Proceedings of the 8th Colloquium for
Information Systems Security Education
West Point, NY June 2004

Teaching Information Security Policy

Herbert J. Mattord, CISSP & Michael E. Whitman, Ph.D., CISSP

Abstract: Information security education includes many topics, some technical and some managerial. One topic that is central to all of these is that of information security policy. Before policy can become the centerpiece of information security education, a coherent model that can encompass the broad range of the topic is needed. In addition to the essential elements of policy, students also need to be exposed to the best practices for managing information security policy. Once a teaching model for policy is selected, faculty can use lectures, project assignments and lab exercises to reinforce student learning.

Index terms – Information Security Education
Information Security Policy
Information Security Lab Practices

I. Introduction

The success of information security programs comes from the use of policy [1]. Successful outcomes in educating the undergraduate in information security topics are improved when a program of study in information security conveys the central nature of policy. This success can be extended even further when an understanding of what comprises sound policy and how to create and maintain a policy management program are also included in the curriculum. Teaching policy effectively is the essential foundation of an effective information security education program. As stated by Charles Cresson Wood, in his widely referenced book Information Security Policies Made Easy,

> "The centrality of information security policies to virtually everything that happens in the information security field is increasingly evident. For example, system administrators cannot securely install a firewall unless they have received a set of clear information security policies. These policies will stipulate the type of transmission services that should be permitted, how to authenticate the identities of users, and how to log security-relevant events. An effective information security training and awareness effort cannot be initiated without writing information security policies because policies provide the essential content that can be utilized in training and awareness material"[2].

II. Why Policy?

A quality information security program begins and ends with policy [3]. The newest revision of *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)* from the National Institute of Standards and Technology (NIST) leaves little doubt that sound policy planning and execution is the only sure foundation for effective information security planning and operation [4]. Teaching students how to properly develop and implement policies enable them to create and manage information security programs that function almost seamlessly within the workplace. Although information security policies are the least expensive means of control to execute, they are often the most difficult to implement. Policy controls cost only the time and effort the management teams spends to create, approve, and communicate them, and that employees spend integrating the policies into their daily activities. Even when the management team hires an outside consultant to assist in the development of policy, the costs are minimal compared to the other forms of control, especially technical controls. Information security students equipped with skills in the development and management of policy will be able to contribute positively to any future employer.

Some basic rules must be followed when shaping a policy:

- Policy should never conflict with law
- Policy must be able to stand up in court, if challenged
- Policy must be properly supported and administered

Since policy is often difficult to implement, Bergeron and Bérubé have proposed guidelines for the formulation of computer policy, which are also directly applicable to information security policy [5]. They further note that policy must be tailored to the specific needs of the organization and, while it is an admirable goal for policies to be complete and comprehensive, too many policies or policies that are too complex can lower end user satisfaction [6].

ISBN 0-87145-192-1/04/$15.00

III. POLICY, STANDARDS, AND PRACTICES

Policy is a plan or course of action intended to influence and determine decisions, actions, and other matters. In other words, policies are a set of rules that dictates acceptable and unacceptable behavior within an organization. The relationship between policy and planning activities is brought into focus in NIST's *Guide for Developing Security Plans for Information Technology Systems* [7]. This widely referenced document notes that not only does organizational security policy govern the planning process, but that effective planning requires the overall direction and guidance of well-formed policies.

Policies must also specify the penalties for unacceptable behavior, and define an appeal process. An example of a policy would be an organization's prohibiting the viewing of inappropriate Web sites at the workplace. To execute this policy, the organization must implement a set of standards that clarify and define exactly what is inappropriate in the workplace and to what degree the organization will act to stop the inappropriate use. A **standard** is a more detailed statement of what must be done to comply with policy. In the implementation of such an inappropriate use policy, the organization may create a standard that all inappropriate content will be blocked and then list the material that is considered inappropriate. Later in the process, technical controls and their associated procedures will be established such that the network will block access to pornographic Web sites. **Practices, procedures** and **guidelines** explain how employees will comply with policy. Figure 1 illustrates the relationship among policies, standards, and practices.

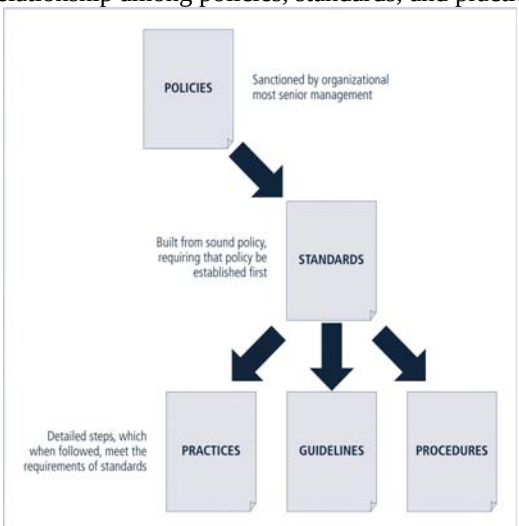

Figure 1 - Policies, Standards and Practices

For policies to be effective they must be properly disseminated, via printed personnel manuals, organizational intranets, and periodic supplements. All members of the organization must read, understand, and agree to abide by the organization's polices. Policies require constant modification and maintenance. As the needs of the organization evolve, so must its policies.

In order to produce a complete information security policy, management must define three types of information security policy. These three types are based on *Generally Accepted Principles and Practices for Securing Information Technology Systems, NIST Special Publication 800-14*, which outlines the requirements of writing policy for senior managers [8].

The three types of policy are:

- Enterprise information security program policy
- Issue-specific information security policies
- Systems-specific information security policies

Each of these policy types is often found in most organizations. The usual procedure is to create the highest level of policy first, the enterprise information security policy. After that, those instances where the general security policy indicates a need for more detailed policies, are supported with issue- and system-specific polices as needed.

Not everyone with a stated approach to information security policy shares that NIST structure and nomenclature used in this paper. For instance, Charles Cresson Wood also supports the concept of a general high-level document, titled simply 'Information Security Policy' in his book Information Security Policies Made Easy [9]. However, he does not adopt the issue-specific vs. system-specific terminology, instead noting that all subsequent policy documents, deriving from the top-level Information Security Policy are collectively called detailed information security policies.

Another approach is offered by Barman who suggests that "rather than trying to write one policy document, write individual documents and call them chapters of your information security policy." [10] This implies that a monolithic or modular approach, with only one level of granularity is his recommendation. Compare this with the other end of the terminology complexity spectrum where Wadlow's treatment of policy preparation avoids terminology altogether noting that "[a simple process] works as well as anything and better than most for getting something useful in place as quickly as possible." [11]

The three types of policy using the NIST recommended nomenclature are described in detail in the following sections.

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

A. Enterprise Information Security Policy

An **enterprise information security policy (EISP)** - also known as a security program policy, general security policy, IT security policy, high-level information security policy or information security policy—sets the strategic direction, scope, and tone for all of an organization's security efforts. The EISP assigns responsibilities for the various areas of information security, including maintenance of information security policies, and the practices and responsibilities of end users. In particular, the EISP guides the development, implementation, and management requirements of the information security program, which must be met by information security management, IT development, IT operations and other specific security functions.

This policy must directly support the vision and mission statements of the organization. It must also be compatible with the ability of the organization to successfully defend its policies if they are challenged in the courts. The EISP is an executive-level document, drafted by the CISO in consultation with the CIO, is usually two to ten pages long, and shapes the security philosophy in the IT environment. The EISP usually does not require repeated or routine modification, unless there is a change in the strategic direction of the organization.

The EISP plays a number of vital roles, not the least of which is to state the importance of information security in support of the organization's mission and objectives. Information security strategic planning derives from the IT strategic policy, which is derived from the organization's strategic planning. Unless the EISP directly reflects this association, the policy will likely become confusing and counter-productive.

1. EISP Elements

Though specifics of EISPs vary from organization to organization, most EISP documents should provide the following:

- An overview of the corporate philosophy of security
- Information on the structure of the information security organization and individuals that fulfill the information security role
- Fully articulated responsibilities for security that are *shared by all members* of the organization
- Fully articulated responsibilities for security that are *unique to each role* within the organization [12].

The following elements are often found in the EISP:

- *Statement of Purpose* - Answers the question "What is this policy for?" Provides a framework for the reader to understand the intent of the document.
  - *Information Technology Security Elements* - Defines information security and can also lay out security definitions or philosophies in order to clarify the policy.
  - *Need for Information Technology Security* - Provides information on the importance of information security in the organization and the obligation (legal and ethical) to protect critical information.
  - *Information Technology Security Responsibilities and Roles* - Defines the organizational structure designed to support information security within the organization.
  - *Reference to Other Information Technology Standards And Guidelines* - Outlines lists of other standards that influence and are influenced by this policy document.

The formulation of program policy in the EISP establishes the overall information security environment. As noted earlier, there are many specific issues that require policy guidance beyond what can be offered in the EISP. The next level of policy document, the issue-specific policy, delivers the specificity.

B. Issue-Specific Security Policy (ISSP)

A sound **issue-specific security policy** provides detailed, targeted guidance to instruct all members of the organization in the use of technology based systems. The ISSP should begin with an introduction of the fundamental technological philosophy of the organization. It should assure the member of the organization that the purpose of the policy is not to provide a legal foundation for persecution or prosecution, but to provide a common understanding of the purposes for which an employee can and cannot use the technology. Once this understanding is established, employees are free to use the technology without seeking approval for each type of use. This serves to protect both the employee and the organization from inefficiency and ambiguity.

An effective ISSP articulates the organization's expectations about how the technology-based system in question should be used while it documents how the technology-based system is controlled and identifies the processes and authorities that provide this control, and serves to indemnify the organization against liability for an employee's inappropriate or illegal system use

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

An ISSP is a binding agreement between parties (the organization and its members) and shows that the organization has made a good faith effort to ensure that its technology is not used in an inappropriate manner. Every organizational ISSP should address specific technology-based systems and will require frequent updates as well as contain a position statement for the issue [13].
An ISSP may be drafted to cover many topics, including:

- Electronic mail
- Use of the Internet and the World Wide Web
- Specific minimum configurations of computers to defend against worms and viruses
- Prohibitions against hacking or testing organization security controls
- Home use of company-owned computer equipment
- Use of personal equipment on company networks
- Use of telecommunications technologies (fax, phone)
- Use of photocopy equipment

1. Components of the ISSP

The typical ISSP includes components such as:

- *Statement of Purpose* - The ISSP should begin with a clear statement of purpose that outlines the scope and applicability of the policy.
- *Authorized Access and Usage of Equipment* - Addresses who can use the technology governed by the policy, and for what purposes as well as addressing legal issues, such as protection of personal information and privacy.
- *Prohibited Usage of Equipment* - The previous section specifies what *can* be done but this section outlines what *cannot* be done. Note that ISSP sections Authorize Access and Usage of Equipment and Prohibited Usage of Equipment might be more efficiently combined into a section entitled Appropriate Use Policy.
- *Systems Management* - Focuses on the users' relationships to systems management. By specifying user and systems administrator responsibilities, so that all parties know what they are accountable for.
- *Violations of Policy* - Specifies the penalties and repercussions of violating the usage and systems management policies.
- *Policy Review and Modification* - Documents policy management procedures and a timetable for periodic review.
- *Limitations of Liability* - The final section is a general statement of liability or set of disclaimers. If employees violate a policy or any law using company systems, the organization will not protect them, and is not liable for their actions, assuming that the violation is not known or sanctioned by management.

A specific ISSP that needs to be included is one regarding incident response. A useful source of insight into how to structure an issue-specific security policy for incident response can be found at the Computer Emergency Response Team Coordinating Center (CERT/CC) within the Software Engineering Institute at Carnegie Mellon University. In an article titled "Establish a policy and procedures that prepare your organization to detect signs of intrusion" the step-by-step needs of this type of ISSP are explored. [14] While the CERT/CC does not promulgate any specific nomenclature regarding the structure or format of information security policy documents, the proposal referenced above is consistent with NIST-based structure proposed here.

2. Implementing ISSP

There are a number of approaches for creating and managing ISSPs. Three of the most common are:

- Create a number of independent ISSP documents, each tailored to a specific issue
- Create a single comprehensive ISSP document that aims to cover all issues
- Create a modular ISSP document that unifies policy creation and administration, while maintaining each specific issue's requirements This results in a modular document with a standard template for structure and appearance where certain aspects are standardized, and others elements and much of the content is customized for each issue. The end result is a number of independent ISSP documents, all derived from a common template and physically well-managed and easy to use.

The recommended approach is modular, which provides a balance between issue orientation and policy management. The policies created via this approach are individual modules, each created and updated by individuals responsible for a specific issue. These individuals report to a central policy administration group that incorporates these specific issues into an overall policy.

C. Systems-Specific Policy (SysSP)

While issue-specific policies are formalized as written documents readily identifiable as policy, systems-specific policies (SysSPs) frequently do not look like other types of policy. They may often be created to function as standards or procedures to be used when configuring or maintaining systems. SysSPs can be separated into two general groups, management guidance and technical specifications, or they may be combined into a single policy document.

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

1. Management Guidance SysSPs

This type of document is created by management to guide the implementation and configuration of technology as well as address the behavior of people in the organization. Any technology that affects the confidentiality, integrity or availability of information must be assessed to evaluate the tradeoff between improved security and restrictions.

2. Technical Specifications SysSPs

This type of policy is used to translate management intent for a technical control into an enforceable technical procedure. There are two general methods of implementing such technical controls:

Access Control Lists - Access control lists (ACLs) include the user access lists, matrices, and capability tables that govern the rights and privileges of users. These specifications are frequently complex matrices, rather than simple lists or tables.

Configuration Rules - Specific configuration codes entered into security systems to guide the execution of the system when information is passing through it.

IV. Policy Management

Policy, once developed, will require ongoing management in order to monitors, maintains, and modifies the policy as needed to ensure that it remains effective as a tool to meet changing threats. The exact management process used to assure that the policy documents are organized and maintained properly will vary with each organization. Regardless of the specific management methods, every organization should manage the policy environment so that each policy element should have built-in mechanisms that ensure periodic review and accountability within the organization as well as the correct assignment of subject matter expertise so that the policies are accurate and effective.

The need for effective policy management has led to the emergence of a class of software tools that support policy development, implementation and maintenance. Whichever vendor provides the software, a centralized policy approval and implementation system should allow policy developers to create policy, manage the approval process with multiple individuals or groups, and distribute approved policy throughout their organizations. It should also assess the readers' understanding of the policy and electronically record policy reader acknowledgements. This reduces or eliminates the need to distribute hard copies of documents that might go unread, and to manage multiple policy receipt acknowledgement forms. Tools such as described here keep policies confidential, behind password-protected intranets, and generate periodic reports indicating which employees have and have not read and acknowledged the policies.

V. Teaching Methods

Lecture alone is insufficient for complete student learning in the area of policy. If the instructor seeks learning outcomes beyond simple understanding, up to the level of competence or mastery, reinforcement techniques using exercises, projects, simulation, practical experiences and/or laboratory exercises will be required.

A common approach used by the authors is to couple direct lecture on the topic with individual exercises and then to follow-up with projects using case assignments. This gives the student the time and opportunity to absorb the material and allows them to absorb and extend the lecture content through the analysis of example policies that emphasize industry best practices. The case assignments used frequently portray organizations with no distinct policies. Students can analyze these cases, ask pertinent questions, and develop draft policies. A review of the strengths and weaknesses of each policy provides clear feedback on policy issues.

A logical next step after this theoretical grounding in theory is for the students to apply the theories by performing an evaluation of information security polices of their academic institution or place of employment and provide critical analyses of these polices in light of the theory. Some students may be positioned to bring policies from their places of employment into the classroom. Many students have received positive feedback from their employers when they brought revised copies of policies back to work. Care should be exercised in sharing the contents of such policies without expressed permission of the source organization, as many organizations treat the policies as both proprietary material as well as being classified as confidential documents. Make sure students that undertake this type of exercise receive the proper permissions from their employers before sharing these policies.

Review of existing policies to reinforce theoretical learning is very useful, but the process can be further extended. The value of having the student engage in the process of synthesis will extend and enhance the learning outcome to another level. The models and frameworks for information security policies presented in lecture and illustrated by example represent best practices as derived from research on the state of the industry. Students will gain value from researching additional practices and examples beyond those included in the base curriculum and can be encouraged to develop individual methods based on the materials and procedures they locate and

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

find useful. Synthesis continues by having the student extend the theoretical frameworks both learned from lecture and developed in research. Building on these basic frameworks will offer the student the opportunity to extend their understanding by creating policy documents using a case study. The case used for these assignments may be drawn from actual organizations or from fictional scenarios. Students then complete the process by customizing the framework to meet the needs of the case setting. In practice, this will result in a great diversity in the work products from the students which can then serve as the basis for in-class evaluation and discussion. Performing analysis and critique of existing policies represents one degree of learning, while creating policy from frameworks and research is at a higher level of mastery.

Of importance at this point is to emphasize that the success of the implementation model will always be a critical aspect of any policy development program. The best practices of the industry crafted into well-written and fully customized policies are destined to be ineffective if they are not implemented, read, understood and agreed to across the organization. Courts have continually held that the policy is not enforceable unless the organization can positively demonstrate that a policy is distributed, read, understood and agreed-to. Teaching students the value of creating effective policy is important, but it is equally important to reinforce the need for effective distribution and management mechanisms. Every student completing the unit of instruction on information security policy must know that simply pinning policies to bulletin boards falls short of the legal definition of distribution. Students must understand that the documents, in whatever physical or electronic form, must be placed into the hands and before the eyes of those members of the organization (employees, contractors and business partners) that need them.

The next lesson is to verify that the student understands information security policy consumers must be able to read and understand the policy that is distributed. Literacy barriers, whether as a result of ignorance, language or culture, can negate the read and understood requirement. It is incumbent on the organization to take whatever steps are necessary to provide all policy content to every member of the organization in a form and format that can be understood.

Finally, the student must understand the impact of the phrase “agreed-to”. Some record keeping mechanism must be in place to document the receipt of the policy content and the acknowledgment of an agreement to comply with that policy. One possibility is for the organization to procure a signed and notarized document that indicates consent of the employees. This is an onerous requirement and few, if any, organizations maintain this level of documentation. Most organizations have settled for signed acknowledgment pages, often distributed as the last page of the policy document. These pages are signed by the member of the organization to document receipt and agreement to comply. The proliferation of electronic distribution mechanisms associated with software, often via corporate Intranets, has seen the emergence of a new paradigm. By replicating the features of software distribution approaches, the policy equivalent of an end-user license agreements (EULAs) allow for the recording of a conscious indication of acceptance. Software distribution mechanisms, such as those used by the products described in the laboratory procedures below are examples of this emerging paradigm.

VI. Reinforcing Policy Learning With Laboratory Exercises

Another valuable method used to reinforce student learning from lectures and policy writing is the use of commercial policy management software. This practice of using commercial software in the laboratory also prepares students to be more productive when they join the work force. Using the demonstration version of a product such as VigilEnt Policy Center from NetIQ Corporation, a student can gain hands-on experiences creating policy and learning valuable techniques in policy management.

A number of laboratory exercises conducted using this and similar products begin with the in-class and homework policy drafting exercises as noted above. Once the student has completed such a policy writing assignment, and has opportunity to correct it, they can use the laboratory setting to gain experience in the use of the policy authoring and management tool.

These types of lab exercise provide a number of opportunities to gain an understanding of the policy management process. This begins with the use of the tool in the policy authoring phase, where the students electronically upload and revise their draft policies. Alternatively, some of the products that may be used, most notably the VigilEnt Policy Center, provide extensive libraries of policy templates that may be used by the student as extended examples, or even initial draft policy documents. These policy documents are then deployed in a simulated organizational environment allowing the student to create access control mechanisms for reviewers and users of the policy. The lists of users with access are then used to demonstrate the policy review and approval procedures. In the lab implementation it is beneficial to organize students into groups and allow each to serve as reviewers, approvers, and ultimately users for their teammates’ policies. This

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

will allow the simulation of the typical organizational setting of management review and approval. The students also gain experience in small group collaboration as they work in a team to review, correct and eventually collaboratively approve their teammates' policies.

Once approved, each student policy author creates a set of questions to test the policy content retention for the future simulated users of the policy. These quizzes are then used in the final part of the lab exercise when students take turns being the users of the policy management software and simulate the reading and acceptance part of the process. The software used provides a thorough examination of the factors faced in real organizations, providing a number of distribution, acknowledgment and non-repudiation mechanisms, including logging the times that the reviewers, approvers, and users access the policies and perform their assigned tasks.
For the user to formally acknowledge acceptance of the policy, they have to attest that they have read, understood and will comply with the policy. To document this, they perform two tasks; First they read and click a check box captioned "I have read and will comply", Second they take a quiz on the policy. The policy author can select the level of performance on the quiz that will signify acceptable understanding of the policy, typically around 70 percent.

This instructional technique involving laboratory use of automated policy management has resulted in substantially better learning outcomes in the teaching of organizational information security policy. While of great benefit to organizations when applied to creation, approval, distribution and maintenance of information security policy, the tools are also useful for virtually any policy or procedural document. With the inclusion of best practices in the development of information security policy, drafted by Charles Cresson Wood, the VigilEnt Policy Center provides both an instructional tool in the development of policy as well as an effective way to teach students about the implementation and ongoing management of policy.

VII. Conclusion

In order for students to effectively learn about the legal, ethical and technical aspects of information security policy, instructors of the subject must first ensure they teach the content from a source drawn from recognized industry best practices. This paper seeks to provide a concise common denominator on the subject providing definitions and frameworks developed from extensive study of published sources in government and industry covering policies at all levels of the organization, from strategic enterprise information security policies, to tactical issue specific and system specific policies.

When the learning experience is richer, providing depth and breadth of content presented in a valid context and suitably reinforced with skill building exercises, there is a higher probability of retention of subject knowledge. Simply lecturing on the proper format and content of policy is insufficient to ensure the desired degree of learning by the student. By requiring students to draft, evaluate, critique, and then implement, review and test on policy, the students gain a much deeper understanding. Not only do they learn the skills of authoring the documents, using policy management software to implement policy, they also learn the reasons behind the policy creation process and the ongoing managerial responsibilities associated with the use of policy in the organization. It is hoped that by understanding the value of both the content and the organizational context of information security policy, the reader will be better qualified to instruct students of information security policy in the subject.

VIII. References:

[1] *Executive Guide to the Protection of Information Resources NIST Special Publication 500-169*. Retrieved March 16, 2004 from the National Institute of Standards and Technology Web site: http://csrc.nist.gov/publications/nistpubs/500-169/sp500-169.txt

[2] Charles Cresson Wood, Information Security Policies Made Easy, Ninth Edition (2003) NetIQ Corporation p 1.

[3] Charles Cresson Wood, "Integrated Approach Includes Information Security", *Security* 37, no. 2 (February 2000): 43-44.

[4] *Engineering Principles for Information Technology Security (A Baseline for Achieving Security), NIST Special Publication 800-27 Rev A*. Retrieved April 25, 2004 from the National Institute of Standards and Technology Web site: http://csrc.nist.gov/publications/drafts/SP800-27-RevA-Draft.pdf

[5] F. Bergeron and C. Bérubé, "End Users Talk Computer Policy." *Journal of Systems Management*. 41(12) December 1990. Pp. 14-17.

[6] Ibid.

[7] Marianne Swanson, *Guide for Developing Security Plans for Information Technology Systems, NIST Special*

Publication 800-18. Retrieved April 25, 2004 from the National Institute of Standards and Technology Web site: http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.PDF

[8] *Generally Accepted Principles and Practices for Securing Information Technology Systems, NIST Special Publication 800-14.* Retrieved April 25, 2004 from the National Institute of Standards and Technology Web site: http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf.

[9] Charles Cresson Wood, Information Security Policies Made Easy, Ninth Edition (2003) NetIQ Corporation p 1.

[10] Scott Barman, Writing Information Security Polices. (2002). P. 7. New Riders, Indianapolis, IN.

[11] Thomas A. Wadlow, The Process of Network Security. (2000): Pp. 15-19. Addison Wesley Longman, Inc. Reading, MA.

[12] Derived from a number of sources, the most notable of which is http://www.wustl.edu/policies/infosecurity.html

[13] Ibid.

[14] "Establish A Policy and Procedures That Prepare Your Organization to Detect Signs of Intrusion." Computer Emergency Response Team Coordinating Center (CERT/CC) within the Software Engineering Institute at Carnegie Mellon University. Retrieved April 25, 2004 from the CERT/CC web site at http://www.cert.org/security-improvement/practices/p090.html

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE