describe a process of building and, more importantly, implementing an Information Security Policy.

The paper attempts to identify the important decisions regarding content, compliance, implementation, monitoring and active support, that have to be made in order to achieve an information security policy that is usable; a policy that lives and evolves as your organisation infrastructure and operational requirements change and a policy that is understood and supported by management and colleagues.

I list the sections of a Security Policy delivery process as Active Support, Content, Monitoring, Implementation and Compliance and will herein attempt to explain what I mean under each of these topics in term of the process of delivering a workable policy.

Topic.	Description.
Active support phase 1.	Senior management support.
Content.	Research and write your policy.
Active support phase 2.	Colleague support.
Monitoring.	How do you know your policy is effective?
Implementation.	Implement the policy.
Compliance.	Map existing compliance and prioritise required work.

I hope that at the end of this paper you will have a relatively non-technical view on how you might achieve a state of collective information security within and for your organisation via a workable security policy. Further, that you will have an understanding of what is required of you and colleagues at each stage of the process, and beyond implementation, to make sure your policy remains alive and valuable in the face of changes circumstances.

Active support phase 1:

Absolute top priority in implementing a workable security policy is active support of both senior management and of colleagues from the top to the bottom of your organisation. Without this in place you will almost certainly fail to achieve your goal.

The support of senior management, by which I mean board level, is critical to obtain any required budget resource and to implement some of the harder policy elements later in the process; elements such as password policy and staff activity monitoring.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

The support of all other staff in your organisation is critical because, workable information security is, and must be, a collective exercise. A policy implemented without support may be seen as:-

- A waste of resource.
- An attempt by I.T. departments to gain/enforce control.
- A matter for I.T. and of no real relevance to non-I.T. staff.

We all know that information security is a complex, wide-ranging and often technical topic so it is very important, when selling the need for a policy to management and the requirements of the policy to colleagues that you remember one golden rule above all other :- **"Know you audience!"**

I.T. Security staff are employed to understand and deliver I.T. Security, accountants to prepare the books, finance staff to manage investments, directors to steer the organisation. In short, your colleagues are not paid to understand the detailed issues underlying information security. Therefore don't be tempted to turn your presentations into an intellectual exercise showing how clever you are and how many buzzwords you know; this will not gather support for your cause!

Directors tend to be busy people so keep presentations targeted at them, short and to the point. Make it clear at the outset that the policy does not yet exist in detail but as a framework at this stage. This isn't a mistake or lack of progress. It is quite proper to get their approval prior to starting the detailed work, indeed that is the correct way to proceed.

Remember that directors control the 'purse strings' so expect to be asked and be able to answer questions on potential policy costs.

Keep presentations as non-technical as possible but have with you technical information to back up recommendations should you be asked.

At all times present only a truthful picture, but it's quite acceptable to emphasize vulnerabilities, potential threats and the real risks that result from a combination of those vulnerabilities and threats.

It doesn't hurt to scare them a little; after all it is the directors who will be ultimately and legally responsible for the security of their organisation's information resources! Remind them of this fact.

Finally, remember you will rarely get a second chance to present to senior management.

++++++++++++++

Assuming you achieve formal approval to implement a security policy from your board, your next step might seem to be to get your colleagues 'on board'. Not so, since at this stage you will not have researched and written your policy and when it comes to getting all your colleagues 'on board' you will need to explain the detail of the policy to them; what it is, why it exists, its scope and its impact on their day to day practices.

Therefore at this point we jump to researching and writing your policy after which we shall return to presenting it to staff at all levels of your organisation.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Content:

Given the time constraints we all tend to work under these days it is very, tempting to plagiarise someone else's information security policy rather than research and write your own.

Stop and think! A policy quickly delivered may achieve short term gain for your organization but, in the long term, may well not be broad and deep enough to properly protect your organization's information assets from the wide range of potential threats. I am not suggesting we all need 're-invent the wheel' and there is certainly plenty of guidance material available on what makes a good security policy. However beyond making use of all the reference material available to you, I believe it is best to research and write a policy specific to your organization and not to take one 'of the shelf'.

The benefit of researching and writing your own policy is that the very act of doing so increases your knowledge of what your organization is about, how things work, who does what, what the I.T. infrastructure is, how it may evolve. You may well find that many assumptions you thought to be correct are indeed not so. Okay, the lead-time to having a policy ready to implement is going to be longer, but the quality of the end product is likely to be much better as will be your knowledge of managing your I.T. security going forward.

