Global Information Assurance Certification Paper

Elements of Security Policy – Considerations for Small Businesses

Christopher Keller

GSEC Certification Practical Assignment, version 1.2f

Introduction

Small businesses, like all businesses, increasing depend on computer systems and networks to do business. Email has become a critical communications tool for many small businesses. Websites are important marketing channels, and for businesses with eCommerce sites important sales producers. With the increasing dependency on computer systems comes and increasing need to secure them, just as the door locks and safes secure the brick and mortar and the valuables and secrets of businesses. The Honeynet Project has researched the security implications of hooking a computer to the Internet through a modest broadband connection of the type many small businesses employ. Windows and Linux systems installed without provisions for security were typically scanned, attacked, and compromised within a week. In addition, from May 2000 through February 2001 the project saw a 100% increase in the number of scans, indicating that the security threat is growing rapidly. Even if too pessimistic by an order of magnitude, these findings indicate a serious threat to information security from connections to the Internet.

Few small businesses, outside of computer consulting and security firms, are inherently or particularly interested in security, network or otherwise. Security and its associated activities is a drain on resources. Those resources are needed for the purpose of the business, or represent the profits the business is intended to generate. Information security is for the most part intangible, its most conspicuous elements less visible than a lock on the door or a safe. In a paper written for GIAC certification, Greg Bassett describes an approach for convincing management of the need for computer security. This paper addresses the considerations that should be made when drawing up a security policy, the foundation document for information security.

Security Policy Document

A security policy document has several functions. As the term suggests, it documents security policies. It does more than just document them. It provides a framework within which policies can be written, modified, and assessed. A security policy document should also provide the context that relates the policies to the business. Internet Security Systems, Walker and Cavanaugh, and many other sources available in books or on the Internet provide outlines for security policy documents. They give guidance for writing introductions as well as individual security policies. Guidelines vary in the specific content and emphasis they recommend. Every security policy document should have an extensive introduction as well as the individual security policies.

Introductory Elements

The introductory section of a security policy document sets the policies in the context of the business they are intended to protect. The introduction should be tailored to the business, but should address at least these areas: the purpose of the document; the scope of the document and policies; specific organizational responsibilities; general and specific objectives of the organization in terms of security policy; and a threat and risk assessment.

Purpose

The purpose of a security policy document, while somewhat standard, can be influenced by the extent to which the business deals with confidential information, and the means by which systems and networks are administered, either dedicated in-house staff, additional duties for other staff, or outsourced.

Scope

The scope definition should clearly delineate what is covered in the policies, and should resolve ambiguity about what is not covered. In particular, a small business must decide whether the security policies cover acceptable use policies and disaster recovery policies. Many sources recommend they do. For small businesses these may not be necessary. For a small group of employees acceptable use may be determined by group consensus. For some small businesses the redundancy required for a full disaster recovery or business continuity plan is financially prohibitive. For others, these and other policies may be supplemental documents, as the Joint Information Systems Committee in the UK suggests.

Responsibilities

Every organization must consider and assign the responsibilities for security. Responsibilities can be assigned to individuals or to positions within the organization.

Objectives

The overall objective of security and security policy is often cited as the triangle of confidentiality, integrity, and availability of information resources. This definition can be found in the European ITSEC security criteria of 1991, but its elements are much older than that. For the purposes of a specific business's security policy the objectives should be enunciated as confidentiality, integrity, and accessibility of specific resources which are important to the business.

Threat and Risk Assessment

The threat and risk assessment is one of the most important elements of the security policy document. The threat assessment identifies what the policies are intended to protect against. Some threats are standard, for example the threat of attacks from the Internet and the Honeynet Project research shows. Other sources of threat may be of less concern to small businesses, such as threats from insiders. The risk assessment allows management to prioritize the threats to security, which allows the limited resources that a small business can devote to security to be spent judiciously. It provides a basis for auditing the document. All policies should address threats identified in this section. If policies are formulated which do not it indicates more threat assessment is needed. The converse is not true, some threats may not justify policies if their risks are low. The risk assessment is very specific to the business and its unique situation.

Policy Attributes

Each policy should define a common set of attributes. The business should decide what attributes each policy should have, and should create a template for security policies which provides a framework for these attributes. The following sections discuss commonly used attributes. These attributes may be tailored to fit the business's preferences, but the information they contain ought to be found somewhere in the security policy document.

Identification

Each security policy should have a unique identification. Policies need to be easy to reference both within the security policy document, in supplemental external documents, and in audit tools such as coverage matrices. Policy IDs can be numeric, alphanumeric, or textual. Many documents use both a unique number and a textual name to identify each policy.

Policy Statement

The policy statement defines the policy. It should be clear, concise, and unambiguous. The statement should convey management's intent, but should not be over generalized.

Elaboration

It can be useful to elaborate upon the policy statement, providing the thinking behind it, clarifying its intent, and discussing its limits.

Threat addressed

Every policy should be mapped to at least one threat identified in the threat and risk assessment. Many policies address multiple threats, but if a policy cannot be

tied to at least one identified threat then either the policy should be dropped or the threats reassessed.

Exceptions

Like many business policies, security policies are not necessarily absolute. The policy should identify any foreseeable exceptions. The circumstances of exceptions should be clearly defined, as should the limits.

Violations

Every business should consider what actions should be taken when security policies are violated. The policy framework should provide a means of documenting actions to be taken in response to violations. While disciplinary policies belong in a personnel manual rather than in the security policy document, the severity of response for violating particular security policies should be considered and guidelines for dealing with violations should be documented with them.

References

Some policies stand on their own. Some policies have meaning only when they override, extend, or complement other policies. The framework should provide a standard way of documenting these relationships.

History

Since policies can change over time, the policy framework needs to allow for tracking the changes to individual policies. The modification history of policies is important for audits.

Areas of Coverage

The areas a security policy document addresses should correspond to the threats identified in the introductory section. However, individual policies are much more narrowly construed, a single threat can give rationale for many policies. Many guidelines can be used to identify areas a business's security policies should cover. The National Infrastructure Protection Center tips and the SANS Top Twenty Internet security vulnerabilities identify areas which should be considered when writing any security policy document. While every security policy document will be different, the following sections enumerate areas that probably need coverage in most of them.

Physical Security Policies

Physical security policies are concerned with physical access to server rooms, computers, and other resources which can be appropriated. These policies may

address the security of media such as backup tapes, emergency recovery diskettes, and printouts; and might address administrative password escrow notebooks. For businesses that deal with highly sensitive documents the policies might specify handling and discarding of printouts, CDs, and diskettes.

Network Security Policies

Network security policies are typically the most numerous and important since networks are vulnerable to both internal and external threats if not secured properly. Network security policies cover firewalls, Virtual Private Networks, wireless access, modem usage, installation of devices on the network, and anything else concerned with connections to the network. These policies may also address network monitoring, logging, and intrusion detection.

Host Security Policies

Policies regarding the configuration of individual computer systems or hosts may be a part of network security policies, but usually are distinctive enough to warrant their own classification. Host policies may cover the configuration of servers, standardization of workstations, allowable software, required software such as virus protection programs, and what data may be stored on what types of host. Since unauthorized control of individual host computers is a frequent security threat host policies may address both intrusion detection that reveals when a host has been compromised, and backup policies which allow recovery from a compromise. Host security policies may cover a broad range, from high risk servers exposed on the Internet to what information may be carried on laptops while travelling.

User Security Policies

User security policies may cover both what is expected of users in terms of behavior which enhances security, and how users are treated. User actions can greatly influence the effectiveness of security policies, for example choosing good passwords and protecting them from inadvertent disclosure. User security policies should also cover how users are given access to systems and documents, and how users are grouped for security purposes.

Document Security Policies

For any business which deals with sensitive information, document classification will be frequently referenced in other security policies. Document handling policies may also be needed. Encryption policies may be a part of document security policies.

Documentation Policies

Documentation is not always identified as a key area of security policy, but having adequate procedure and network documentation greatly enhances the ability to implement policy, to audit for security, and to insure that policy implementation remains effective as personnel change.

Incident Handling Policies

While thorough implementation of good security policies can greatly reduce the likelihood of a security incident, no action can guarantee an incident will not take place. Defining incident handling policies in the security policy document is the first step in effective incident handling. Incident handling policies should express management priorities in responding to security incidents, such as preservation of evidence verses restoration of services. Such decisions are best contemplated before they are needed.

Audit Policies

Audit policies specify the frequency and intensity of various types of security audits. Security is an ongoing process. Over time threats change, security countermeasures change, the network changes, and the business changes. Periodic reassessments are necessary to adapt to these changes. The security policy document itself should be assessed from time to time. The systems and procedures put in place to implement security policies should be audited to insure they are providing the security intended. Audit policies should also specify who will carry out different audits, whether employees or external auditors.

Conclusion

The security policy document is the foundation upon which security procedures and practices are built. It must be a living document, growing and changing over time as the business activities and threats change. A strong document framework and good security policy templates facilitate the creation of a thorough, useful security policy document, and provide the flexibility and control needed for effective modifications. Small businesses need flexibility in creating and modifying security policies in order to align the needs of the business and the resources available for security with the threats.

References

The Honeynet Project, "Know Your Enemy: Statistics", 23 July 2001, URL: http://project.honeynet.org/papers/stats.

Bassett, Greg, "Developing a Computer Security Proposal for Small Businesses - How to Start", SANS Information Security Reading Room, 8 August 2000, URL: http://www.sans.org/infosecFAQ/policy/cssb.htm.

Internet Security Systems, "Creating, Implementing and Managing the Information Security Lifecycle: Security Policy, E-Business and You", 25 Sept 2001, URL: http://documents.iss.net/whitepapers/SecurityCycle.pdf.

Walker, Kathryn M. and Linda Croswhite Cavanaugh, Computer Security Policies and SunScreen Firewalls, Sun Microsystems Press, ISBN 0-13-096015-2, July 1998.

Joint Information Systems Committee, "Developing an Information Security Policy", 27 Feb 2001, URL: http://www.jisc.ac.uk/pub01/security-policy.html.

Department of Trade and Industry, London, "Information Technology Security Evaluation Criteria: Harmonized Criteria of France, Germany, The Netherlands, and The United Kingdom", 1991, URL: http://www.cesg.gov.uk/assurance/iacs/itsec/documents/formal-docs/media/ltsec.pdf.

National Infrastructure Protection Center, "Seven Simple Computer Security Tips", URL: http://www.nipc.gov/publications/nipcpub/computertips.htm.

SANS Institute, "The Twenty Most Critical Internet Security Vulnerabilities: The Experts Consensus", 10 October 2001, URL: http://www.sans.org/top20.htm.