Internet Security Systems

Creating, Implementing and Managing the Information Security Lifecycle

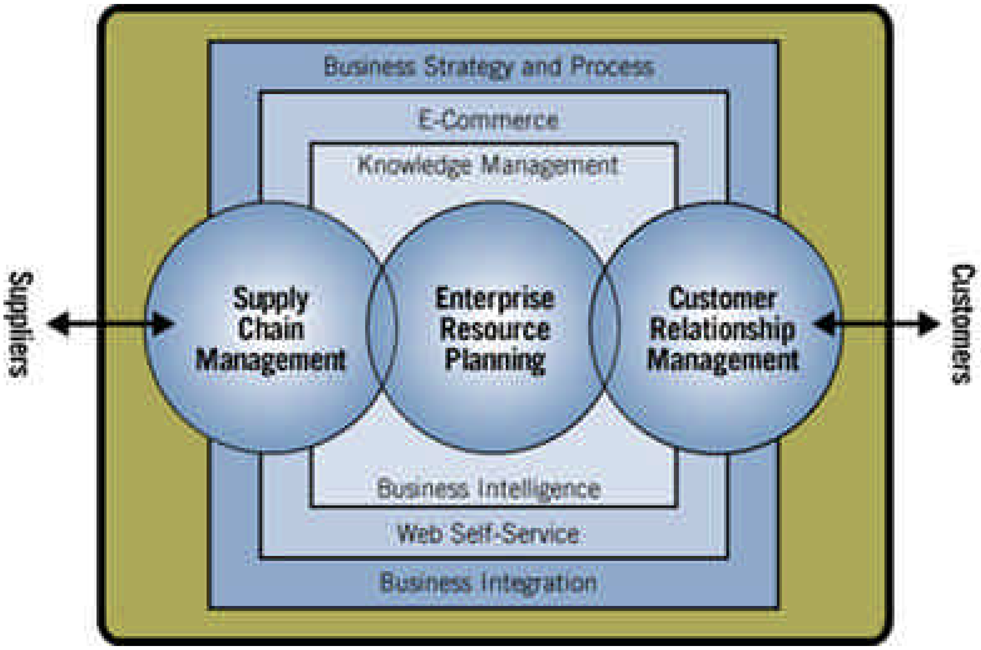
Security Policy, E-business and You

Security policy has become a generic term with different meanings for diverse audiences. This whitepaper describes how a standards-based approach helps define security policy as a specific, measurable and data-driven framework encompassing multiple user and management needs across an organization. By applying this framework, organizations encourage broad-based support for an information security solution. The end result is an efficient and effective ongoing security management system, including both insourcing and outsourcing options.

Standards-based Security Policy

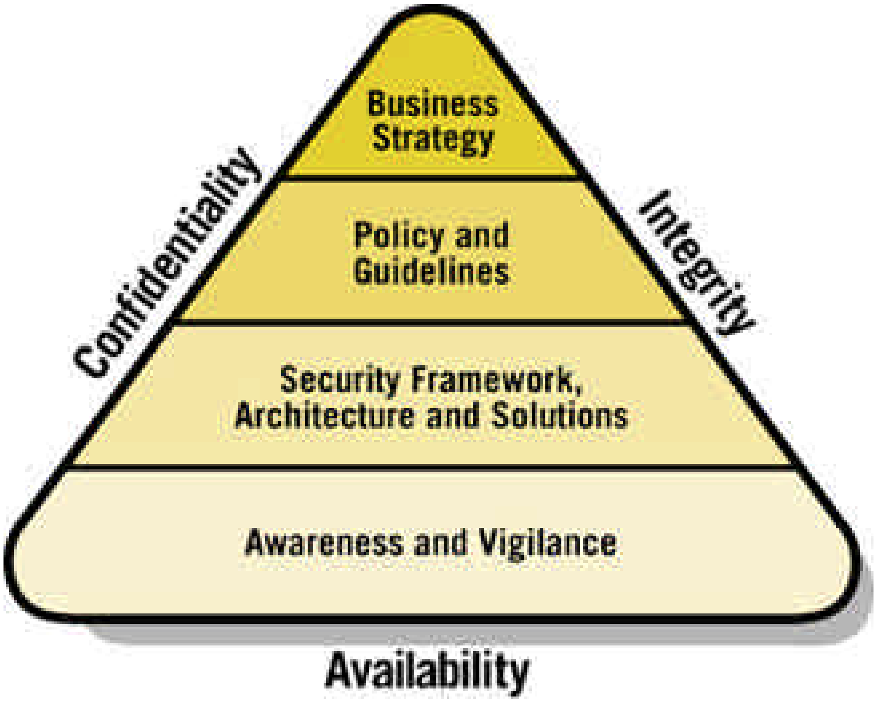
Security is a business fundamental in the physical world. No organization would even consider opening operations without securing all facilities against theft, fire and vandalism. Nevertheless, companies engaging in E-commerce routinely shortchange their protection of key online assets and systems. A single security breach in the online world can be far more damaging than it would be in the physical world in terms of strategic information lost, bad publicity, loss of customer and partner confidence, and stakeholder liability. Once this realization hits home, information security quickly becomes a key priority for e-business.

Trust, therefore, has become the fundamental issue for organizations using information technology to grow through acquisition, move aggressively into new online business ventures or streamline existing business operations. Can IT and senior management trust that information is being properly used and safeguarded by employees? Can customers trust vendors to protect their privacy? Can organizations trust vendors and partners to properly secure their interconnected online assets? What is the financial impact when a specific segment of the network security infrastructure is compromised or fails? Without this confidence, it becomes very difficult to successfully deploy vendor/supplier extranets, Customer Relationship Marketing (CRM)/Enterprise Resource Planning (ERP) enterprise applications, electronic commerce or other online necessities for competing in today's wired marketplace.



Complicating the issue is a general lack of security management awareness at all levels of an organization. From senior management to customers and suppliers, security is perceived at best as a necessary evil. At worst, it is an expensive and unwanted intrusion into normal business operations. This inappropriate view must be overcome in order to establish strong, consistent security practices. And yet, without a clear demonstration that security management adds value through network transparency, any security process will be actively subverted by its users. Both individuals and operating units must understand and invest in a process that clearly demonstrates security management as an enabler that accelerates achievement of business goals.

A successful security management solution should begin as an integral part of an organization's overall business strategy. Once security management is accepted as a core business operation, it necessitates the development of guidelines that create the security practices necessary to support the business strategy. These guidelines, therefore, are what most organizations understand to be their security policy. The policy in turn drives the development of an overall security management architecture. Finally, this framework is monitored for vulnerability, attack and misuse. The end result is improved information availability, integrity and confidentiality, from both inside and outside the organization.



It sounds straightforward. But there is one significant obstacle to meeting this simplified set of objectives – very few corporations know what information resides on their networks, where it is located, who has access to that information and the cost of having a given set of information compromised. This lack of self-knowledge becomes a crippling limitation when it comes time to convert generalized principles into an enforceable security policy. If guidelines can't be converted into data and metrics for assessing performance, security policy cannot be applied effectively.

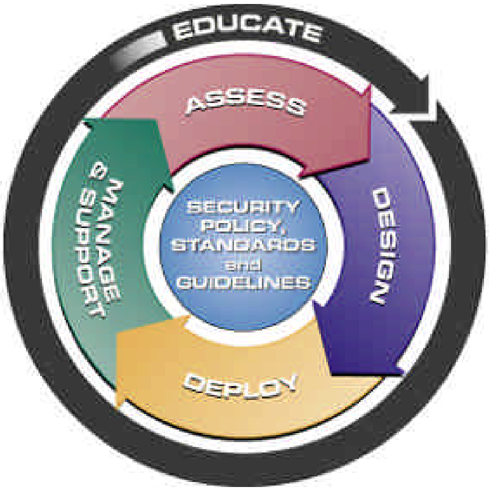
British Standard 7799 (BS7799) is a blueprint for tying the various interpretations of security policy into a single methodology that extends from broad-based security mission statements to specific implementation and configuration guidelines and performance metrics for individual users and network devices. Currently under review as an ISO international standard, BS7799 is a generalized, structured approach to network security that is broadly applicable across any organization seeking to protect its critical online assets. This whitepaper uses BS7799 as a guideline for describing security policy, securing support for the policy from end user to senior executive, implementing the policy and managing the policy as an ongoing, adaptive process.

The Information Security Management Lifecycle

Without an accurate understanding of their online investment, organizations can't know what security applications or services are needed. They cannot gauge what quantities of which technologies to buy. They do not know where to deploy these purchases for best effect. In many cases, the tools become "shelfware" – expensive monuments to good intentions gone awry. Lack of attention to management and user needs is another obstacle to information security success. Even when networks are properly protected, managers and users will actively subvert the system if it creates obstacles to their daily business operations.

The key to creating useful, transparent and enforceable network security comes from adopting a process that provides broad-based needs input, careful identification of network resource and access requirements, and data-driven implementation and management services. This process results in a proper security policy that significantly improves information availability, integrity and privacy. Just as importantly, a properly executed information security policy encourages buy-in across the organization. By building education and participation into the security management lifecycle, organizations encourage voluntary compliance and greatly enhance the possibility of a successful implementation.

This fundamental security management life cycle contains five interrelated processes – assess, design, deploy, manage/support and educate. These five elements work as a closed-loop system, allowing the security cycle to grow and respond to changing network needs and conditions. Each element is defined below, with detailed descriptions of the four sequential steps in the following sections.



Assess – A BS7799-based, systematic baseline identification of all network devices and resources, and the establishment of valuations for all groups of data residing on the network. Assessment converts general descriptions of the network into measurable data sets that can then be used to design an effective security management policy and infrastructure.

Design – Conversion of assessment data into lists of network security applications, deployment locations, implementation strategies and specific configuration guidelines for each network device or security application. At the completion of this stage, the security policy exists as a completed document, accompanied by a deployment plan for all necessary technologies.

Deploy – The physical process of implementing the plans created in the design phase. Includes installation, testing, training and conversion to a production environment.

Manage and Support – Measuring performance data from the network security infrastructure against the goals stated in the security policy. Non-compliant systems and events trigger specific actions, as stated in the policy, including a re-evaluation of the policy and restart of the policy generation process. This stage can manifest itself as either in-house operation or, more commonly, as outsourced managed security services, and should include a detailed incident response plan.

Education – An ongoing effort to raise awareness of the need for network security at the executive, management, administrator and end user levels. This process cuts across all other steps, and includes both administrator training for emerging threats to systems and awareness among end users
of the benefits of working within the security architecture.

Security Management Lifecycle Details

Assess

Assessment turns general statements of intent into quantified, regulated sets of data that can be converted into an automated and measurable information security system. Information gathered in the assess process includes:

What is on the network?

- Identification of all network devices, applications and services
  - Identification of who has access
  - Identification of value
  - Identification of risk of compromise from inside workgroups, networks or the enterprise
  - Identification of risk of compromise from Internet Service Providers (ISPs) partners, vendors, customers and anyone else with external access
  - Valuation of damage from compromise from the inside
  - Valuation of damage from compromise from the outside

- Identification of all data stored on the network
  - Identification of who has access
  - Identification of value
  - Identification of risk of compromise from inside workgroups, networks or the enterprise
  - Identification of risk of compromise from Internet Service Providers (ISPs), partners, vendors, customers and anyone else with external access
  - Valuation of damage from compromise from the inside
  - Valuation of damage from compromise from the outside

- Identification of hosts, network devices and databases already susceptible to attack
  - Attacks from inside the network
  - Attacks from outside the network
  - Attacks against affiliated partner/vendor/supplier networks from inside the network
  - Attacks against affiliated partner/vendor/supplier networks from outside the network

Who needs to be involved in the security policy decision-making process?

- Executive level
  - Which staff?
  - What are the business goals that improved security management supports? ***Education*** helps support this part of the process.
  - What is necessary to co-opt support, reach consensus and obtain signed approval?

- IT level
  - Which staff?
  - Will they be threatened by new processes and procedures? ***Education*** helps support this part of the process.
  - What is necessary to co-opt support, reach consensus and obtain signed approval?

- Security management level
  - Which staff?
  - Will they be threatened by new processes & procedures? ***Education*** helps support this part of the process.
  - What is necessary to co-opt support, reach consensus and get signed approval?

- Human Resources and Legal staff
  - Do current and proposed security measures meet corporate employment policy standards?
  - Do current and proposed security measures meet the organization’s legal requirements? Is legal liability sufficiently controlled?

- End users, vendors, partners, customers, etc.
  - What are the advantages to them for adopting a more secure corporate posture? ***Education*** helps support this part of the process.
  - What are the business goals of these outside entities that an enhanced security posture supports?

- What is necessary to co-opt support, reach consensus and get signed approval?

Asking the correct questions is a surprisingly simple process, but the amount of data that is generated in even a small organization can be intimidating. As a result, many organizations use outside specialists to provide assessment services. This sizeable collection of data, once collated and organized, represents a data web illustrating the breadth of the entire security management environment. Its comprehensive reach becomes the foundation for designing an effective security management architecture. Once published, this document is the enterprise security policy.

Design

Design is where details describing the network and its contents become a comprehensive security policy document encompassing guidelines for policy implementation at the business unit level and network device configurations that support and enforce the policy. As part of this step, the organization needs to make a fundamental decision – bring network security in-house, or use managed security services through an outsourcing model. Some organizations will opt for local control. Others will prefer to let someone else handle the workload and liability. Either option, however, requires proper assessment and design for any reasonable expectation of success.

The first priority of the design stage is to create standardized levels of security service based on the data gathered in the assessment stage. Access privileges and trusted relationships between hardware, software and staff must be matched with these services. It can get complicated. Individuals or systems may have different levels of security for different sets of similar data. Likewise, the same individuals or systems may require different levels of security for different business requirements or network management events. Data stored at multiple locations on the network may have different security needs dictated by the various locations.

In the end, the design process delivers a web of interrelationships between information, systems, users and tightly defined levels of security needs. Based on this data, it becomes possible to start designing a security architecture that transparently supports the organization’s overall business strategy.

The next step is to define implementation guidelines – the standards by which an element of the security policy will be judged as compliant or not. This process should define the following:

- Is this an allowable event? On which systems and under which circumstances? Should this event trigger an alarm? Who should receive it? What action should be taken?
- Is this vulnerability allowed? On which systems and under which circumstances? Should this event trigger an alarm? Who should receive it? What action should be taken?
- Delineate chains of command for incident escalation
- Define the requirements for reporting – who should receive which reports, in what format, at what time intervals

Once these requirements/relationships have been correlated into data, it is time to build a shopping list of hardware and software. The implementation guidelines lead to lists of detailed configuration guidelines, which in turn determine the devices and applications needed to establish and manage the security policy. These implementation and configuration guidelines also provide the baseline metrics by which security assessment and intrusion detection applications evaluate policy compliance once the system has been deployed. In other words, a well-designed security management system limits its scope to specific operations on specific network segments. The result is faster security management response time, focused reporting and limited effects on network performance.

Deploy

Deployment, which is where most organizations currently concentrate their security efforts, is actually the simplest and most straight-forward aspect of security management. Since deployment is much like launching any other online initiative, most organizations already have a structure in place for testing and implementation. Unfortunately, this same familiarity leads many organizations to follow only this step, giving short shrift to assessment, design and management/support. In essence, the security management process is disregarded once deployment is complete. This narrow view of information security can easily lead to an inefficient, inadequate or under-performing network security infrastructure.

Education is a critical element for successful deployment. In fact, deployment provides the best opportunity to educate the entire range of staff affected by the security policy, including how it benefits both individuals and the organization in technical and financial terms. This last step is frequently overlooked, but it often becomes the determinant factor in whether a security implementation thrives or fails.

Deployment begins with the purchase of hardware and software, as dictated by the plan created in the design phase. Once the equipment is in place, it must be rigorously installed and tested to ensure that performance meets specifications, and that network operations are not adversely affected. Once the system is assured of matching the requirements detailed in the security policy, then the system moves out into the production environment.

Management and Support

Management and support take multiple forms. On one level, it is the process by which the success of the security can be measured. Are corporate assets adequately protected? Is the online environment and supply chain sufficiently transparent? Are users comfortable with the level of security, or are there active attempts to subvert an overly restrictive system? Has the enterprise environment evolved sufficiently to require a reassessment of the security policy? These may be generalized questions, but a security policy with tightly defined, data-driven parameters for measuring performance will have no trouble delivering immediate answers.

On a more technical level, the security policy dictates how security is supported once the deployment stage is complete. Since management requirements and user needs have been converted into a data-driven set of implementation and configuration guidelines, it is very possible to create a system that learns to manage itself, including escalation procedures. In this environment, security information is correlated and analyzed so that human resources can concentrate on “hot spots” that require immediate, non-standard attention.

There are two paths for proper security management and support. The first uses in-house staff and applications to monitor the network for attack and/or misuse, plus periodically test the network for vulnerabilities and non-compliance with security policy. This cycle of continuous security improvement works as follows:

- Security assessment and intrusion detection applications routinely watch the network for signs of improper activity or policy non-compliance. Since these applications look only for signs of attack, misuse and misconfiguration that match specific security policy profiles, they minimize their impact on network performance and significantly reduce the event-driven data that must by analyzed as part of the reporting process.

- If a security event does occur that indicates a violation of security policy, these applications respond according to predefined rules for action. Relatively insignificant violations can be dealt with automatically. More serious situations trigger email, pager or FAX notification of appropriate staff. Extreme situations alert senior security staff, with continuing escalation until the crisis has been resolved. Enterprise-level reporting tools quickly correlate and analyze emerging situations, enabling staff to concentrate attention where it's needed most.

- Finally, these applications use the security policy to reconfigure the network itself in response to attack. Once an intrusion is detected, the system launches security assessment scans against other segments of the enterprise. If other hosts, databases or devices vulnerable to that type of attack are located, they can be reconfigured to block misuse until the situation is under control. If the attack or misuse is outside the security policy, then administrators are alerted, so that the assessment process can begin again, closing the security policy process loop.

Security is one of the most dynamic elements of the IT infrastructure. Unlike the physical world, automated online security threats do not fatigue, requiring constant vigilance encompassing every change in an organization's networks. As a result, many companies are turning to managed security services to provide a cost-effective alternative to in-house security policy management and support. For many organizations, the cost of hiring, training and supporting an in-house network security staff more than outweighs the perceived advantages of having localized control over security operations. Outsourcing provides efficient and effective information protection. Management overhead and liability exposure become shared with and diluted through the managed services vendor. More importantly, organizations can use managed security services to unlock IT resources for other needs while ensuring networks are globally secure 24x7, 365 days a year.

Managed security services usually consist of a multiple of offerings from best-of-breed vendors. This broad menu of offerings allows organizations to select the range of services that best fit their needs. Recommended offerings should include:

- Firewall and router management
- Intrusion detection and response
- Virtual private networking (VPN)

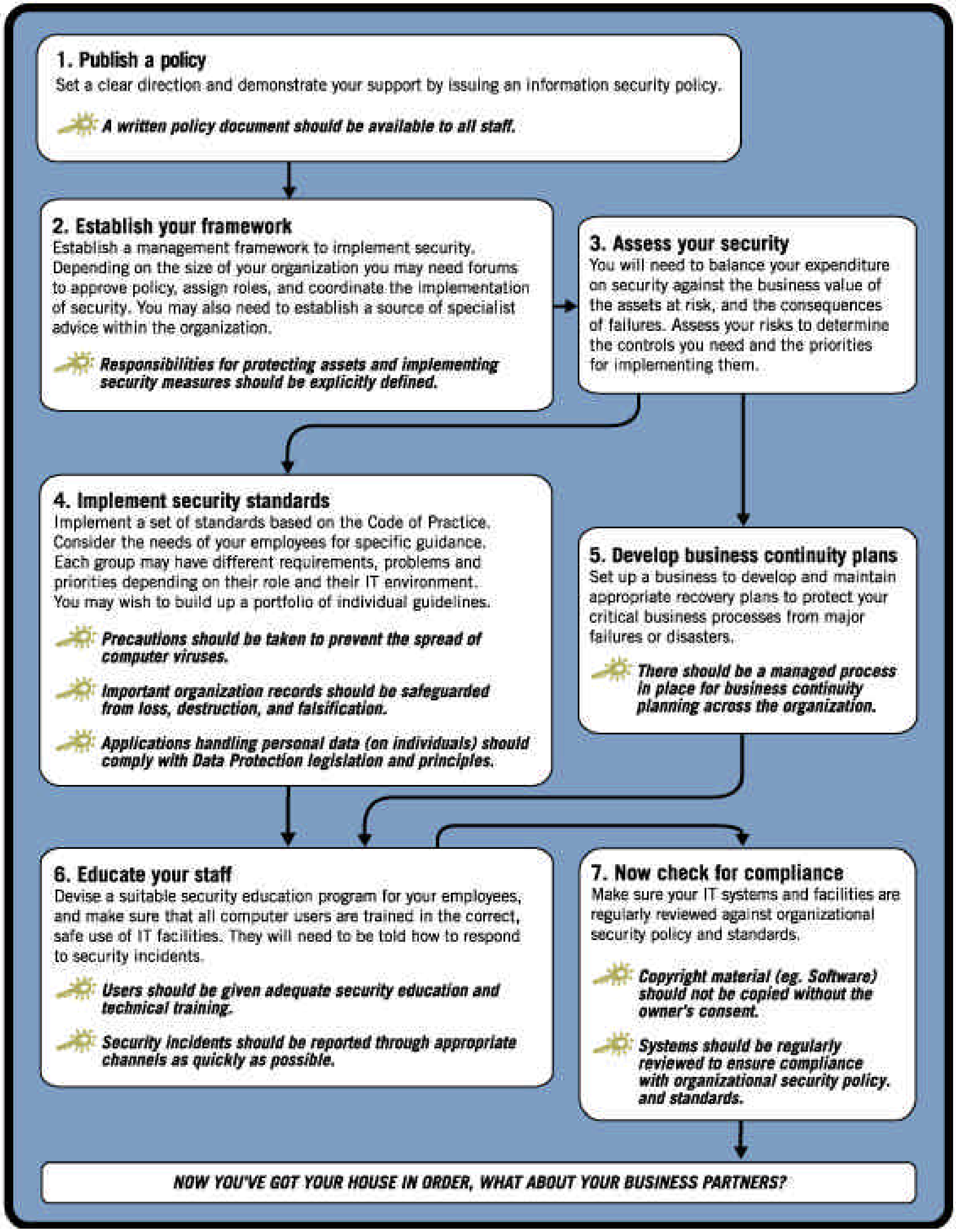
- Access control, authentication and encryption
- Virus and vandal protection
- Web site filtering
- Security policy consulting, creation and management
- Software update/patch services
- Configuration backup/restoration
- Security reports for authorized managers via hardcopy and Web browser
- 24x7 security monitoring and phone support

In the end, the choice of in-house versus outsourced managed security services comes down to budget, corporate culture and business strategy. Regardless of which path an organization takes, proper use of globally security policy will deliver an appropriate level of protection.

The Information Security Lifecycle – A Key Element of E-business Success

Effective security management requires more than firewalls and intrusion detection solutions. In order to adapt as new technologies and new opportunities impose changing demands on the network infrastructure, security management must become a closed-loop cycle of continuous security improvement. This goal can only be met through a structured, standards-based approach to generating and implementing security policy. Once this rigorous policy – the information security lifecycle – is in place, security management becomes a data-driven process that supports streamlined business operations while simultaneously focusing and reducing the huge amounts of data generated through managing the security management process.

THE ACTION PLAN FOR IMPLEMENTING INFORMATION SECURITY MANAGEMENT



1. Publish a policy

Set a clear direction and demonstrate your support by issuing an information security policy.

A written policy document should be available to all staff.

2. Establish your framework

Establish a management framework to implement security. Depending on the size of your organization you may need forums to approve policy, assign roles, and coordinate the implementation of security. You may also need to establish a source of specialist advice within the organization.

Responsibilities for protecting assets and implementing security measures should be explicitly defined.

3. Assess your security

You will need to balance your expenditure on security against the business value of the assets at risk, and the consequences of failures. Assess your risks to determine the controls you need and the priorities for implementing them.

4. Implement security standards

Implement a set of standards based on the Code of Practice. Consider the needs of your employees for specific guidance. Each group may have different requirements, problems and priorities depending on their role and their IT environment. You may wish to build up a portfolio of individual guidelines.

Precautions should be taken to prevent the spread of computer viruses.

Important organization records should be safeguarded from loss, destruction, and falsification.

Applications handling personal data (on individuals) should comply with Data Protection legislation and principles.

5. Develop business continuity plans

Set up a business to develop and maintain appropriate recovery plans to protect your critical business processes from major failures or disasters.

There should be a managed process in place for business continuity planning across the organization.

6. Educate your staff

Devise a suitable security education program for your employees, and make sure that all computer users are trained in the correct, safe use of IT facilities. They will need to be told how to respond to security incidents.

Users should be given adequate security education and technical training.

Security incidents should be reported through appropriate channels as quickly as possible.

7. Now check for compliance

Make sure your IT systems and facilities are regularly reviewed against organizational security policy and standards.

Copyright material (eg. Software) should not be copied without the owner's consent.

Systems should be regularly reviewed to ensure compliance with organizational security policy. and standards.

NOW YOU'VE GOT YOUR HOUSE IN ORDER, WHAT ABOUT YOUR BUSINESS PARTNERS?

(*British Department of Trade and Industry*)

About Internet Security Systems

Internet Security Systems (ISS) is a leading global provider of security management solutions for the Internet. By providing industry-leading SAFEsuite security software, remote managed security services, and strategic consulting and education offerings, ISS is a trusted security provider to its customers, protecting digital assets and ensuring safe and uninterrupted e- business. ISS' security management solutions protect more than 6,000 customers worldwide including 21 of the 25 largest U.S. commercial banks, 10 of the largest telecommunications companies and over 35 government agencies. Founded in 1994, ISS is headquartered in Atlanta, GA, with additional offices throughout North America and international operations in Asia, Australia, Europe, Latin America and the Middle East. For more information, visit the Internet Security Systems web site at www.iss.net or call 888-901-7477.