If, you take the decision to research and write a policy specific to your organisation, before you start there is one more key decision to make. You must at this point decide what your policy is and, more importantly, what it IS NOT.

At best your information security policy should deal solely with information security. "Rather obvious", you may say but in practice a good number of organisations require that their security policies encompass what may loosely be describe as behavioural, or indeed moral policy. That is to say as well as items that represent a specific security threat, they cover Internet Usage, E-mail usage, and, in the case of one I am aware of, even sexual and ethnic harassment issues. Whilst all of these issues are important in their own right they are not directly relevant to information security.

If your senior management require your policy to cover such issues, then you probably, beyond arguing the point, have no choice and must make the best of the 'poison chalice'. If you do have a choice, then I advise you have nothing to do with any matter that does not directly relate to information security threats against your organisation. The reason I make this point strongly is that, in my experience 'selling' your policy and its implications to your colleagues and getting their active support is a difficult task in itself. It becomes almost impossible if your colleagues see the policy as a covert attempt to monitor their activities in matters other than information security. Policies that throw all these issues into a general pot are usually a short sighted attempt to save costs and hint at less than sincere support of the real issue; securing your organisation against threats to its information assets.

So, hopefully, you have now decided to research and write your own policy; where do you start?

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Start with the numerous sources of information available on the Internet together with a few good books. Those which I have found to be most useful are listed in the Reference section of this paper.

A broad and deep security policy may well run to a few hundred pages. Further, its very content represents a security risk in its own right; if you wanted to attack organisation 'X' what better start could you have than obtaining a copy of their security policy. Finally, few of your colleagues will be required or expected to read the whole thing. The response to all these points is to break your policy up into, not only manageable size sections, but also into sections that allow you to easily manage its distribution to different groups of colleagues. So start with a look at your organisation structure chart, understand the staff group structure and then design your policy sections to get the required information, all the required information and nothing but the required information to each specific staff group (i.e. All Staff, Directors, Senior Managers, Technical Staff, Non-Technical Staff, Auditors (internal and external) etc).

In terms of audience groups, remember, unless there is a need to widely distribute a particular section of your policy, then don't!

As a general guide I would propose the following sectionsbut this obviously depends on your particular organisation.

Section: Overview / Section Relevance.
Summary: Matrix showing which sections of your policy are applicable to whom.
Notes: Start out by guiding colleagues as to which sections of your policy are applicable to them. For most of your colleagues a limited portion of the policy will be required reading but for a few, i.e. I.T. staff who are responsible for implementing the infrastructure, a good deal more of the policy will be directly applicable.

Section: Overview / Scope of Policy.
Summary: Where and to whom does your policy apply.
Notes: Decide and define at what locations in your organisation and to whom does your policy apply. I.e. At all offices owned and leased by your organisation in all locations, in all countries and to all staff, visitors and contractors.

Section: Overview / Purpose of Policy.
Summary: Defines the purpose of your Policy.
Notes: May seem rather obvious but it doesn't hurt to have a high-level mission statement defining the purpose of your policy such as:-. "Organisation 'X' provides and maintains computing resources to support its front-line business units and service departments. To preserve the integrity, privacy & availability of these computing resources, this policy sets forth the responsibilities of each member of staff in the secure use of said resources…."

Section: Overview / Policy Goals and Target.
Summary: A summary explanation of your policy goals and target position.
Notes: Setting the primary goals of a security policy is one of the few easy steps, in that the information security community has long since agreed and defined goals for you. The generally accepted standards are:-

> Integrity: Information only has value if we know that it's correct. A major objective of information security is thus to ensure that information is not

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

modified, destroyed or subverted in any way whilst stored or in transmission over networks.
Privacy: Stop interception/disclosure of information to unauthorised parties, be they internal or external to your organisation..
Availability: Computer systems assets must be available to authorised parties when and where needed. The security policy must not obstruct the organisation from efficiently conducting its business.

As far as your target position is concerned, you may wish to consider the following as an example.

1. To be aware of all possible **types** of threat.
2. To negate all possible threats by a pro-active threat reduction regime.
3. To have in place policies, procedures and proven technology to minimise potential security threats.
4. To have in place policies, procedures and proven technology to identify & deal with actual security attacks against your organization.

Section: Overview / Policy Stance.
Summary: Explain you chosen policy stance.
Notes: Choosing a stance to adopt in relation to the planning, implementation and monitoring of your security policy is critical. Defining the potential stances has, once again, been done for you in that there are accepted standards as follows:-

Promiscuous: Everything is permitted, which in effect equates to having no security in place.
Permissive: Everything not explicitly prohibited is permitted. This is considered a high-risk stance since the default is 'to allow'. In order for security to be effective under this stance, your prohibited list & associated configurations must be fully up to date at all times.
Prudent: Everything not explicitly permitted is prohibited. This is considered the best option for commercial organisations, since the default action is 'deny'. (Forgetting to expressly permit something carries minimal risk.)
Paranoid: Nothing is permitted. Whilst this is the option of choice for military, health service and security service type organisations it compromises the 'Availability' target and is therefore often not acceptable in a commercial organisation.

Your choice of stance is very much dependant on the business of your organisation and should be defined by senior management and not by yourself. However to aid senior management in the decision process make sure you clearly explain the options and the associated risks and costs that each stance represents. As a very general rule of thumb, if your organisation is not sure what stance to adopt, then Prudent is probably the best basis for a secure yet workable policy.

Section: Security Model.
Summary: Describes the chosen Security Architecture Model**.**
Notes: Defence in Depth (DoD); should be your target architecture model. However be aware that quality DoD costs money and if it's going to cost then be ready to explain what the model is, how it works and why it is the recommended.

Put simply; the idea of DoD is an assumption that any one layer of your defences will be defeated. Therefore you implement a multi-layered model consisting of some or all

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

of the following; border router filtering, firewalls, intrusion detection systems, host protection, cryptography, physical security, incidence response, defined standards and active monitoring and testing. Some of these layers are security products and others are procedural. Many will overlap in functionality.

Critically, for an attack to get to any layer, it must first get through or bypass all the previous layers. In short, you maximising the effort required and minimising the potential gain to any attacker thus making your organisation an unattractive target.

Section: Standards.
Summary: Defines your current Security Standards.
Notes: For those in your organisation tasked with delivery I.T infrastructure your policy needs to provide a single point of reference for what is currently allowed or disallowed in terms of standards.

Such standards should cover things like; Operating Systems, Servers, Databases, Encryption, Passwords, Network Protocols, Purchasing Procedures, Penetration Testing schedules etc.

Your standards should not be set in stone! They must be able to be challenged, reviewed and changed as your organisations requirements change, as long as the potential risk of any change is made clear to your organisation and said risks are accepted or mitigated. Thus standards should not dogmatically compromise the availability target of your policy.

Having said that, whatever is in your standards policy section at any one time must be implemented and policed rigidly. By all means allow an organisational unit to request a change to the standards to meet changing requirements but do so through formal process. Under no circumstances allow infrastructure or products to be implemented without undergoing formal review to ensure it meets with your current security requirements.

Section: Incidence Response.
Summary: Action tracks for responding to security threats & incidents.
Notes: The incidence response section of your policy should define, in detail, the action that you expect your organisation to take in the event of either:-

- Notification of a potential threat.
- Actual attack against your organisation.

It is important to understand that speed of action is often critical in limiting the damage caused by an attack. However undue hast may cause more trouble than the attack itself. Therefore, in having your procedures clearly documented, in the event of an attack occurring quick, effective and controlled action may be undertaken with limited risk, to contain and repair the situation.

I would summarize the two action tracks in the following terms. (See - McMillan Rob, "Site Security Policy Development."
http://www.auscert.org.au/Information/Auscert_info/Papers/Site_Security_Policy_Development.txt

Notification of Potential Threat.

- Monitoring

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- Security Bulletins
  Monitor security bulletins on each main area of your infrastructure.
- Web Sites
  Monitor relevant web sites for security related information. This monitoring should be done on information security web sites, newsgroups and also on 'underground' (hacker) websites.
- Business Associates / Colleagues
  Keep in touch with security staff in other organisations and with colleagues in other parts of your own organisation if its size merits it.

- Security Patching
  When you become aware of a threat through anyone of the above channels, undertake to apply associated security patches as soon as is possible.
- Anti-Virus systems.
  Make sure your AV systems are bought up to date when a new threat is identified
- Firewall/IDS – What actions take place when threat identified.
  Actively configure, manage and monitor both your firewall and intrusion detection system to ensure they are up to date to handle the potential threat.

Actual Attack Response.

- Before You Start.
  - Consult: the relevant sections of your security policy to remind yourself of the procedures to be undertaken.
  - Inform: appropriate management informed, at regular intervals, of what response procedures are being initiated and progress thereof.
  - Document: all steps taken in recovering the situation and keep, wherever possible, all technical evidence of the attack.
- Regaining control
  - Disconnect: To regain control, disconnect all compromised machines from the network including dial in connections. If you do not do this, you continue to run risks as you restore the situation.
  - Copy: Next secure an image copy of the compromised system for future reference.
- Analyse the Intrusion
  Thoroughly review log files and configuration files for signs of intrusion, modifications etc.
  - Attack Source: Analyse the source of the attack and, where possible, make formal representations to the domain's technical contacts advising them that they are suspected of being involved in an attack. Provide all possible evidence & information, requesting that they investigate as soon as is possible. Bear in mind that they may well be innocent victims of a distributed Denial of Service attack, so don't assume they are bad guys in your approach to them
  - System Configuration: Check configurations, looking for modifications made to system software, binaries and configuration files.
  - Data: Look for modifications to data.
  - Tools: Look for any tools left behind by the attack (i.e. Sniffers, Trojans etc).
  - Logs: Review log files to better understand how the attack took place.
- Recover from the Intrusion
  - Re-Install: In general, the best way to trust that a machine is 'safe' is to reinstall the operating system from the distribution media and install all of the

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

security patches before connecting back to the network. If it is not appropriate to restore from distribution media, then appropriate backups should be used.

- Disable: all unnecessary services.
- Patch: Install all vendor security patches. This is a major step in defending your systems from attack.
- Secure: Consider changing critical passwords.

- Reconnect to the Internet

  If you disconnected from the Internet, the best time to reconnect is only after you have completed all the steps listed above.

- De-Brief & Update Security

  Carry out a full de-brief with all parties concerned in order to understand:

  - How the compromise took place.
  - What technical changes need to be applied to avoid further compromise.
  - What procedural changes need to be made to

Section: Responsibilities.
Summary: Defines the responsibilities of all organisation staff.
Notes: This is one of the most important sections of your security policy. This is often the only section that will be widely published and should be made available to all colleagues in your organisation. It defines the day-to-day requirements and responsibilities that your organisation's security policy places on them, such that they play an active part in achieving and maintaining collective information security.

Alongside a clear and concise list of do's and dont's it should, I believe, justify those requirements. If you are asking your colleagues to take certain actions and avoid others, the least they deserve is the courtesy of explaining and justifying why. This also acts as a QA exercise for yourself, in that if you cant justify a requirement on the grounds of security then it probably shouldn't be in your policy.

Finally, if you can, require that all colleagues sign this section of the policy as a clear statement that they understand their responsibility. Having to sign a document often makes people think more carefully about the requirements and gets them to ask questions where necessary.

Section: Procedures.
Summary: Detailed procedural rules for defined functions.
Notes: As soon as you implement your policy you will need to be able to securely manage everyday business functions such as those listed below:-

- New Staff: Security Induction.
- Staff-Leavers: Security Requirements.
- Network Account Access Control.
- Data Access Control (File Systems).
- Data Access Control (Applications).

Make no mistake, these are not issues you can come to post-implementation. Making such procedures both secure and workable can be a huge challenge and much discussion will be required with all interested parties to make them workable, manageable and acceptable. So in regard to this section, give yourself plenty of time.

++++++++++++++++

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

So there you have my view on the general sections you should consider as part of your security policy, what each section is about and to whom the section actively applies.

Obviously its easy to list potential sections of a policy and much more difficult to researched and write the detailed policy in relation to your own organisation. Indeed this may be many months work, talking to colleagues to understand what they do and why, understand where your security is good and where it needs strengthening, understand where your organisation wants to be in the near to mid-term and understand where your policy might well come into conflict with those plans or with current practices. Any conflict will have to be addressed at some time before policy implementation so it is best to scope the potential for problems as soon as is possible in the process; remember without active support of your colleagues you're in trouble!

Assuming you get to the stage where your policy is written, you can now look to the next stage; getting active support from your colleagues.

Active support phase 2:

So there you sit; you have your senior management approval and you have your splendid new security policy researched, written and tucked away in a secure place and you are feeling pretty pleased with yourself after months of hard work.

Well now it gets harder! Now you have to convince your colleagues as to the need and benefits to them of finding time in their busy working day to adopt the policy.

To throw in another golden rule at this stage; **Talk to Them!**

Its good to have senior management support and sponsorship, indeed critical, but it wont be enough to say "The senior managers want this so you, dear colleagues, must want it!"

They may adopt it, they may sign it, some may even take an interest in your efforts but what you are really after is their active support. Active in that they understand the potential risks, active in that they think in a secure way, active in that they encourage each other to support the policy for the common good and active in that they want your policy to help them make their organisation safe against information security attacks.

This is a tall order when, as I say, in many organisations your colleagues have, up to this time, had a logical mission statement of "Get your job done as quickly as possible, using your specific skills". They have not been asked to play an active part in collectively securing the organisation's information assets; that's a job for I.T! Isn't it?

I labour the point, but at this stage you really must be prepared to get out from behind your desk and meet with your colleagues. If it's possible within your organisation, speak to everyone at group presentations and offer those presentations at all the locations of your organisation that you can get to. In short, make it easy for people to attend. The temptation is often to send an e-mail with appropriate attachments and say

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

"Read this, sign it…and, oh by the way, it's being implemented next Tuesday!" Resist and go forth!

Remembering our first golden rule (Know your Audience!) make your presentations non-technical and no more than an hour. They may be more technical than those made to the board of directors but don't baffle people – it's a turn off! The time limit is two fold; firstly more than an hour and people get bored, secondly managers may well be loathe to release their staff to presentations that take too much of their working time. Therefore you need to keep it simple, brief, interesting and enjoyable. A difficult recipe but one worth trying out on close colleagues first to get it right. For your recipe ingredients you might consider: What is information security? Why do you need to bother? What are the threats and where do they come from? Why do the threats exist? How the policy has been arrived at. How the policy acts to mitigate the threat? What will the policy mean to colleagues in their every day environment? What monitoring will be carried out and what sanctions may be imposed for those who will not support the policy?

Do bear in mind that at this stage of the process you are not there to negotiate the policy. You must explain it and justify it but, at the end of the day, it's being implemented on behalf of the senior management, for the good of the organisation and to achieve collective security. It is not negotiable! That is not to say that you shouldn't listen to feedback. You absolutely must in order to understand how best to implement the requirements of the policy into the working practices of the organisation without compromising the availability target and to understand any simple changes or clarifications to the policy that will help in achieving the support you are after.

Monitoring.

Now you have support from all levels of your organisation and a policy ready to go. So you implement! Right? Well hold on just a moment!

On the day you implement your policy you need to be able to know if it's working. It's too easy to say, "We have an implemented security policy so we must be secure", when what you actually need is certainty, that as far as it is possible for your organisation to be secure, it has been achieved.

Therefore, before you implement be ready and able to monitor the effectiveness of your security policy.

There are many ways to monitor policy effectiveness and to what level you do it depends very much on your organisation but I would certainly at least consider the following:-

Item.	Monitor.
Firewall	Monitor firewall activity logs and adjust configuration as required.
IDS	Monitor IDS activity logs and make sure this covers both external and internal sourced traffic.
Hosts	Scan all network hosts regularly for known vulnerabilities.
File Systems	Monitor activity on your file servers (Files being created, unusual

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

	file suffixes, unusual file access attempts etc)
Applications	Monitor unusual transactions.
E-Mail	Inbound attachments for viruses. Outbound attachments for viruses and data being sent outside your organisation where it shouldn't be.
Purchasing	Monitor all items requested for purchase against you policy standards and for known vulnerabilities.
Physical	Wander around looking for passwords post-its stuck to monitors, network hubs in unattended rooms, servers left logged in etc.

My final comment on monitoring echoes, once again, my call to keep your colleagues informed. Make sure that your policy clearly states on what basis monitoring of staff activity may be undertaken by your organisation and by whom. Define what the potential sanctions are in relation to deliberate ignorance of the policy requirements. Ensure that any such monitoring is a legal activity in your country/state and that it does not conflict with any other legislation (i.e. data protection / privacy acts etc)

Implementation.

When you are finally ready to implement your policy set a realistic date. Don't be rushed or bullied into going too early, but when you do set a date make sure you stick to it. A delayed implementation date will immediately give the impression that the policy is not ready and thereby devalue it from the outset.

You will also need to decide whether you do a rolling implementation, perhaps country by country or office by office or even down to a departmental level. This very much rests on the size and complexity of your organisation's operations. My advice, is wherever possible go with 'big bang'. Though all you efforts to date you will have been pushing the concept of collective secure whereby unless everyone plays their part the process is flawed. This should be reflected at implementation, clearly sending the message that security is here for everyone at every office and in all locations.

I appreciate that sometimes a more pragmatic approach may be required of you by your management and that you may have no choice but to go with a gradual implementation plane. If this is the case than at least make the rollout as swift as is possible and insist that the least secure minded areas of your organisation are implemented first.

Finally, advise your colleagues, that there will be problems and issues to expect and resolve in the first few days. Implementation will rarely be a seamless exercise so make sure you have adequate support in place in the early stages to guide and assist your colleagues. Remember you have asked for their support in this and must be ready to reciprocate quickly and efficiently.

Compliance.

My final topic is compliance. If you are a 'green field' site implementing a security policy at start-up then your monitoring regime will in effect also cover compliance in

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

that as each new area of infrastructure, application etc is installed it meets with the policy requirements and compliance is thereby met.

However you are unlikely to have the luxury of implementing a policy into a new start-up business. In the real world you are more likely to be working for an organisation with an infrastructure that has evolved over some years, with applications that have been amended as the business has expanded and with a body of staff who have never even considered information security beyond news items about teenage hackers and recalling once having seen 'War Games'.

If this is your environment then you have to look at compliance as a distinct part of the overall process. By compliance in this scenario I mean setting some baseline standards and then checking your current state against those baselines. Items should be noted as either:-

Compliant: No action required.

Not Compliant but required: Why is it not complaint, what is required to meet compliance and what priority does the item carry.

Not compliant and accepted: Formal noting of the non-compliance of an item that will not be actioned. Notes should be kept regarding the basis upon which your organisation is prepared to accept the associated risk of non-compliance. Item in this category should be agreed by senior management.

Once you have carried out this 'mapping' exercise you can assign priorities to the outstanding items and put in place action plans to achieve the required compliance. You should not underestimate the time, staff resource and potential capitol expenditure required to make a large relatively non-secured organisation compliant so your timescales need to be realistic. Some insecure areas may remain so for some time but at least being aware of the vulnerability helps you monitor it more closely.

There are two obvious questions in regards to compliance:-

Where do you get a list of security baselines to map compliance against?

The answer to this depends on your time availability and your budget. There is plenty of information out there to be found but you will need to identify multiple sources and cross-reference them to get a broad picture of what a secure set of baselines might be for your organisation. Further you will need to do this for all major infrastructure areas within your organisation (i.e. Unix, NT, Network, Databases etc).

If you have the luxury of a sizeable security budget then you might consider using a respected third party, such as a consultancy company, who should be able to provide some starting-point baselines for you from their experience in conducting security audits. The quality of this source of material is usually good but make no mistake it is rarely cheap and even with it, you will need to carefully consider if and how each items relates to your organisation.

Whether you write your own baselines or get some from a third party you must involve your expert colleagues in each infrastructure area to agree the baselines and to work closely with you in gaining compliance status. They will usually be better

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

qualified to work on detailed compliance than you are because they know the specific implementation in your organisations.

How can you implement a security policy before full compliance is met?

Be pragmatic! Detailed compliance against a security baseline must be achieved but, as stated, it may take a considerable time. In my opinion this need not hold up the formal implementation of a security policy, since the sooner you do implement your policy the sooner no new vulnerabilities will be introduced. Backward compliance for existing infrastructure can then be addressed alongside, and in association with your policy.

++++++++++++++++++++++++++++

References:

Guttma Barbara, Bagwill Robert, "Internet Security Policy: A Technical Guide" National Institute of Standards & Technology (NIST).
http://csrc.nist.gov/isptg/html

B.Fraser (Editor), Various (Authors), Various(Reviewers), "RFC 2196: Site Security Handbook", Ohio State University.
http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc2196.html

Internet Security Systems, "Creating, Implementing & Managing the Information Security Lifecycle."
http://downloads.securityfocus.com/library/securityCycle.pdf

McMillan Rob, "Site Security Policy Development."
Australian Computer Emergency Response Team
http://www.auscert.org.au/Information/Auscert_info/Papers/Site_Security_Policy_Development.txt

The Network Security Library, Various Information Security Papers.
http://secinf.net/ipolicye.html

Brenton, Chris. Mastering Network Security. Sybex:, 1999.
ISBN: 0-7821-2343-0

McClure Stuart, Scambray Joel, Kurtz George. Hacking Exposed 3rd Edition.
Osbourne / McGraw-Hill, 2001.
ISBN: 0-07-219381-6

K Dr. A Complete Hackers Handbook. Carlton Books, 2000.
ISBN: 1-85868-943-0

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 21st, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced