Global Information Assurance Certification Paper

Organizational Information Security From Scratch – A Guarantee For Doing It Right

Patrick Jones
July 2000

Introduction

The need to have a comprehensive, verifiable information security management strategy in place has grown significantly in recent years. The most compelling reason is the increasing likelihood that your organization may find itself in a courtroom defending its security practices against the expected growth in liability lawsuits. "You can expect to see major liability lawsuits in the next 18 months" says Randy Marchany, a member of the Virginia Tech Computing Center. In some instances, individual managers may be the target of fines or jail time. The focus of these lawsuits is a combination of the traditional procedures used in protecting proprietary information and new business processes emerging from electronic commerce initiatives (i.e. sharing your corporate information with business partners, vendors and shareholders), especially the use of the Internet as a business tool. Lawsuit targets include an organization's inadequate preparation against distributed denial-of-service attacks, spread of computer viruses, public disclosure of confidential information or financial loss to customers and investors.

In some cases technology may even contribute to this growing concern, instead of helping to guard against it. "For no good reason whatsoever, Microsoft has equipped Windows 2000 and XP with the ability FOR ANY APPLICATION to generate incredibly malicious Internet traffic", says Steve Gibson of Gibson Research Corporation. This will provide any internet connected PC with the ability to more easily initiate denial of service attacks.

The foundation for establishing the necessary protections and demonstrating the required diligence towards protecting your organization's proprietary information can be found in a security infrastructure that has been around in one form or another since the early 1990's. It provides a means to combine the technical protections (network firewalls, intrusion detection systems, traffic analyzers, etc.) with business processes (risk & vulnerability testing, information security policies and procedures, etc.) into an overall information security infrastructure. The purpose of this document is to provide an overview of this infrastructure and a strategy for implementing it.

A comprehensive, verifiable approach towards information security management identified

The focus of information security management can't be limited to controlling system access, or just the technical infrastructure supporting these systems. It must also address the organizational infrastructure and related data protection activities outside the data center environment. Finally, there must be an ongoing means to confirm that your efforts are effective.

So, can you just log on to Amazon.com, order a copy of ***"Information Security Management for Dummies"*** and follow the instructions? Obviously not, but a foundation on which you can build a logical, defensible methodology does exist. Its called the ISO 17799 Security Standard, first published in December 2000. This document does not go into the history of ISO 17799, but

will detail how it can be used to establish a sound information security management process in an organization of any size.

The ISO 17799 Security Standard identifies all aspects of information security management that every organization, regardless of size, must address. It breaks them down into ten control categories:

Organizational Infrastructure

1. ***Information Security Policies*** - Written policies, providing management direction and support for information security-related activities, are available to all employees.

   A comprehensive suite of information security policies will address four focus areas: Enterprise policies apply to all employees, regardless of their role in the organization and focus on sound information management practices. Computer system, application and related media policies focus on Information Technology department-specific activities. Network policies address those activities performed to provide connectivity to / from computer systems and applications. Finally, policies that address the physical security of computer and network systems / applications must be established. Listed below is a suite of foundation information security policies that every organization should consider:

Enterprise Information Security Policy - *A high-level "master" policy that covers the basics of information management and references more detailed policy documents as required.*
Information Ownership Policy - *The "owners" of corporate data typically reside outside the IT Department. This policy defines the do's and don'ts for these "owners".*
Training and Security Awareness Program - *Educating employees on their responsibilities regarding information management and maintaining the required level of awareness is vital. This policy addresses the required education and awareness activities.*
Business Continuity - *Business continuity and disaster recovery activities are not restricted to the IT Department. Business continuity policies help ensure the consistent implementation of continuity planning at the business process level.*
Software Licenses - *With PC's on almost every worker's desk, guidelines for ensuring compliance with software vendor requirements at the individual worker level are necessary. Additionally, a formalized set of policies help to eliminate or reduce the potential severity of penalties when instances of non-compliance are identified.*
E-Mail Policy - *Everyone uses e-mail, but computer viruses, objectionable transmissions and excessive amounts of data pose threats. E-mail policies define acceptable practices to safeguard this medium. It should also define privacy expectations for all workers.*
Retention Requirements / Information Disposal - *Corporate information exists in many forms and locations-User PCs, file space on servers, off-site back-ups, e-mail attachments and so on. A comprehensive plan for preserving data and deleting it when no longer needed is required. This policy identifies the procedures required for each medium.*
Virus Control Policy - *Whether managed centrally or separately on every machine, guidelines designed to ensure that anti-virus activities are performed will be identified in this policy. It will also identify procedures to follow in response to suspected virus attacks.*
Personal Computer Security - *Workers tend to overlook key aspects of PC use, focusing only on the their use in supporting the specific task at hand. This policy addresses these overlooked activities such as backing up your data, ensuring license compliance, controlling access to the PC and the data on it and so on.*
User Access Administration - *Consistent procedures for controlling user access in all corporate systems help to ensure effective control of proprietary information. This policy defines access administration procedures.*

