Summer 2008

Recommendations for Applying Security-Centric Technology Utilizing a Layered Approach in the Era of Ubiquitous Computing: (A Guide for the Small Business Enterprise).

YeVetta Gibson
Regis University

Regis University

School for Professional Studies Graduate Programs

Final Project / Thesis

DISCLAIMER

Recommendations for Applying Security-Centric Technology Utilizing A Layered Approach in the Era of Ubiquitous Computing: (A Guide for the Small Business Enterprise).

By

YeVetta Gibson

YeVettaGibson@yahoo.com

A thesis/Practicum Report submitted in partial fulfillment of the requirements for the degree of Master of Science in Computer Science and Information Technology Management

School of Computer & Information Sciences
Regis University
Denver, Colorado
Aug 20, 2008

Chapter 1

Abstract

Gibson, YeVetta. MSCIT Program. The School of Professional Studies. Regis University, Denver, Colorado. May 2008. Applying Security-Centric Technology Utilizing A Layered Approach in the Era of Ubiquitous Computing: (A Guide for the Small Business Enterprise).

The purpose of this work is to advise and assist Small Business in applying security centric technology to better manage and secure their information assets. Computer Crimes and Incursions are growing exponentially, in complexity, and in their sinister application. In the face of this onslaught small businesses, indeed organizations everywhere, need to accept this as a business constant or reality, identify the threats, acknowledge the vulnerabilities, and make plans to meet these challenges.

This project proposes to provide small business with the principles of desktop, laptop, remote, and network security along with the tools and strategies by which they may select an approach more appropriate for their organization.

Acknowledgement

I would like to gratefully acknowledge and thank my academic advisor Shari Plantzmaster and my instructors Henry Tshibambe, Dee Bilo, Paul Vieira, Eric Welch, Erik Moore, Mike Nims, Douglas Hart, Donald Archer, John Wessels and Don Archer for their help, direction and master tutor ledge during this journey.

And last, but not least, I wish to thank wholeheartedly my family for their support and patience though this lengthy but rewarding process.

Table of Contents

Introduction

The Problem

The business of the new millennium is, inundated daily, with a barrage of attacks – externally, internally, domestically and from abroad. Avoiding, mitigating and recovering from these assaults are a constant in business. How successful an entity is in thwarting such assailant's lies in its ability to identify, categorize, locate and assess the vulnerability of each of its assets and to safeguard and secure them.

Failure to discern and manage threats to assets places an organization at a decided disadvantage as the defense of its databases; systems, confidential records and intellectual property are of utmost importance to the business process and in particular to organizational survival. Ongoing risk assessment is a must in the quest to deliver enterprise wide protection. Determining what is to be defended, how it is to be guarded, and the scope of the security, is a major consideration.

Thesis Statement

The application of a security-centric technology program enables a business or organization to identify and secure its information assets, shore up vulnerabilities, and establish buttresses against potential threats and the likelihood of an impending event.

The Project Need

Identifing and mitigating security risks has been, for eons, a basic business tenet. In fact, this aspect of business has always factored into the price of goods and services. Yet, in years prior, IT assets were seen either as investments or items for appreciation or depreciation on the balance sheet. The development of the global market changed this. Hard and soft IT assets have become integral to the decision making process. Therefore, protecting these assets allow an organization to ensure the reliability and integrity of the data they rely on to make decisions.

“Unfortunately, today’s small business owner faces big risks every day”. More than ever before they must consider

“…what sort of new risks has technology introduced into the world of small business…imagine if a server fails…or if a hacker steals customer’s personal account information…or if a virus infects the entire network”. Small business must able to contend with the damage, the cost of repairs and recovery, the ramifications of a blemished reputation and prepare for the possibility that “business would be down while the problem was fixed” (The Hardford Group, 2008) .

Research Focus

Chapter 1

Chapter 1 consists of the acknowledgement, abstract, problem statement, the thesis statement and project need. Also included, are the Research Focus, Project Limitations and Scope of Project.

Chapter 2

This chapter contains a review literature and research related to the work past and present.

Chapter 3

This chapter will cover project research, planning and methodology.

Chapter 4

This chapter contains the project overview.

Chapter 5

This chapter will consist of a summary, discussion and recommendation.

Project Limitations

Ascertaining risk and implementing IT security protocols within an organization is not an exact science. An organization must analyze, access and evaluate threats and vulnerabilities encountered by businesses, in general and also those peculiar to their organizations. This work suggests using a layered methodology. One cannot say that this approach is superior to another or whether or not it should be combined with others approaches for the correct solution.

Scope of Project

The purpose of this paper is to acquaint small business with the concept of security-centric technology and to give advice on a group of security components that when utilized collaboratively yield a formidable bulwark against a variety of threats that can negatively impact business.

It is expected that this effort will offer a practical, working understanding of Security-Centric technology, support

small business in the selection of a suitable line of defense and present an easy to follow checklist for successfully implementation.

Literature and Research

The function of a security-centric defense program is to assist management in the development of effective and appropriate stratagems and controls for the stewardship of the organization's information assets. Armed with the tactics for a layered defense, an organization is able to expand security applications and/or defenses to perform in synchronicity. Instituting IT security in such a fashion allows a business entity to repel attacks that originate from a range of sources.

The following literary review support and validate the research.

The literature assembled in support of this project has been collected from professional journals, book publications, and organization websites, and technical white papers related to the subject matter.

System security is not *just* an IT issue it is a business wide concern. Protecting and securing a network is an enterprise wide endeavor from senior management to the

“lowly” mailroom clerk. For this reason, the approach must be proactive, assertive and relentless beginning with an assessment to evaluate and categorize risks. Shortcomings of any kind, in this regard, either by a deficiency in IT security or by users, can compromise company systems. Vigilance combined with the application of strategic security tools, and an adherence to the company’s security policy, is one of the best mechanisms for thwarting determined attacks. The first step, however, begins with assessment, as it is an essential component of any system security (McNab, 2004).

Network Security centers around three basic tenets: confidentiality, reliability and accessibility. The confidentiality aspect is tasked with preventing unauthorized access to sensitive data either inadvertent or intentionally. The reliability component prohibits the modification of data by unauthorized persons or entities. Assuring data consistency is a primary consideration. Accessibility ensures that vetted users are able to connect to resources in a timely manner. These three principles work in sync. The lack of any one of these key

principles signals a serious defenselessness in the security design (Cole, 2005).

Corporate communication is all about connections, connecting people, places and resources. Hence, organizational resources are only as secure as the machines and/or devices to which it connects. A single unprotected or vulnerable node or host can unwittingly serve as a conduit of reconnaissance or function as a point of attack. It is for this reason that IT security must be viewed as a journey and not a destination. As technology innovates, upgrades and evolves so does the tools, techniques, strategies, and methods used by attackers. Thus those charged with the protection of corporate systems have to learn to be adaptive, proactive and reactive as security is always in a constant state of evolution (Lockhart, 2006).

Implementing wireless security solutions is tricky. The path is littered with pitfalls; rough patches and yet when configured successfully it can be, hands down, a formidable business enabler. Therefore, it is absolutely essential to have a good understanding of all of the components that constitute the organization's network i.e. hardware, software and, in

particular, the networking protocols. Such knowledge will prove invaluable when navigating and configuring the network cloud interconnecting and securing the network, client devices and servers (Geier, 2008).

Organizations that venture into the global theater soon discover that they are immerged in an intensely competitive environment demanding innovation, creativity and rapid deployment. Some call this progress as they rush to employ new technologies and services to keep pace. Often this leaves little time to test and implement protective mechanisms. As a result safeguards are applied *a posteriori*. This leads to a network comprised of a series of security patches. The consequence of this is an unyielding and complex system. Complications of this sort generally lead to impediments that prove detrimental. With this in mind, it is important to note the traits that characterize secure systems: authentication, access control, confidentiality, integrity, privacy, non-repudiation and availability (Buttyan, 2008).

In the new millennium IT is tasked with overcoming security challenges set in diverse and disparate scenarios. The business theater is now an international marketplace and the workforce is global, mobile and always connected. IT security professionals of today are challenged to engage security mechanisms that ensure trusted on-going communication anytime and every time. The global marketplace of the 21st century demands accessibility 24/7 without the tethers of yesteryear (Zhang, 2008).

The world has changed drastically. Hackers of all stripes (spammers, saboteurs, phishermen, virus writers and other no- accounts) now all associate unabashedly in an online economy, within the confines of this medium and affiliation they (criminals and ne'er-do-wells) survive and evolve. Hence, the need for the discipline of security engineering.

The science of security engineering offers a developing and deploying system that is dependable and agile enough to remain reliable even in the face of malice, terror, error and/or happenstance.

It has been said that while software engineering is about setting things in motion or making things happen, security engineering is concerned about making sure they don't. Security engineering at its best requires several aspects to come together. Thus good protection relies on the following processes: (a) policy, (b) the tools used to implement the policy, (c) assurance, (d) and the motives of the system's guardians and attackers as all of these interact (Anderson, 2008).

Consider carefully the employees who access the network daily to perform various tasks in the execution of their duties. While they are not the enemy so to speak they are certainly not friends and as such they must be treated accordingly. Limits should be set to establish boundaries in regard to what employees can and cannot do on the network – accidentally or intentionally. Security is more about a healthy balance between paranoia and practicality. The operative word for security is mitigation and not elimination. No one can eliminate risk and still do business (Dubbin, 2008).

The IT infrastructure has now, without question, become an intricate component of the business model of the new millennium. The nature of the relationship between IT and the business prime necessitate a new kind of IT risk assessment. The IT risk assessment of today must be lightweight and supple allowing for a more comprehensive understanding of the interdependencies of risk in a complex and ever-changing environment.

Just as risk assessment has broadened so has its constituency. Today's IT risk assessment constituency must include all of the organizational stakeholders is the appraisal is going to deliver a true benefit. IT risk assessment of the new millennium is designed not only to be in keeping with the corporate mission, to meet the needs of its varied and distinct stakeholders, but also to comply with the rules and regulations of a number of corporate governing bodies. All of these assorted drivers greatly impact the type of risk assessment carried out, and the skills and tools required to get the job done (Jones, 2005).

One of the central themes of Information Security is access control. “ Generally, an access control is any hardware, software, organizational administrative policy or procedure that grants or restricts access, monitors and records attempts to access, identifies users attempting to access, and determines whether access is authorized. Access controls provide protection for the confidentiality, integrity and the availability of corporate assets. The area of access control is divided into two categories function and purpose (Stewart, 2004).

Koller’s research exposed several misconceptions about risk assessment that poised a threat to its successful implementation. The first was that outsiders, and indeed many insiders, looked upon the corporation as a single unified body when in actuality these organizations were more of a compilation of competing and relatively autonomous components. And, in regards, to risk and uncertainty each unit had a differing view and practice. Some were even diametrically opposed in their views, practices and approaches

to risk and uncertainty. Koller's breakthrough book serves as a no-nonsense guide to applying risk assessment in a real-world business environment (Koller, 2005).

Recommendations for Applying Security-Centric Technology

Utilizing A Layered Approach in the Era of Ubiquitous Computing

(A Guide for the Small Business Enterprise)

A well-defined security methodology entails considerably more than the installation of a few security devices. It requires a detailed, systematic and strategic approach involving the marriage of a multitude of instruments, security tactics, plans and policies all working in concert to defeat assailants that often attack in coordinated fashion.

It is important to note that no single security device, system or even approach is in itself infallible nor can it be expected to be. This is not to say that all is lost. It is instead to say that successful security systems adopt a layered approach involving an assemblage of components working in unison to afford protection against a myriad of threats through these multiple layers defense is provided in-depth.

Based on the concept of concentric circles, protection is achieved by enclosing assets and resources within logical circles of security protections. Assets are shielded by administrative access controls, which are in turn encased within logical and/or technical controls, and which are further encircled by physical access controls.

This treatise will discuss applying security-centric technology in a layered approach as its preferred methodology. This approach will involve the physical security of systems, access security, the safeguarding of operating systems, the application of viral defense tools and mechanisms, the monitoring and filtering of data packets, erecting firewalls, the skillful use of proxy servers to conceal software and data, the operation of DMZs, incorporating IDS, VPNs and effectively employing logging and administration.

Access Security Controls
(Establishing "Right of Entry")

Access Security Controls

It has oft been said that the best defense is a good offense and nowhere, bar none, has this old adage been truer. It has always been easier, and indeed better in the long run, to introduce measures to repel an invading horde rather than try to collect and marshal forces to dispatch them once the barriers have been breached. Therefore a substantial amount of time and effort must be devoted to preventing and constricting access to corporate systems.

Restricting and controlling access to organizational resources is a major theme of security. The underlying rule of access control is to refuse access by default if “right to use” is not granted specifically to a user and/or entity. Access controls are essential to secure the confidentiality, integrity and the availability of organizational assets and data. Access controls focus on limiting files and corporate services users may gain entry to.

There are seven crucial categories of access controls with an additional three involving implementation. The access controls are as follows: preventative, deterrent, detective,

corrective, recovery, compensation, and directive. Categories of implementation include administrative, logical/technical and physical.

Preventative access controls are designed to prevent unwelcome or unauthorized action from transpiring. The use of guards, biometrics, and security cameras are a few examples of the tools used to deny unsanctioned access. Deterrent access controls persuade against the abuse of security policies. The use of encrypted transmissions, intrusion alarms, and electronic locks are illustrations of deterrents in action.

Detective access controls, on the other hand, are employed to reveal unwanted or ascertain unauthorized occurrences. Surveillance and recording devices, audit trails, and sentry details are all tactics used to detect anomalies and braches. Corrective access controls such as patches, hot fixes, and software updates and IDS systems are instituted to restore systems after prohibited activity.

The use of recovery access controls help to mend or restore resources, operations, and facilities after a breach in policy. Fault tolerance, mirrored systems, and automated

backup services are representative of the many elements brought into the job of a recovery.

Compensation access controls are deployed to grant alternatives to other controls in regards to the prosecution and re-enforcement of organizational security policies. Updating security guidelines, increasing staff supervision, and monitoring are typical of these kinds of controls.

Directive access controls are intended to instruct, curb or control the activities of users or entities in an effort to compel or promote compliance with business security policies, the usage of security policies, official written notifications, and awareness training are a few of the techniques engaged here.

Other access controls such as administrative, logical/technical, and physical access controls are characterized by the method by which they are implemented. Administrative controls are the rules and regulations established within the organization's security policy to enforce institution wide access controls. Administrative controls are characterized by the use of background checks, data

verification, security inspections and human resource practices.

The hardware and/or software tools by which IT systems are managed, maintained and safeguarded represent the logical and technical access controls. Such controls are represented by restrictive interfaces, firewalls, router, smart cards and passwords. Passwords, it must be noted, are part of the main shield when providing a secure environment for the information we protect, which is stored within the computer. Organizations do not stress this enough and this fact is known by intruders and is always used to their advantage (Magalhaes, 2004).

Physical Access controls are corporeal defenses engaged to stave off direct contact with business resources, systems or facilities. The central theme of physical access control is to prevent and/or restrict access to corporate resources or assets by entities or persons known or unknown lacking authorization.

The chart below describes the access controls discussed along with examples of their application.

Access Control	Tools/Techniques or Strategies
Preventive	Walls/fences/gates, canine patrols, guards, biometrics, mantraps, lighting, alarms, encryption, auditing, monitoring, smart cards, ID badges, security cameras, penetration testing, security policies and more.
Deterrent	Electronic locks, security guards, security and ID badges, separation of duties, mantraps, cameras, intrusion alarms, encryption, auditing, security training for users, and etc.
Detective	Job rotation, compulsory vacations, security details, guard dogs, motion detection devices, surveillance and recording systems, audit trails, IDS systems, violation reports, incident investigations, regulation and review of users for example.

Access Controls	Tools/Techniques & Strategies
Corrective	IDS systems, Anti-virus/spy ware and Spam solutions, System patches/fixes, system alerts, mantraps, recovery plans, security policies and procedures for instance.
Recovery	Server clustering, server mirroring, backups, restores, and fault tolerance, etc.
Compensation	Security guidelines, staff supervision, monitoring and work task procedures.
Directive	Awareness training, Security policies, guards, canine patrols, exit signs, written notifications, monitoring, supervision and more….
Administrative	Background checks, security policies, security procedures, human resource practices, hiring practices, data verification, supervision, reviews, testing and additional administrative checks and balances.

Access Control	Tools/Techniques or Strategies
Logical/Technical	Encryption, smart cards, passwords, restrictive interfaces, authentication, biometrics, firewalls, routers and IDS systems.
Physical	Fences, guards, motion detection devices, secured doors and entrances, cable protection, swipe cards, lights, mantraps, alarm systems, security cameras, and canine patrols.

Access controls restricting, deterring and denying admission form the foundation of a good security methodology.

Physical Security

(Preventing Intruders and Theft)

The first layer of defense is ample physical security. The physical protection of corporate systems and resources from acts of theft, unauthorized access (internal or external), vandalism or abuse is essential. The basic goal of the physical layer is one of prevention, the elimination or the substantial reduction of events that promote or aid unsanctioned access to corporate technical property. Such precautions safeguard vital technical equipment, organizational resources and, indeed, the infrastructure itself from unwanted attention by either employing constraints or a combination of detection, delay, and response.

To some, the application of physical deterrents may seem obvious, in actuality; it is infrequently practiced to any appreciable degree. Physical security is all too often relegated to a secondary position as organizations focus the bulk of their efforts and expenditures on minimizing electronic intrusions from the Internet. Though most assuredly a necessity, the physical security and welfare of technical assets is of equal value. Sadly, it is only after the experience of a physical

breach that many companies began to understand and acknowledge how such deficiencies truly impact their organizations.

Individuals who have physical access can not only steal a PC or confidential data but can also compromise network security… Combining various types of access controls is the only means by which a reasonably secure environment can be developed (Mehdizadeh, 2004). Statistically, more attacks occur through poorly defended physical barriers i.e. via social engineering, impersonation, insufficiently monitored or in-secured assets than any other means.

It must be noted, that the successful control of physical access to a company's resources actually involves the marriage of logical and physical asset restraints. In this section, however, we will concentrate only on the physical constraints. Physical access controls may involve the use of biometrics, physical barriers, security guards, canine patrols, Smart cards, ID cards and badges, locking mechanisms, electronic monitoring, alarm systems, and more.

Biometrics allow organizations to prevent or restrict entry of access by using a person's physical traits or characteristics to determine if they are authorized to access the medium or not. Biometrics technology may be based on the following identifying features: fingerprints, facial features, hand and/or palm prints, iris, retina or voice scans. Because the human body is a living organism and subject to change there are some inherent weaknesses that must be acknowledge in the use of biometrics. Nevertheless, biometrics can be quite an effective tool for authentication and controlling right of entry especially when used in collaboration with other security mechanisms.

Physical barriers are one of the oldest and most dependable means of preventing unauthorized entry. Physical barriers may include walls, fences and/or gates. The scope and sophistication of each of these devices depends primarily on what is to be protected and the level of security needed by the organization. Walls, fences and gates offer both a subtle and compelling form of prevention.

Security Guards are yet another component of the “physical” barrier. Unlike walls, fences and/or gates, human guards are dynamic having the capacity for human reasoning. Human assets offer a different level of security as they have the ability to access and evaluate a changing security landscape and respond immediately and accordingly without requiring additional programming.

Canine assets provide an additional layer of precautions when securing valuable property. Used in conjunction with human assets or alone they can be integrated quite seamlessly into the umbrella of technology tools and strategies. Canine assets provide the added benefit of superior sight and hearing and often can work and function in areas where human assets cannot.

Smart cards/ ID Badges offer an added measure of physical control by visually validating and authenticating the bearing of the card or badge while the magnetic strip or chip embedded within the card/badge present additional information on the user with details about the scope and type of access allowed.

For the high security facilities there are mantraps. Mantraps provide yet another layer of physical security in that an individual wanting access must pass through this area and respond to a set of security protocols. If the protocols are satisfied, access is granted if failed, the person denied is trapped to await a security detail.

Physical Security Controls		
	Control	**Function**
	**Barriers**	Gates, Fences or Walls
	**Biometrics**	Eye scans, fingerprints, Voice or Signature recognition
	**Security Guards**	Manned patrols
	**Canine Patrols**	Canine assets can be deployed alone or partnered with a Security Guards
	**Smart cards**	Electronic badges with authorization encoded on a magnetic strip on back of card

Physical Security Controls		
	Controls	**Function**
	**ID Badge**	Badges with pictures indicate granted right of access
	**Surveillance Cameras**	Security cameras look for unauthorized persons or activity
	**Mantraps**	Another security station to authenticate those wanting right of entry
	**Electronic Locks**	Electronic locks offer a myriad of options beyond the traditional “lock & key”
	**Motion Detection**	Connected to other alarm system give out warnings of intruders
	**Thermal Detection**	Connected to other alarm system give out warnings of changes in temperature that could signal fire or intrusion

Environmental Security Controls

(Warding off Natural Disasters, Fire & Flood)

Environmental Security Controls

Another major interest in the ongoing challenge to secure and safeguard information assets is the security of the working and operational environment for human and non-human assets. Too often this aspect of IT security has been relegated to maintenance and/or facilities departments. While they are quite proficient at maintaining the comfort of human assets most are not familiar with the needs and idiosyncrasies of information systems nor the hardware and software that protect them.

It is important to support utilities, such as heating, ventilation and air conditioning, power, water and other utilities, as they have a significant impact on the continued safe operation of a facility. Extreme temperatures, elevated humidity levels, electrical fluctuations and the interruptions of water, sewage, and garbage services can create conditions that inject vulnerabilities into systems designed to protect information. Thus, each of these utilities must be properly

managed in order to prevent potential damage to information and information systems (Whitman, 2005).

It must be stated that while all computer systems, information assets and their related devices and resources should be shielded from harmful environmental agents it is particularly so for those assets designated as “mission critical”. Consequently, we will focus mainly on the mission critical assets though non-critical assets may also benefit.

Most organizations do not fully realize the importance of location in terms of protecting their mission critical assets. Too often businesses think physical security and environmental security are one in the same when the two are quite distinct. Still environmental hazards can be just as disrupting if not, disastrous to business’ operations. For this reason the following factors should be considered in the placement and location of the mission critical assets.

Whenever possible, organizations should avoid locating “Mission Critical” assets in areas prone to natural disasters such as fire, flood, earthquake, lightening, landslides/mudslides, tornado or severe windstorms,

hurricanes, typhoons, or tsunami's. These ferocious acts of nature are almost always followed by terrible damage and/or severe interruptions to operations and service. Where economically feasible, it is best to locate critical informational assets elsewhere.

Man-made works can also carry their own set of risks and thus require careful consideration when locating crucial assets within their jurisdiction. Airports, expressways, penal complexes, refineries, pipelines are example of man-made works which by virtue of their existence and use bring increased incident and risk factors. Prudence demands the avoidance of such locales when reasonably possible. The control objective at play in avoiding geographical locales of high risk is to mitigate or significantly reduce the probability of threats based on proximity or acts of nature.

The risk of fire is a reality no matter where "mission critical" assets are stationed. Because of this it is much better to adopt a stance of prevention. Flammable materials of all kinds must be banned from areas that house vital equipment and resources. Note: smoking especially should be disallowed

on or around the premises. Fire protection systems are essential and should be installed and rigorously maintained by certified professionals. Often overlooked but just as important in fire prevention is the use of non-flammable or self-extinguishing furnishings including furniture, wall coverings, window coverings, fixtures and more. While non-flammable products may carry a slightly higher price than conventional alternatives they are, in the long term, a sensible and warranted investment.

Rooms housing “mission critical” resources require fire doors with ceiling and walls constructed of materials with the capacity to withstand and contain flames for several hours. Doorframes, walls, floors and ceiling must be properly seated and sealed with fire stop sealants where appropriate. Hand-held fire extinguishers specially rated for electrical fires should be at the ready and in reach of designated personnel. In addition policies and procedures for dealing with fires of all types should be clearly displayed along with graphics in the vicinity. It is important to state that the prevailing goal here

for all of these preventive measures is to limit the probability of damage caused by fire and smoke.

Like fire, flooding can be just as damaging and affect business continuity. Properly sealing roofs, doors and other perimeters is of immense importance in the effort to safeguard against the affects of water damage. Installing water leakage detectors and sump pumps is yet another way to ward off harm caused by flooding, leakage or moisture. Additionally, it is important to ensure the accessible positioning of emergency stop valves.

Technology runs on power in particular electrical power and it is for this reason that it is absolutely essential that all assets especially “mission critical” ones have contact with reliable power sources. Insufficient capacity more often than not leads to fire and destruction while overloading goes in front of brownouts, spikes and sudden failure, both of which are quite disruptive to business operations. For best results having multiple power sources in such locations to balance the demands can improve power quality and lessen the possibility of deficiencies or overloading. Monitoring amperage, voltage,

frequency, spikes and noise is another key component in guaranteeing a continued and uninterrupted supply of power. Lastly placing emergency on and off switches in access-controlled locations is a must. There should also be a system of annual maintenance and testing of all power systems to ensure reliability. For smooth operations and business continuity the goal is to secure clean and reliable sources of power to all resources but in particular “mission critical” assets.

Technical resources generate heat. Heat is unwelcome and potentially harmful to systems. Hence, the need for air conditioning units the scope and size of which are peculiar to the systems they are cooling, the organization and more.

Installing air-conditioning units allow critical corporate technical equipment reside in conditions as prescribed by the manufacturers. Systems design to monitor heat and humidity can be linked to air conditioning units and programmed to go into operation based on alerts from temperature alarm systems. The intention, of course, is to both monitor and

sustain acceptable temperature and humidity levels conducive to an optimum working and functioning environment.

It must be noted here that the business continuity of vital corporate resources and assets is also dependent on the quality and reliability of environmental controls, conditions and safeguards. The requirements for power, physical access controls, etc. may be broadly similar but the impact of security failures are generally much less, therefore lesser controls are usually appropriate…it is advisable to assess the risks in your specific situation to determine the appropriate security requirement. Furthermore, the risks vary over time; meaning that security should be reviewed periodically to make sure that it remains sufficient to the need (Noticeboard, 2004).

The chart below lists environmental threats to avoid.

Environmental Security Threats		
Avoid	***Areas prone to***	***Results***
☛	Natural Disasters	Fire, flood, earthquake, lightening, landslides/mudslides, tornado or severe windstorms, hurricanes, typhoons, or tsunami's
☛	High Risk Man Made Works or Facilities	Airports, expressways, penal complexes, refineries, pipelines
☛	Fire threats	Smoking, Flammable, or combustible materials
☛	Flooding and excessive water	Flooding, leakage and moisture
☛	Insufficient electrical capacity	Spikes, brownouts, power failure, and fires
☛	Single power sources	Overloading, disruption, or power outage
☛	Excessive heat	Loss of power, increased humidity

The table below illustrates a checklist for environmental security best practices.

Environmental Security Best Practices		
Do	***What***	***How***
☑	Centralize, monitor and guard	Mission critical servers, routers, switches, and data centers
☑	Secure equipment and facilities	Use smart cards and biometrics
☑	Mitigate fire threats install and maintain fire protection systems	Use of non-flammable or self-extinguishing furnishings including furniture, wall coverings, window coverings, fixtures
☑	Ward off flooding, leakage or moisture build up	Install water leakage detectors and sump pumps
☑	Improve power quality and lessen deficiencies	Monitoring amperage, voltage, frequency, spikes and noise
☑	Multiply power sources	Overloading, disruption, or power outage
☑	Control heat	Install UPS systems appropriate for the environment

Strengthening Information Assets

(also known as hardening)

Hardening Operating Systems, Applications, and More

Attacks on information assets are of such a frequent nature that they are no longer considered out of the ordinary but rather a common workplace occurrence. Thus, an organization' s should adopt the stance and philosophy of preparing for the worse and when, instead of if. …Preparing for the worse involves establishing a security baseline of defense. Then you are ready to withstand and recover from an attack (Ciampa, 2005). The process by which a business diminishes its vulnerability is known as hardening. Hardening informational assets provide organizations with another layer of security by which it can shore up its defenses.

It is important to note that even before beginning the process of hardening operating systems that non-essential systems and services must be identified and disabled. Doing so greatly reduces, if not, eliminates the number of entry points or vulnerabilities by which an invader and/or hacker may gain access to exploit corporate resources or move against organizational systems.

The hardening of operating systems and software applications entails two main activities (a) applying the latest updates such as service packs, hot fixes, patches and/or software updates to repair security defects and other issues, and (b) the prohibition of unauthorized access thus safeguarding data stored on all systems.

Below is a brief checklist of the primary tasks that constitute the hardening of operating systems and applications.

Hardening Operating Systems and Applications	
✓	Applying the latest updates of service packs
✓	Applying the latest updates of hot fixes
✓	Applying the latest updates of patches
✓	Applying the latest software updates
✓	Limiting system access by unauthorized users

Strengthening (Hardening) Servers

Sometimes, despite best efforts, determined and enterprising hackers may still challenge corporate resources. It is for this reason that another layer of security is employed - that of hardening servers.

Hackers who replace legitimate content and images with their own often molest web servers. In addition web servers that support e-commerce functions are often raided for their credit card members and user information. Thus hardening is essential to prevent the occurrence and or frequency of such events. Hardening web servers involves isolation from internal networks, restricting browsing and navigation rights by users, eliminating common gateway interfaces, deleting unused scripts, frequently administering patches, fixes, and updates, and deleting sample files which accompany the web server's installation.

The table below lists some of the major tasks that must be performed before a web server may be considered hardened and thus secure from harm.

Hardening the Web Server	
✓	Isolate from internal networks
✓	Restrict browsing and navigation by users
✓	Eliminate common gateway interfaces
✓	Delete unused scripts
✓	Frequently administered patches, fixes, and updates
✓	Deleting sample files which accompanied the web server's installation

Strengthening (Hardening) Mail Servers

Mail servers are often victimized via a process known as open relay. During an open relay a mail server may be conscripted to process e-mail that is neither sent to nor intended for the local user. E-mail messages are, in essence, bounced from one outside unrelated source to another all without the knowledge of the local user.

Hardening the mail server requires two tasks (1) the elimination of all applications except for those related to the mail server, (2) configuring the mail server to disallow open mail relays, and (3) encrypting messages when possible.

The chart below depicts the basic components of the hardening process as it relates to mail servers.

Hardening Mail Servers	
✓	The elimination of all applications except for those related to the mail server be stricken from the server
✓	Configuring the mail server to disallow open mail relays
✓	Encrypting message transmissions
✓	The regular application of patches, hot fixes and software packs

Strengthening (Hardening) FTP Servers

Hardening the FTP server is a must since it can be re-configured to permit unsanctioned users to transmit documents and/or files in a manner known as a “blind FTP”.

The hardening of an FTP server necessitates the disabling of anonymous logons, permitting only approved IP addresses, restricting the number of log on attempts and configuring the ACL to read only for the FTP server which allows downloads.

Charted below are the major steps that constitute the hardening of FTP servers.

Hardening FTP Servers	
✓	Disabling of anonymous logons
✓	Permitting only approved IP addresses, restricting the number of log on attempts
✓	Configuring the ACL to read only for the FTP server which allows downloads
✓	The regular application of patches, hot fixes and software packs

Strengthening (Hardening) the NNTP Server

NNTP servers by their very function i.e. that of broadcasting to every site (within their scope) makes for a rather attractive target for a would be hacker. By commandeering this server a hacker could send malicious and/or damaging communication to all of its members. Hardening significantly reduces this risk.

Hardening this server consists of (a) the regular application of patches and software packs and (b) establishing the ACL with the appropriate permissions.

The table below charts the steps needed to harden NNTP servers.

Hardening NNTP Servers	
✓	The regular application of patches, hot fixes and software updates
✓	Establishing the ACL with the appropriate permissions

Strengthening (Hardening) the Print and File Server

Print and File servers present an especially juicy target for an assailant as a breach provides an opening to access files stores on these assets.

Hardening the print and file server includes limiting the "right to use" resources on these machines to only trusted users, restricting users to opening only the services for which they are approved thus allowing users ready access to just their files, folders and/or shared folders for which permissions have been granted.

The table below offers a guide for hardening print/file servers.

Hardening Print and File Servers	
✓	Limiting resources only to trusted users
✓	Restricting users only to files, folders and resources for which they have been cleared
✓	Allowing users ready access to files/folders and shared spaces for which permissions have been granted
✓	Regularly scheduled application of patches, hot fixes and software updates

Strengthening (Hardening) DHCP Servers

A compromised DHCP server lays bare an entire network offering an assailant a cornucopia of options ready for exploitation as breaches within this server provide an attacker with the ability to run damaging code and/or programs with the highest level of privilege. The successful invasion of this server can offer a hacker complete control over company systems as it literally and figuratively hands over the "keys to the kingdom". Enterprise security demands the protection of this server physically and logically. Applying vendor prescribed updates, patches, service packs and hot fixes as well as physically prohibiting access to the server itself can diminish security flaws within this server.

The checklist below offers a handy template for hardening DHCP servers.

Hardening DHCP Servers	
✓	Limiting administrative rights to trusted personnel
✓	Regularly scheduled application of patches, hot fixes and software updates
✓	Physically protecting server from unauthorized access externally and internally

Strengthening (Hardening) Data Warehouses

Company data warehouses generally consist of directory services and corporate database. Residing within these repositories is information about network users, the network, its configuration and associated devices and information on privileges to resources. Also located within the confines of these storehouses are customer records, corporate financial details, confidential documents and more all of which provide attackers with an appealing target. A successful assault on this server would provide an assailant with ability to manipulate the data within, how it is deposited, and where it is stored effectively compromising the integrity of the data.

Hardening a data warehouse requires a good measure of planning to determine who should access these resources, the scope of the access and the type of access all of which are necessary to ensure that the permissions are granted only to the proper personnel.

Defending Against Stealth Invaders

(Viruses, Trojans, Worms, Spyware, and etc.)

Cyber criminals have a veritable smorgasboard of stealth weaponry at their command. The level of sophistication, the wealth of technology, and the sheer volume of what is available to these miscreants is quite staggering.

The US government alone reports upwards to 3 million attacks daily. Hence it is encumbent upon organizations, the world over, to be cognizant of these threats and the popular avenues of attack.

In order to defend against and remedy the effects of a host of viruses and bugs, organizations must employ frequent applications of anti-virus scan and spyware protection software to innoculate computing and network systems. Despite thes best efforts, without the complement of regular employee training in security and computer usage all of this is for naught.

The following chart lists some basic computer attack strategies, a brief look at how they work, and solutions and/or defenses against them.

A Compendium of Common Attacks		
Attack	**How it Works**	**Solution**
Social Engineering	Uses subterfuge and deception to gain access to resources	Employee education and strong policies regarding passwords and right of entry
Password Guessing	Try different password combination	Lock system or account after three unsuccessful tries
Dictionary	Uses words from the dictionary and hashes it in the same fashion the system encodes passwords	Passwords should expire frequently, must be at least 8 characters and include both letters and numbers
Software Exploitation	Searches for vulnerabilities in software to circumvent security	Apply vendor recommended updates and service packs
Mathematical Attacks	Analyzes encrypted text and uses statistical dissection to defeat and decrypt data	Do not send the same encrypted data more than once
Man-in-the-middle	Intercepts, manipulates data that redirects communication	Prohibit network devices from forwarding anything redirected
Spoofing Attack	Poses as a valid device on the system fooling users into sending messages to them	Difficult to defend against

A Compendium of Common Attacks		
Attacks	**How It Works**	**Solution**
Smurf Attack	A request is sent to all computers on the network the resulting response from all of the systems on the network overwhelms and crashes the server	Access system on a management channel not directly linked to those systems
Viruses	Attaches to a file or program and activates (for malicious purpose) when it is opened	Use Anti-Virus Software
Worms	Distributed by e-mails or executable programs	Do not open programs transmitted by e-mail, avoid downloading anything from unfamiliar internet sites, apply all vendor prescribed patches, updates and hotfixes
Logic Bombs	Malicious code buried a computer program until activated by an event, date and or scenario	Difficult to defend against. Apply updates, monitor network and employees

A Compendium of Common Attacks		
Attacks	**How It Works**	**Solution**
Trojan Horse	Combine one or more malicious programs under familiar filenames for criminal purpose.	Implement Anti-Virus tools, and Anti-Trojan software, other third party software designed to detect trojans
Backdoor	An alternative means of accessing the network by-passing security. Note: usually created by testing teams.	Erase the backdoor once system is tested. Also use software designed to scan for, listen for and locate these programs

Securing the Network Perimeter (Packet Filtering)

In many ways packet filtering can been seen as the first line of defense. If not the first, it is most certainly the simplest. Packet filtering allows an organization to govern, restrict or manage all of the activities done in house and on the internet.

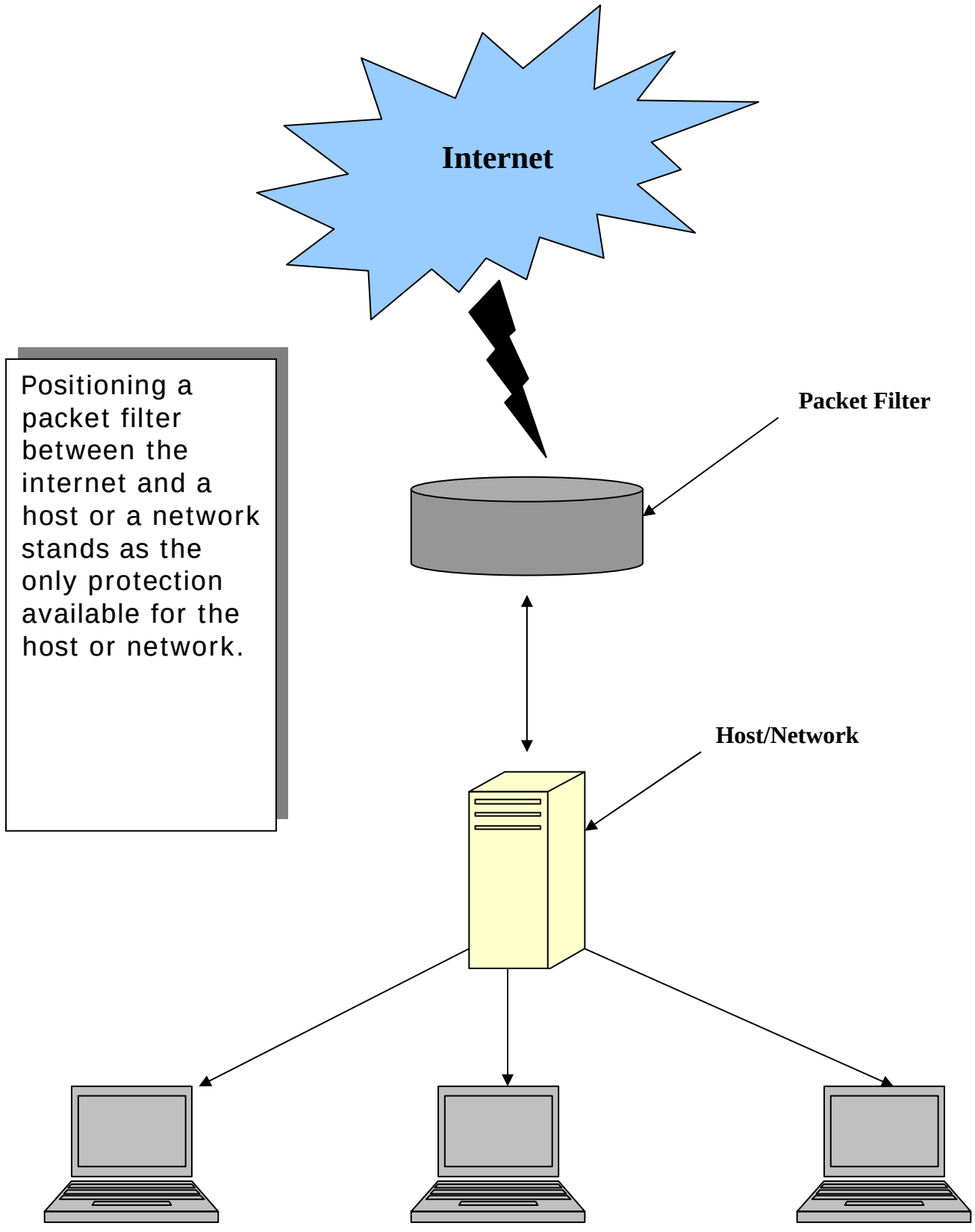
Instituting packet filtering offers a network an additional layer of security by securing its perimeter. Widely used, packet filtering controls network access. Packet filters decide whether or not to allow packets to travel to and fro within a network based on information included in its packet header. Utilizing filtering provides the network with the added ability to tailor incoming traffic and to vett outgoing traffic.

Packet filters can be used in conjunction with other firewalls as a layer of an intricate defense-in depth posture or as a standalone solution in lower-risk areas or where budgets are tight. After all, protection of information is a balancing act between the value of the data and the cost to protect it. Packet-filtering technology can be a useful means to protect

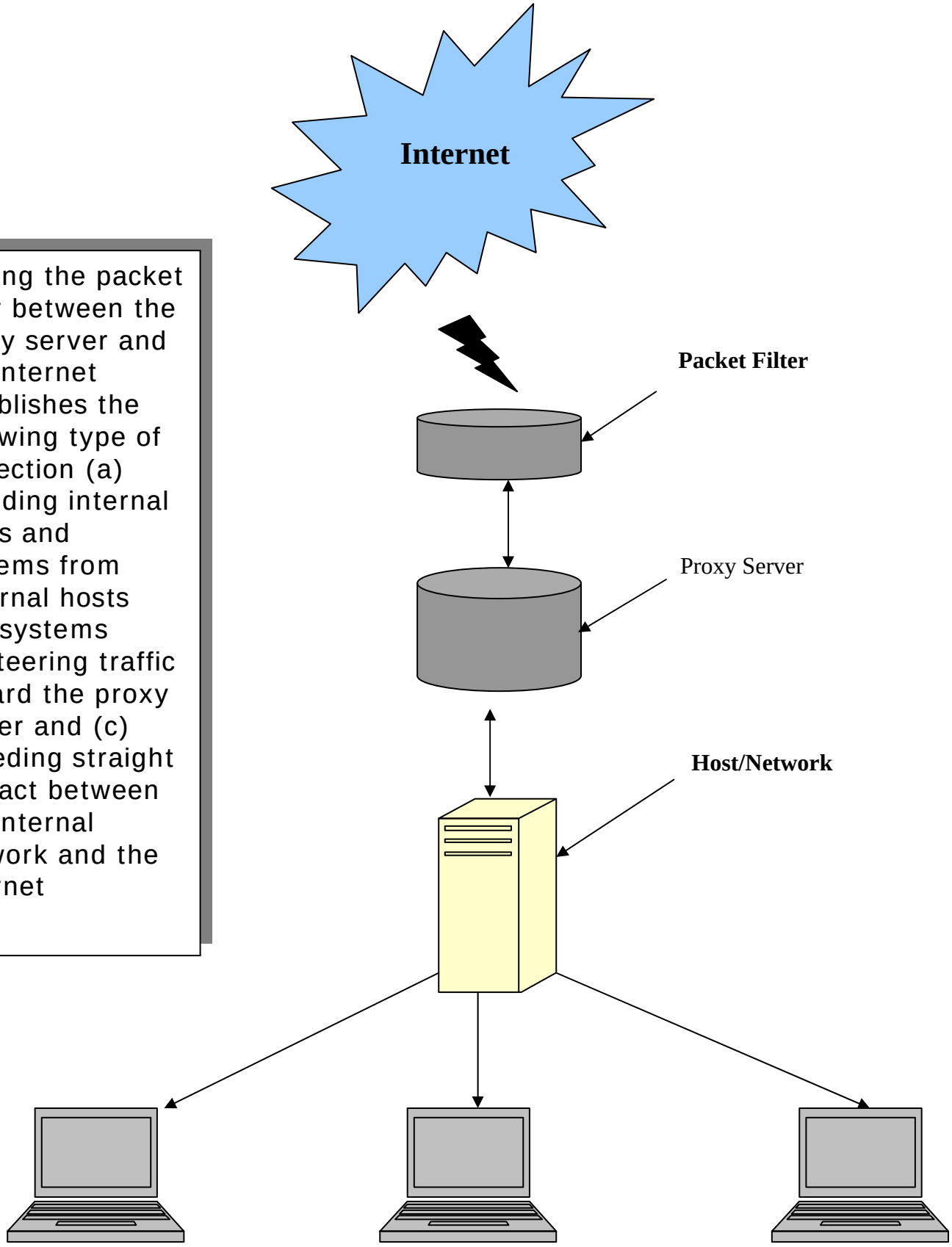
your network as long as you implement it with due consideration to its strengths and weaknesses (Zeltser, 2005).

However, the type of filtering done by a packet filter ultimately hinges on its placement in the configuration of the perimeter. Configuation here is critical as all inbound and outgoing traffic has to be scrutinized by this filterer. Placing the packet filter between the proxy server and the internet establishes the following type of protection (a) shielding internal users and systems from external hosts and systems (b)steering traffic toward the proxy server and (c) impeding straight contact between the internal network and the internet.

The chart on the next page illustrates how the positioning of the packet filter affects the type and scope of protection afforded the network.


Internet
Positioning a packet filter between the internet and a host or a network stands as the only protection available for the host or network.
Packet Filter
Host/Network

Placing the packet filter between the proxy server and the internet establishes the following type of protection (a) shielding internal users and systems from external hosts and systems (b)steering traffic toward the proxy server and (c) impeding straight contact between the internal network and the internet



Building the Bulwark Against the Digital Horde (Firewalls)

The purpose of the firewall is to ward off attacks from the Internet and from countless external networks. In practice however firewalls filter packets from external sources, aid in concealing IP addresses, and in authenticating users, both internal and remote.

Firewalls afford an organization a layer of protection that is in keeping with the organizational security policy. It in effect puts the security policy into practice. Firewalls can be configured to control network traffic as prescribed by the corporate security policy. A firewall should enforce the overall policy established by the administration of the organization being protected (Holden, 2003).

Nevertheless, the basic purpose of a firewall (and for which it is adequately suited) is to fend off external attacks from other networks and from the Internet. Hence its major focus is on incoming traffic.

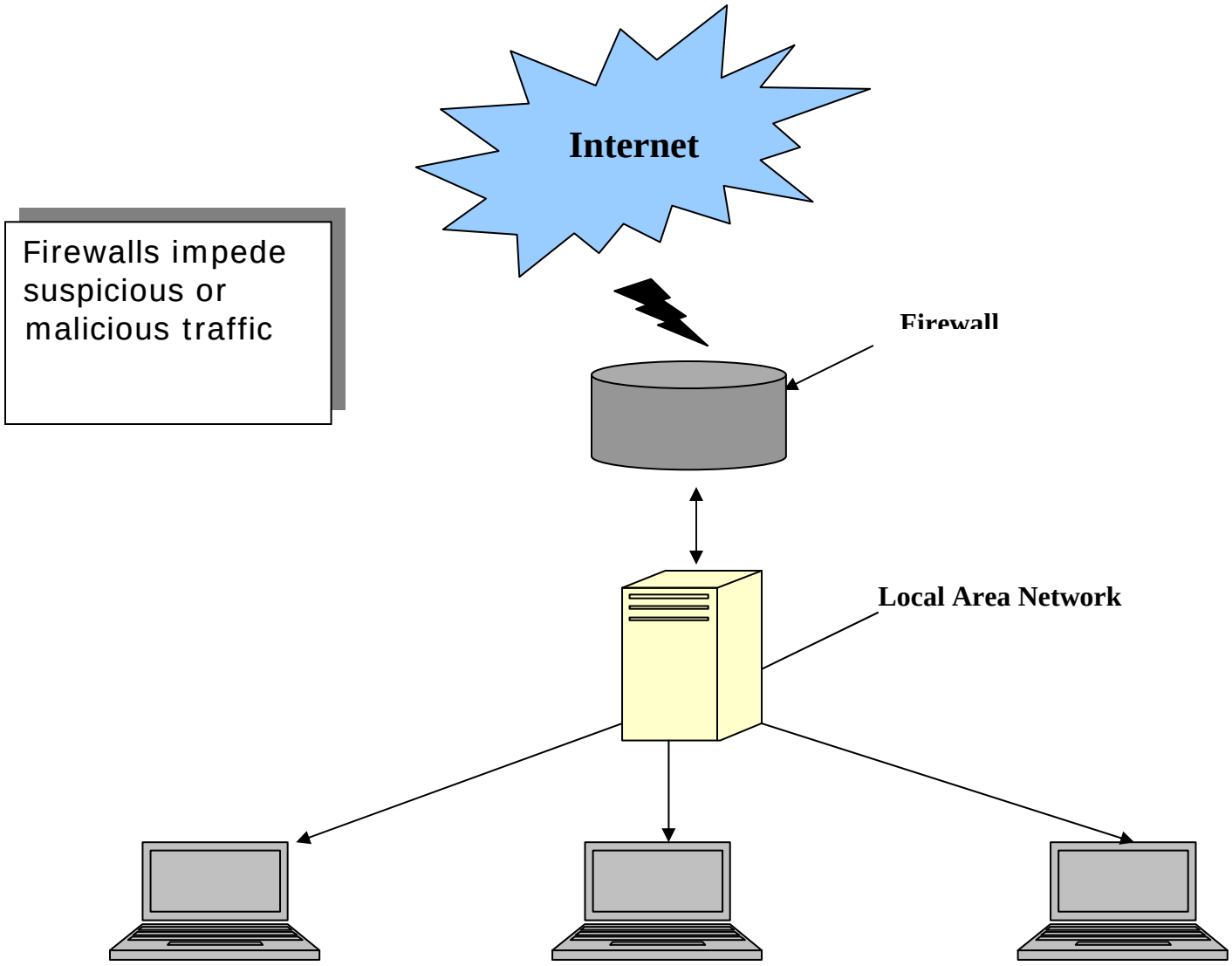
The selection of the firewall requires careful consideration. Listed below are a number of factors which weigh heavily on the choice.

- ✓ The type of firewall technology best suited for the organization. Software or hardware based?
- ✓ Determine what features are desired to meet the needs of the organization.
- ✓ Confirm the level of technical expertise required to set up and configure the firewall?
- ✓ How easy or complex is it to set up, configure and maintain?
- ✓ Ascertain if the firewall be agile enough to expand with the organization?
- ✓ Verify the startup investment costs?
- ✓ Identify the long term expenditures required to maintain the system?

Outlined below are a few of the best practices each organization should contemplate when deploying a firewall.

Recommended Firewall Configurations		
	Best Practices	**How they benefit the organization**
■	Permit all traffic to past from trusted networks	This ensures that trusted users may move about unvetted
■	Ensure firewall is not accessible by public or internal users for modification	Only authorized firewall administrators may access and manipulate the configuration
■	All SMTP data should be routed thru an SMTP gateway	This allows for the secure routing and filtering of messaging traffic
■	All ICMP data must be prohibited	Denying ICMP data helps to prevent hacker spying
■	Block all Telnet services to internal networks	This will mitigate the risk of zone hacking and prevents hackers from crasing the entire network
■	Deny HTTP traffic connect with internal networks	Ensuring the corporate internal services are invisible to the outside

Firewalls can not safeguard a network from internal threats with approved access nor can it protect against connections that do not connect through it. Thus, it must be stated that the firewall is only a component of an overall security solution and must never be construed as *the* solution.



Employing Proxy Servers (Concealing Internal Networks)

Proxy servers offer a layer of security that simultaneously protects and monitors activity on the network. Such servers shield end users from attack by concealing the ip addresses from targeted attacks. Proxy servers should be included to provide another measure of filtering and virus protection by inspecting the data payload of a packet.

A proxy server is a “mediator” for computer communications… Placing a proxy server on your network gives you several advantages, including security enhancements, caching enhancements, and greater control over your network users (Hudson, 2000).

The proxy server has three missions (a) to offer security at the application level (b) to log outbound traffic from internal networks and (c) to monitor outgoing traffic. The primary goal, however, is to restrict external users from having direct connection with the internal network.

The type of proxy server chosen is peculiar to the requirements of the organization. But it is important to note that different categories of proxy servers perform dissimiliar and distinct functions.

Nevertheless, while the proxy server does offer a wealth of benefits it is not without its drawbacks. The table below showcases the strengths and vulnerabilities of the proxy server.

BENEFITS	VULNERABILITIES
Inspects the contents of each packet and screens based on the insides	The rule must be carefully configured hence an inherrent weakness
Conceals internal IP addresses	Dereases network performance
Reduce network load by caching webpages	Compulsory reconfiguration of users programs in order to function as a proxy
Logging is concentrated into a single point	A single point can be catatrophic when a failure occurs

Securing with the Demilitarized Zone (Safe Haven)

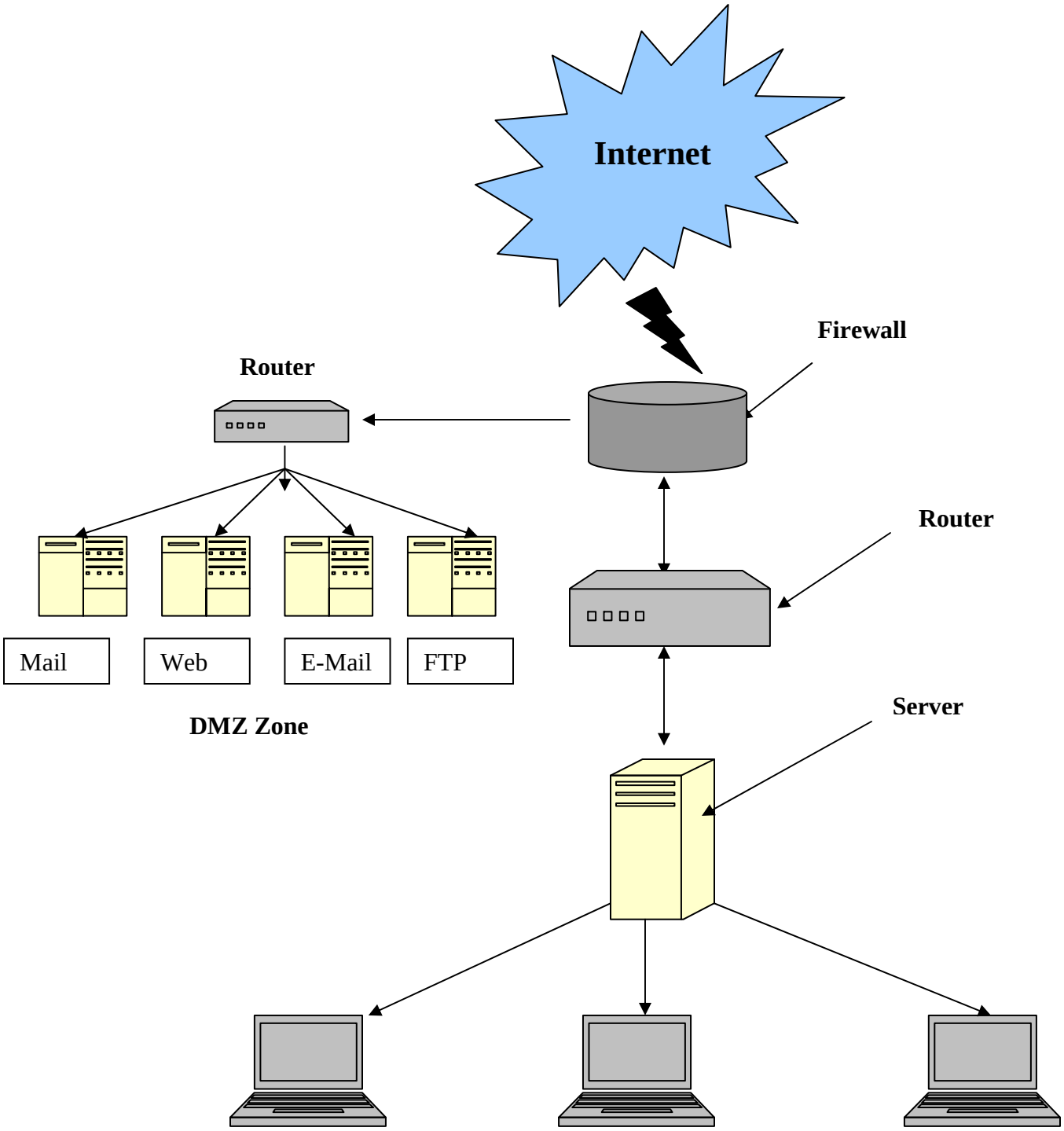
In the global theatre of today, particularly in the wake of e-commerce, the DMZ or the Demilitarized Zone delivers unparalleled layers of security. This subnet network, by residing outside of the internal network, can supply publicly available services all the while utilizing the advantages of the firewall. It is important to note that in so doing the internal local area network is being safeguarded.

DMZ's are a crucial aspect in the business to business e-commerce arena. Such zones are necessary to shield and guarantee successful transactions.

Nevertheless, the DMZ does have its own set of flaws the very act of allowing outside access opens the door for attack. However, when used as part of a comprehensive solution it can offer considerable security.

The image below depicts how the DMZ functions and demonstrates its position within corporate systems.

DMZ's allow external users to gain entry to the DMZ zone but not enter the secure network



Intrusion Detection (Alarms & Warnings)

Prevention, detection and response are the three core tenets of the Intrusion Detection Systems. The goal of the intrusion detection system is to permit approved communication into the network while disallowing unwanted and unauthorized traffic.

Intrusion Detection Systems come in three categories network intrusion detection systems, host-based intrusion detection systems, and hybrid intrusion detection systems. Used in coordination with firewalls, intrusion detection systems work to search for and identify possible attacks and once encountered alert system administrators so that countermeasures can be mounted.

The selection of an Intrusion Detection System is not a matter to be undertaken lightly as an organization must decide if their needs can be met by a software based product, a hardware based solution, or a combination thereof. In addition, an organization should consider what features the IDS is

required to have. And, lastly there has to be a determination as to how the system will be implemented as this also factors into the acquisition process.

Highlighted below are categories of Intrusion Detection Systems.

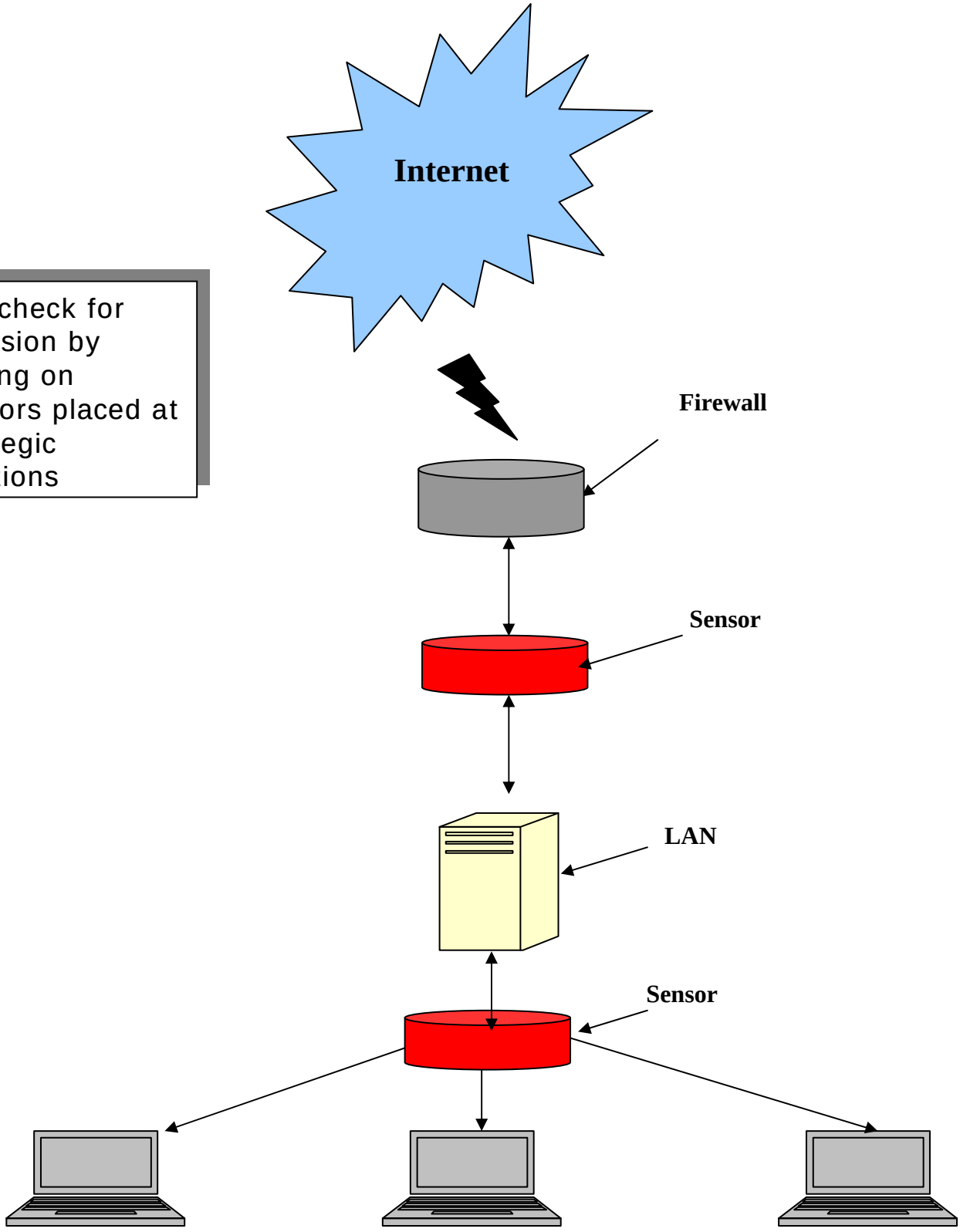
Assessing Intrusion Detection Systems		
Category	**Stationed**	**Features**
Network-based Intrusion Detection Systems	In a single location on the network perimeter	Include packet detection and the capability to transmit alerts to and fro
Distributed Network-based Intrusion Detection Systems	In a single location on the network perimeter	Utilizes sensors to access and evaluate packets and send alarms to the command console
Host-based Intrusion Detection Systems	Placed on every host on the local area network.	Inspects log files and end user activity
Hardware-based Intrusion Detection Systems	As per the client's needs	Greater capacity to handle traffic network wide, is scalable and offers the ease of plug and play

Assessing Intrusion Detection Systems		
Category	**Stationed**	**Features**
Cisco Secure Intrusion Detection Systems	Depends on sensors placed around the network	Relies on a database of attack signatures to detect and identify attack attempts as well as watches for systems of attack

It is important to state that the decision to buy is not an if but a when and which one because the IDS is most certainly another essential tool in the layered defense methodology.

Note: the chart below offers a visual demonstration of an IDS deployment and its location within an enterprise.

IDS check for intrusion by relying on sensors placed at strategic locations



The Virtual Private Network (Safeguarding Remote Users)

Setting up VPNs or Virtual Private Networks adds a measure of protection for remote clients with the security advantages of a LAN. VPNs bestow remote users with encryption to preserve information integrity, authentication to ensure only authorized users have access and encapsulation as an added and extended form of extension.

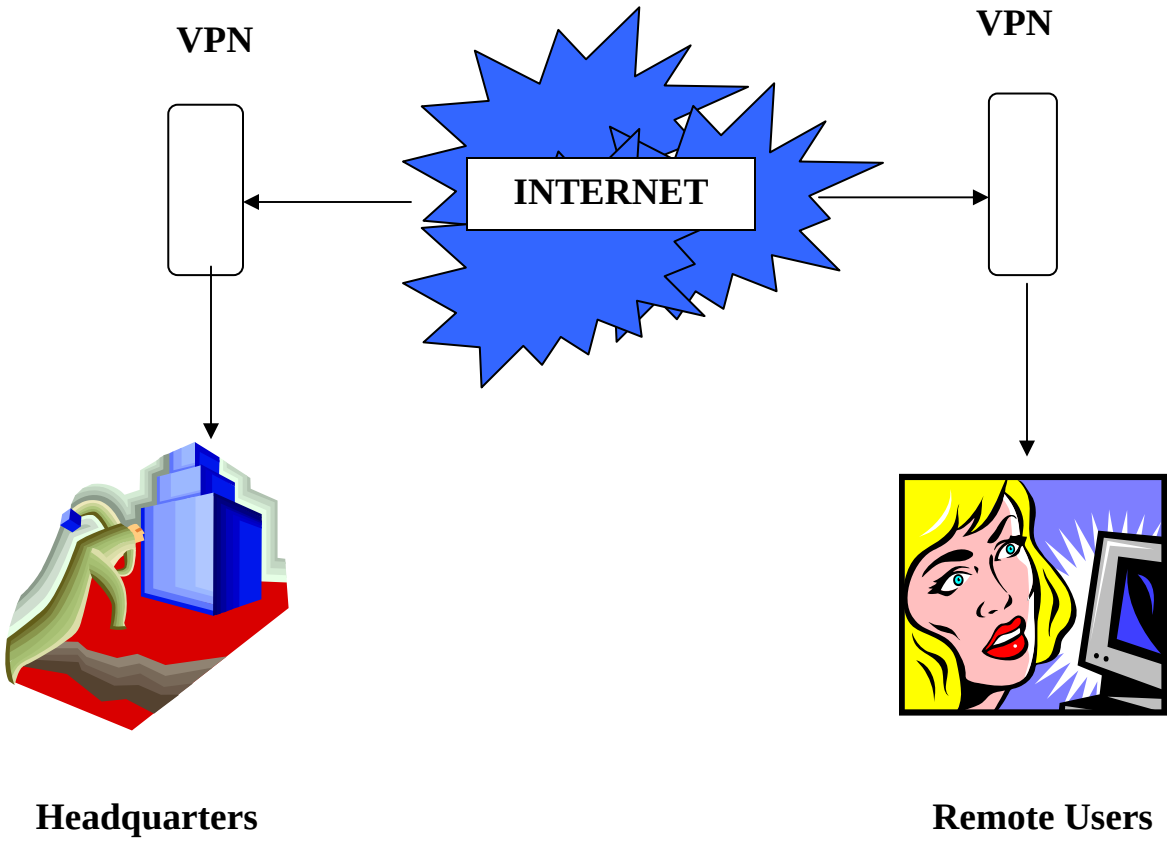
It is interesting to note that a VPN may be implemented in one of two ways: tunnel mode and transport mode. Transport mode encrypts the data inside the IP packets as opposed to the header information thus permitting the end user to establish a secure connection directly with remote host. Though this method allows communication at a reduce cost this configuration, however, is vulnerable to packet eavesdropping.

The tunnel mode calls for the use of two perimeters tunnel servers encrypting all traffic conveyed over an unsecured network. Unlike the transport mode, in tunnel mode

the complete packet is encrypted and sent from one tunneling server to another. The packet is then decrypted by the receiving server and forwarded to the final destination.

VPNs provide organizations with the security needed to connect all aspects of the business, despite geographical locations.

VPN Technologies		
VPNs	Conveyance Mode	Functions
The Trusted Virtual Private Network	Leased circuits	Transmits communication over leased circuits
Secure Virtual Private Network	Unsecure public networks	Utilizes security protocols while encrypting transmissions
The Hybrid Virtual Private Network	Leased circuits and/or Unsecure public networks	Combines the features of both sending encrypted transmissions


VPN
VPN
INTERNET
Headquarters
Remote Users

Findings and Analysis

The primary mission of Information Security is to guarantee that systems and their contents remain constant. This is done by ensuring the organization's ability to function and conduct business, assure dependable performance of all applications deployed on organizations systems, safeguard the data the organization secures and uses and finally, shield the technological assets and resources used by the organization.

While a number of security methodologies are advocated, the best approach seems to be one that delivers protection by enclosing assets and resources within logical circles of security protections. This layered approach combinations a series of security measured coordinated in a fashion to provide the optimal network defense.

Hence the security recommendation for small business computing is the layered methodology which employs a combination of security components arranged in a fashion to

provide the optimal enterprise wide defense. The example below provides a picturial depiction of a layered plan.

References

Anderson, R. J. (2008). Security Engineering: A Guide to Building Dependable Distributed Systems. IN: Wiley Publishing, Inc.

Benson, C. (2007). Security Planning. Microsoft Best Practices for Enterprise Security. [Online] Available: http://www.microsoft.com/technet/archive/security/bestprac/bpent/bpentsec.mspx [2008, April].

Bhaiji, Y. (2008). Network Security Technologies and Solutions. (CCIE Professional Development Series). IN: Cisco Systems, Inc.

Burnett, M., Kleiman, D. (2006). Perfect Passwords: Selection, Protection, and Authentication. MA: Syngress Publishing, Inc.

Buttyan, L., Hubaux, J. (2008). Security and Cooperation in Wireless Networks. Cambridge: Cambridge University Press.

Cheswick, W., Bellovin, S. M., & Rubin, A. D. (2003). Firewalls and Internet Security: Repelling the Wiley Attacker (2nd Ed.). MA: Pearson Education, Inc.

Cole, E., Krutz, R., L. & Conley, J. (2005). Network Security Bible. IN: Wiley Publishing, Inc.

Contos, B. T., Derodeff, C., & Crowell, W. P., & Dunkel, D. (2007). Physical and Logical Security Convergence: Powered By Enterprise Security Management (Paperback) MA: Syngress Publishing, Inc.

Di Pietro, R., & Mancini, L., V. (2008). Intrusion Detection Systems (Advances in Information Security. NY: Springer Science + Business Media, LLC.

Dubin, J. (2008). The Little Black Book of Computer Security. 2nd Ed. CO: Penton Media, Inc.

Fennelly, L. (2004). Effective Physical Security. 3rd Ed. MA: Levier Butter worth-Heinemann

Fowler, D. (1999). Virtual Private Networks: Making the Right Connection (The Morgan Kaufmann Series in Networking). CA: Morgan Kaufmann Publishers, Inc.

Garcia, M. L. (2008). Design and Evaluation of Physical Protection Systems. 2nd. Ed. MA: Butterworth-Heinemann.

Geier, J. (2008). Understanding 802.1X Security Solutions for Wired and Wireless Networks. IN. Wiley Publishing Incorporated.

Gollmann, D. (2006). Computer Security. West Sussex, England: John Wiley & Sons.

Gupta, M. (2003). Building Virtual Private Network (One off). OH: Premeir Press.

Heare, S. (2001). Data Center Physical Security Checklist. SANS Institute.

Holden, G. (2003). Guide to Network Defense And Countermeasures. MA: Course Technology.

Hudson, K. (2000). An Introduction to Microsoft Proxy Server. Windows IT Library. [Online] Available: http://www.windowsitlibrary.com/Content/265/1.html#3 [2008, May].

IR&C. (2006). IT Risk Assessment. Information Resources and Communication. [Online] Available: http://www.ucop.edu/irc/itsec/risk.html [2008, May].

Jenkins, B. D. (1998). Risk Analysis, Risk Assessment, Risk Management. [Online]. Available. http://www.nr.no/~abie/RiskAnalysis.htm [2008, Oct].

Jones, A. & Ashenden, D. (2005). Risk Management for Computer Security: Protecting Your Network and Information Assets. Oxford: Elevier Buttersworth-Heinemann.

Kaufman, C., Perlman, R., & Specinar, M. (2002). Network Security: Private Communications in a Public World. NJ: Prentice Hall.

Koller, G. (2005). Risk Assessment in a Business and Decision Making Industry: A Practical Guide 2nd. Ed. FL: Taylor & Francis Group.

Komar, B., Beekelaar, R., & Wettern, Joern. (2003). Firewalls for Dummies. 2nd. Ed. NY: Wiley Publishing, Inc.

Lee, W., Wang, C., & Dagon, D. (2008). Botnet Detection: Countering the Largest Security Threat. NY: Springer Science + Business Media, LLC.

Lemos, R. (2005). Computer, Physical Security Expected to Merge. Cnetnew.com. [Online] Available: http://news.com.com/Computer%2C-physical-security-expected-to-merge/2100-7348_3-5534312.html?tag=news.1 [2008, February].

Lockhart. A. (2006). Network Security Hacks: Tips & Tools for Protecting Your Privacy (Hacks). CA: O'Reilly Media, Inc.

Magalhaes, R. M. (2004). Using Passwords as a Defense Mechanism to Improve Windows security (Part 2). WindowsSecurity.com. [Online] Available: http://aolsearch.aol.com/aol/redir?src=websearch&requestId=47eb4293d1f757e3&clickedItemRank=2&userQuery=a+word+about+password+security+for+system+defense&clickedItemURN=http%3A%2F%2Fwww.windowsecurity.com%2Farticles%2FPasswords_Improve_Windows_Security_Part2.html&title=Using+passwords+as+a+%3Cb%3Edefense%3C%2Fb%3E+mechanism+to+improve+Windows+%3Cb%3Esecurity%3C%2Fb%3E+%3Cb%3E...%3C%2Fb%3E&moduleId=matchingsites.jsp.M&clickedItemPageRanking=2&clickedItemPage=1&clickedItemDescription=WebResults [2008, February].

Mansfield, R. (2000) Hacker Attack. CA: Sybex, Inc.

McNab, C. (2004). Network Security Assessment: You're Your Network. CA: O'Reilly Media, Inc.

Mehdizadeh, Y. (2004). Convergence of Logical and Physical Security. SANS Institute. [Online] Available] http://www.sans.org/reading_room/papers/download.php?id=1308&c=41507eac94d142791d84fe9cd4e99299 [2008 October].

Noticeboard. (2004). Securing Physical Access and Environmental Services for Datacenters.

Parker, D. (2005) Access Controls: What it is and how can it be undermined? Windows.com. [Online]. Available. http://www.windowsecurity.com/articles/Access-Controls-What-is-it-how-undermined.html [2008 January].

Rhodes-Ousley, M. (2004). Network Security: The Complete Reference. CA: McGraw-Hill/Osbourne.

Risk Management Insight. (2007). FAIR Basic Risk Assessment Guide. Risk Management Insight, LLC. [Online]. Available: http://www.riskmanagementinsight.com/media/docs/FAIR_brag.pdf [2008, February].

Santos, O. (2008). End-to-End Network Security Defense-In-Depth. IN: Cisco Systems, Inc.

Silberschatz, A., Galvin, P. B., & Gagne, G. (2005) Operating System Security. NJ: Wiley & Sons, Inc.

Skoudis, E. (2006). Computer Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses (2nd Ed.).

Stallings, W. (2006). Network Security Essentials: Applications and Standards (3rd Ed.). NJ: Prentice Hall.

Stewart, J. M., Tittel, E., & Chappel, M. (2004) CISSP: Certified Information Systems Security Professional Study Guide, Third Edition. CA: Sybex, Inc.

Surman, G. (2002). Understanding Security Using the OSI Model. SANS. [Online]. Available. http://www.sans.org/reading_room/papers/index.php?id=377 [2008, March].

Tyska, L., & Fennelly, L. (2000). Physical Security 150 things you should know. MA: Butterworth-Heinemann

U.S. GAO (Government Accounting Office) (1999). Information Security Risk Assessment Practices of Leading Organizations. [Online]. Available. http://www.gao.gov/special.pubs/ai00033.pdf [2008, August]

Webopedia. (2007). What is Packet Filtering? Webopedia.com [Online] Available: http://www.webopedia.com/TERM/P/packet_filtering.html [2008, February].

Whitman, Michael E. & Mattord, Herbert J. (2005). Principles of Information Security. 2nd Ed. MA: Thomson Course Technology.

Wikipedia. (2008). Proxy Servers. [Online]. Available. http://simple.wikipedia.org/wiki/Proxy_server [2008, August].

Zhang, Y., Zheng, J., & Hu, H. (2008). Security in Wireless Mesh Networks (Wireless Networks and Mobile Communications). FL: Averbach Publications.

Zeltser, L. (2005). Inside Network Security Perimeter: Packet Filtering. Informit.com. [Online] Available: http://www.informit.com/articles/article.aspx?p=376258 [2008, Feb].