

Management Briefing Paper

Security Policy Considerations

High-level considerations for organisations when developing and implementing a security policy.

Increasingly, both large and small organisations are adopting security-based guidelines to aid infrastructure design and maintenance. As their networks become more complex and diverse, many understand the need to exert more control over their communications infrastructure to minimise disruption as problems occur.

Companies need formal guidelines on protecting their networks. In our experience, these guidelines can be provided by a security policy tailored specifically for each organisation. Here are some key considerations:

Policies should be simple to understand and relevant. Policy documents are *guidelines* – and should be treated as such. They will provide organisations and their IT support groups with essential reference material to maintain and develop a secure IT infrastructure. This will only be achieved if the information is understandable and specifically targeted at the company.

Information should be **immediately accessible to relevant parties**. To ensure standards are adopted, guidelines and procedures will need to be available at all times. By using mediums such as the company intranet or laminated reference cards (to name but two), groups such as IT Production Support will have reference material to hand when performing tasks such as vital system fixes.

Organisations should **own the policies and guidelines**. With management support, guidelines and policies should be incorporated into day-to-day working practices. Rather than be viewed as separate, self-contained documents, policy guidelines should be integrated into operations guidelines. This should start to establish security deeply within the fabric of IT operations and the organisation as a whole.

No organisation can, or should stand still. As new infrastructure is rolled out and security threats evolve, policy guidelines should keep pace. It is vital that information is **easy to access and maintain** for designated staff. Any updates should be reviewed as a matter of urgency thus ensuring that approved changes enter the Production environment with the minimum of bureaucracy.

Contribution counts. All staff should feel **ownership** of the policy – directly contributing to the various changes that need to be implemented. People should feel that the policy is working for them (and not against them) – protecting the company and therefore their day-to-day operations. It won't happen overnight, but once started, it will help 'lift' policy communications and aid early adoption of standards and guidelines.

A 'typical' company profile...

Organisations that use a third party (such as ourselves) to drive policy development, typically:

- have an open culture based on information sharing. This culture should be maintained wherever possible
- already have basic information controls in place. However, the organisation does not have a wide-ranging, strategic security plan.
- look to adopt a recognised standard, such as BS7799.
- require solutions to be as transparent as possible. Ideally, products and technologies employed should offer the required level of corporate information control, with as little impact to personnel as possible.
- look for a long term, strategic approach.
- require limited (internal) management involvement and overall sponsorship for the project. Senior management will support and ‘champion’ developed policies when communicating guidelines and educating staff.
- initially require an intensive vulnerability assessment project to facilitate a full understanding of the environment. This can be translated into a draft security policy and defined sections of work. It also follows standard recommendations made by BS7799.
- introduce the strategy in phases. Each defined section of work will identify and introduce ‘quick wins’ as well as developing the overall company security strategy.

Rollout considerations

“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.”

SANS Institute

In theory the concept and objectives of a security policy and the resulting change in behaviours appears to be straightforward. After all – the aim is to protect the business and create security awareness.

The reality is often quite different. Initially, staff are fully supportive of policy objectives. However, once mechanisms are implemented that restrict them from free reign over previously uncontrolled areas, support can quickly disappear.

Typically, the groups that are most effected by changes in security are the systems administration staff. These will be the people who have immediate and pressing environment fixes to complete. They will rapidly lose patience if they do not have the necessary controls to fix a machine and get business groups operational.

Some organisations have a dedicated security team that is physically located away from the groups that provide system support. Generally, security teams that communicate using email and telephone are less effective in working together than teams that work side by side.

It may appear like common sense, but in our experience the most successful projects:

- Are phased – implementing realistic objectives in a controlled manner
- Have key teams working closely together. It might be wise to have the security team working in the same physical area as the people who administer the systems.
- Have administration buy-in. Secondment of a key member of the administration team (not as security manager) to retrain as a security professional might gain the trust and buy-in from IT support groups.

A key factor when introducing controls is what do with staff who break the rules. In some respects, if this situation has arisen it could be considered that the policy has failed.

Failed – because it hasn’t been *effectively communicated and understood*.

Whatever the reason, staff need to understand what punishment to expect if they do break the rules. This can range from verbal warnings to summary dismissal. Some organisations have a dismissal policy for offences such as having a dial-in modem (surprisingly, in many cases this does not act as a deterrent).

In most cases good education, encouragement and understanding offer greatest reward.

Developing the policy framework...

Approximately 80,000 UK businesses are now compliant with BS7799 and a further 40,000 are planning to be in the next year

DTI Security Breaches Survey 2002

For many organisations, a phased secure infrastructure implementation will support developing smaller, targeted policies. Collectively, these will represent a security policy covering the whole organisation.

There are a number of key considerations that will dictate how the overall company policy will develop. These include:

- Does the policy fit the company's business needs?
- Does the policy fit the company's unique culture?
- How will the policy be implemented – how can staff be educated?
- Is the policy enforceable and does it relate to the activities that actually take place within the organisation.

There are many example documents and resources available to complement standards such as BS7799. However, these have often been developed for a specific organisation.

Implementing off the shelf policies normally **fails** as boiler-plate guidelines bear little relevance to a specific organisation's needs.

It is only after an initial analysis period¹ that an approach can be formulated. However, based on expected findings and recommendations, the overall policy:

- Should be simple to understand and relevant. Once that has been achieved, it will be simpler to communicate and adopt.
- Should be flexible – allowing for infrastructure change.
- Should be accessible – possibly on the company intranet.
- Should be owned by the organisation with the overall aim of establishing it deeply into the fabric of the organisation.
- Should be easy to maintain.
- Staff should feel ownership – directly contributing to the various changes that need to be implemented. This will help 'lift' policy communications.

Several of our customers successfully use their security policy as an important education tool to build understanding of basic security principles.

A key principle is that of “**defence in depth**”. This principle requires that no single point of failure within an organisation can represent an overall vulnerability. The principle can be applied to team organisation, network infrastructure, application design, server builds and security policy.

¹ Such as a vulnerability assessment – see http://www.ambersail.com/resources/tech_bulletin/security_strategy.pdf

A good example of ignoring the principle would be an organisation that protects their entire network via a single firewall and no other measures. If breached, the entire network becomes exposed – presenting innumerable opportunities for exploitation.

Conclusion

A well-designed and executed security policy can bring real benefit to an organisation. During its development it will force an organisation to address key areas of weakness – both in terms of security and best practice.

Once completed, policy introduction and subsequent maintenance will ensure that key business IT infrastructure is accountable, well designed and configured for future enhancements.