Audit Trails, Security Review Procedures - *The consistent collection of data throughout all systems and establishment of sound review procedures ensure that the data needed to analyze unauthorized changes (intentional and inadvertent) to corporate data bases are available.*
Web Development / Implementation / Certification Guidelines, Content, Design, Administrative, Legal, Security, Usage - *As the ability for anyone / everyone to publish webpages on corporate networks, procedures to ensure the secure management of web content are needed. Additionally, if not properly configured, web servers represent a starting point for potential intruders.*
Computer Operating Systems - *To ensure that operating systems are configured consistently and for maximum security and performance.*
Computer Applications - Internal Control / Program Security - *To ensure that all mechanized applications are configured for maximum performance and security. The decentralization of many application development activities increase the importance of this policy area.*
Disaster Recovery Planning-Data Center Recovery - *Taking business continuity to greater detail in the data center environment, this policy addresses the activities required to identify and support minimum processing requirements.*
Disaster Recovery Planning-Application Recovery - *Business functions rely upon the processing of supporting applications. This policy identifies procedures for determining recovery requirements and alternative strategies.*
Network Security Administration (Intrusion Detection, Incident Response, Network Monitoring, etc.) - *Guidelines are required, not only to guarantee efficient operations, but to ensure that legal concerns are addressed.*
Network Security Infrastructure (Firewall Configuration, Network Routers, VPN Implementation, Third Party Network Connections, etc.) - *Especially important for larger and international organizations, policies ensuring the consistent configuration of the network are needed.*
Telecommuting / Remote Access - *To ensure secure and controlled access from outside corporate firewalls in addition to ensuring effective remote work habits.*
Network Disaster Recovery Planning (LANs, WANs) - *To ensure that all recovery plans are consistent in content and that required testing procedures are defined.*
Telephone System and Voice Mail Security - *To ensure that phone systems are configured to prevent unauthorized use, to ensure that voice mail storage requirements are identified / maintained and, as in the e-mail policy, to clarify privacy expectations for workers.*
Internet/ Intranet / WWW Use Policy - *Guidelines for the do's and don'ts of internet and corporate intranet. This policiy also defines the potential penalties for non-compliance.*
Data Processing Facilities Security - *Policies define and ensure the consistent implementation of safeguards for controlling access to computing facilities.*

2. ***Security Organization*** - Responsibilities for the management of security processes are defined and assigned.

   Depending on the size and complexity of an organization, the number of people required to staff the Information Security group will vary. However, several distinct skill sets will be required and the areas of responsibility can be patterned after the same categories that information security policies fall into. An enterprise-level management function is required to address information security-related issues impacting the enterprise as a whole. The focus of this function includes topics such as maintaining information security awareness throughout the enterprise, ensuring sound information security practices and procedures at the worker level and performing IS-related investigations in coordination with Corporate Security. This position requires an overall knowledge of information security management

principles.

A systems and applications function is needed to coordinate configuration and access control activities for all corporate systems and applications. Data center and/or system administrator experience provides a good foundation for this role. A network security function is needed to address both the security infrastructure and to manage security monitoring and response procedures. This role requires a combination of network administration experience and security knowledge (both principles and tools). Finally, the physical security surrounding IT assets must be addressed. Typically, physical security and information security-related investigations are coordinated with an organization's Corporate Security Department.

3. ***Asset Classification and Control*** - Enterprise informational assets are defined and the required level of control for each has been identified. Safeguards are in place, ensuring that all informational assets receive the appropriate level of protection.

   The first step is to establish the categories that any informational asset may fall into. Typically, all assets fall into one of three categories. Open or public data is viewable by anyone inside or outside the organization. Company only or private data is viewable only by employees of the organization. Confidential data is viewable only by a sub-set of employees within the organization. There are instances where private or confidential data would be appropriate for viewing by external agencies or individuals such as vendors or business partners, but can be easily placed into these categories if proper access administration procedures are established.

   Every informational asset should have an identified "owner" who is responsible for defining which of the three categories that the asset should be placed into. If a confidential asset, the "owner" is also responsible for defining the subset of employees approved for viewing or manipulating the data. Owners should also be responsible for defining and ensuring the completion of user access administration procedures.

   Finally an independent group, such as Internal Audit, should perform periodic evaluations to ensure that the overall asset classification and control process is effective.

Technical Infrastructure

4. ***Computer and Network Management*** - Security procedures are incorporated into routine computer and network operations to maintain the integrity and availability of information processing and communication.

   Specific activities where security procedures should be incorporated include: Change management / testing – a risk assessment component should be included in any change management activity impacting the operating system environment, supporting network infrastructure or applications residing on the network. This will ensure that new security exposures are not created when changes or updates are performed. Appropriate audit trails for each operating environment and application should be implemented to facilitate the

identification and resolution of inadvertent and / or intentional security incidents. Anti-virus software and response procedures should be put in place. Network intrusion detection, vulnerability assessment and incident response processes should be established.

5. ***Physical and Environmental Security*** - Physical and environmental protections for IT assets are in place.

   In addition to preventing physical damage to or theft of IT assets, sound physical security procedures help to prevent system or application intrusions. For example, if an unauthorized person gains access to a data processing facility, he may be able to access system terminals to steal data or inject virus routines. While excessive heat to modern systems is not the threat (in many cases) it has been in the past, an environmental protection strategy is still needed to address fires, earthquakes and any other external influences that could impact a data processing facility.

6. ***System Access Control*** - Controls protecting against unauthorized access are in place for administrators as well as users.

   There are two primary focus areas in controlling system access: Security configuration and user access administration. Both of these focus areas must be addressed at several levels. At the application level, the security configuration must effectively control the desired types of access (read, write, update) and administration procedures must restrict these access types to currently authorized users. Database(s) utilized by the application must be configured to restrict direct access to authorized administrative and support personnel and administrative procedures must be in place for this user group also. Finally, security configuration and user access administration procedures must be in place to control access to the underlying operating system. If not in place, access to application databases may be possible. In most cases, those responsible for the security configuration and user access administration are different at each level. Sound policies and procedures are necessary to ensure that the required controls are consistently performed at each level.

7. ***Systems Development and Maintenance*** - Security checks and balances are built into application and systems development / maintenance procedures.

   The three primary checks and balances in the systems development and maintenance processes are testing, change management procedures for ongoing maintenance activities and user participation / signoffs in all facets. Including security testing in the development process ensures that the required controls are identified and implemented before the system "goes live". Including them in the change management process will ensure that security controls already in place are not "undone" as changes / upgrades are made. Finally, and most importantly, user participation will ensure that they have the final word and approval on the security controls that are in place to protect their data.

Information Protection

8. ***Personal Security*** - Users are aware of information security threats / concerns and are trained / equipped to support corporate security policies.

   An employee "lifecycle" approach can be taken to ensure that information security-related issues and threats are effectively addressed. The foundation of this "lifecycle" approach is the delivery of an information security overview to each employee at the time of hire (typically part of the orientation process). It should identify the organization's informational assets (paper based, system based, on PCs, on desktops, etc.) and the employees responsibilities and means for protecting them. The availability and location of supporting resources (policies, security staff, etc.) should also be provided. Where appropriate, job specific training should be provided (for example, public relations personnel should be trained on what can or can't be disseminated to the public). An ongoing "Awareness Program" will help to maintain the required level of understanding of and compliance with information security practices. Finally, periodic revalidations of each employees understanding of and commitment to information security should be performed. This can be done through annual reviews and employee signoffs.

9. ***Business Continuity Planning*** - Business continuity plans are in place across the enterprise to counteract interruptions to critical business activities / processes from the effects of major failures or disasters.

   There are two basic facets to the business continuity planning model. The source end addresses processing systems and the environment they are housed in and the destination end represents the business unit(s) that utilize the data. With the proliferation of midrange and microcomputers, the location of source and destination functions are not always separate and distinct as they were in the days when all processing took place in the data center. However, the planning requirements for each are the same regardless of the physical location of either the system(s) or user(s). Plans for the source end will always require the identification of processing requirements (provided by the user) and the development and testing of a strategy to meet those processing requirements. Conversely, plans on the destination (user) end will always need to take the same processing requirements and identify procedures to address them outside of the normal processing environment. While a comprehensive business continuity plan can range from a single sheet of "blue line" to a multi-volume binder, a successful plan must always include both source and destination components. All too often, only the source end is addressed.

10. ***IS Policy Compliance*** - Reviews are performed to ensure ongoing compliance with security policies and to avoid breaches of any criminal or civil law, and of any statutory, regulatory or contractual obligations.

    Information security is not a ***set it and forget it*** concept. System, application, people, laws and contractual obligations constantly change. As a result, both the activities governed by IS Policies and the policies themselves must be continually re-evaluated and tested. Although the IS staff should take a leadership role in the routine testing of business processes for IS policy compliance and the maintenance of policy content, there efforts should be augmented by internal and external audit organizations. Ideally, audit schedules will be jointly developed to ensure effective coverage.

A strategy for implementing ISO 17799

While the successful execution of this strategy begins with the ISO 17799 structure itself, an auditor's risk & control mentality is needed to ensure an effective implementation. After identifying the risks associated with each information management activity, procedures can be developed to mitigate or control the threats associated with each risk. Using user access to a key business application as an example, the primary risk (allowing unauthorized access to the application) and related threat (loss or manipulation of proprietary data) can be controlled through the development of sound administrative and maintenance procedures. The secret to a successful implementation strategy: ***Plan from the top down and implement from the bottom up.***

Planning from the top down

The top level of the planning hierarchy should identify those areas of information security management that, if effectively addressed, will stand up to the security demands of your CIO and other enterprise leaders, internal audit, business partners, customers and ultimately your investors. The ISO 1799 Security Standard defines these information security management focus areas in its ten control categories.

The next step as we move downward in our planning model is to identify those specific activities unique to every organization, that when addressed, provide the required assurances that each control area has been effectively addressed. An abbreviated sample listing of required activities for each control category is provided in the chart below.

The 10 Key ISO 17799 Control Categories for Information Security									
IS Organizational infrastructure			***IS Technical Infrastructure***		***Information Protection***				***Confirmation***
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
IS Policies	**Security Org.**	**Asset Category/ Control**	**Computer & Ntwk. Mgt.**	**Physical / Environ. Security**	**System Access Control**	**Systems Develop. And Mtce.**	**Personal Security**	**Business Continuity Planning**	**IS Policy Compliance**

- Identify required policy topics - Establish a policy review / approval process - Assign policy owners to prepare each policy - Make updated policies available to enterprise	- Identify and staff required positions - Establish clearly defined roles for each position	- Define asset security classes - Establish owners for all data items - Assign all data items to the appropriate class	- Establish information security procedures for all operational activities	- Identify and implement needed physical security changes	- Establish user access approval procedures - Establish ongoing userid mtce. procedures.	- Implement a universal change mgt process - Add security approval steps to the change mgt process	- Establish an information security awareness program - Establish a working relationship with Corporate Security	- Develop a common business continuity planning framework - Assign responsible business continuity managers for each key process	- Establish a testing process to evaluate the effectiveness of compliance controls

After the activities needed to provide the proper risk and control protections have been identified in our top down approach, procedures for performing those activities must be put in place. The effective implementation of these procedures requires a bottom up approach.

Implementing from the bottom up

The first step in the implementation of this bottom up approach is to break down each process into easy to perform and measure tasks. For each process, the following must be identified or performed:

- ***Establish role clarity***: While it seems obvious, all too often the "owner" is not clearly identified. Assigning responsibility / accountability for each process is the first step towards its successful implementation.

- ***Define duties and responsibilities***: Defining duties and responsibilities aids the process owner by clearly defining the scope of his / her responsibility. You can't be sure that you've completed "everything" unless you know what "everything" is.

- ***Identify specific tasks***: This step allows you to identify the specific tasks that must be performed to effectively address the assigned area of responsibility. Breaking things down to the task level enables you to move to the next step.

- ***Define completion standards***: Clearly defined completion standards and methodologies for measuring them provide the means to confirm the successful completion of each task.

- ***Implement the measurement / confirmation process***: This final step provides assurances that you have successfully completed all individual tasks.

Using the development and implementation of your organizations information security policies as an example:

- ***Establish role clarity***: Establish an owner for the overall policy development / maintenance process.

- ***Define duties and responsibilities***: Duties and responsibilities can be defined as: (1) Maintain the information security policy universe; (2) Oversee policy review / approval process; and (3) Ensure employee awareness of policy content.

- ***Identify specific tasks***: For (1) Maintain policy universe – Create a listing of all required individual policies and assign an owner for each policy. For (2) Oversee policy review / approval process – Identify and assign appropriate managers to act as review board, establish the review / approval process and schedule policy review dates. For (3) Ensure employee awareness of policy content – Prepare intra-company announcement of policies and place them on corporate intranet.

- ***Define completion standards***: In the policy example, the completion standards are evident in the listing of specific tasks. However, measurement criteria that define the successful completion of each standard should be defined.

- ***Implement the measurement / confirmation process***: One method for implementing this step is to have your internal audit organization perform an independent assessment of the overall information security policy process.

Barriers to success

The overall goal of this process is to identify, define and establish solutions or preventions to potential barriers. As a result, the remaining barriers fall into two areas – gaining the required support from upper management and non-IT departments and putting forth the effort required to perform the activities identified in this document.

The importance of gaining upper management approval cannot be overstated. Because a successful strategy requires interaction with and the participation of every employee, upper management support is needed to ensure this participation where the required time might not otherwise be allocated.

For most organizations, the concept that their proprietary information is a significant asset has yet to be fully appreciated. As a result, it has been easy for many organizations to put forth only a token effort towards addressing all the required activities.

In Conclusion

If you have identified the focus areas that must be included in your organizations information

security management strategy (the 10 ISO 17799 control categories), the activities that must be performed for each focus area, broken down each activity into measurable and manageable tasks and have confirmed that each task has been successfully completed, what have you accomplished?…..

You have taken a concept (information security), given it shape (using the ISO 17799 Security Standard as the foundation) and added substance by identifying all the activities that must be performed ….. using a process that is scalable for any business type and size. In addition to the ability to confirm your effectiveness in managing one of your organization's key assets (and liabilities) – its information, you now have a means to define / defend your strategy at any level of detail to any potential audience – your CIO and other enterprise leaders, Internal Audit, business partners, customers and ultimately your investors. Hence, you have a comprehensive verifiable approach towards information security management – your primary safeguard against information security litigation in the 21st century. Remember – ***Where there are no laws, the laws will be built in the courtroom.***

References

1. Can be taken to court
Vijayan, Jaikumar. "IT Security Destined For The Courtroom" Computerworld 21 May 2001. URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO60729,00.html (31 May 2001).

2. Companies / Individuals can be fined, go to jail
Schreider, Tari. "The Legal Issues of Disaster Recovery" Disaster Recovery Journal April, May, June 1996.
URL: http://www.drj.com/new2dr/model/schr.htm

Cronin, Kevin. "As Courts Increasingly Hold Firms Liable For Losses Caused By Computer Failures, Recovery Capabilities Are Fast Becoming A… Legal Necessity" Disqaster Recovery Journal.
URL: http://www.drj.com/new2dr/w2_022.htm

3. ISO 17799 Security Standard overview
URL: http://www.securityauditor.net/iso17799/what.htm

4. Information Security Policies & Best Practices
URL: http://iwsun4.infoworld.com/articles/op/xml/00/11/20/001120opswatch.xml

5. Technology as a problem facilitator
Gibson, Steve. "The Strange Tale of the Denial of Service Attacks Against GRC.COM"
URL: http://grc.com/dos/grcdos.htm