Global Information Assurance Certification Paper

Information Technology and Security Topics As Applied to a Small Business Environment

Gayle Shipp

GSEC Practical, Version 1.4b, Option 1

October 15, 2003

Author's Note: I was approached by the management of a small manufacturing and engineering business (approximately 100 employees) with the request that I advise them of considerations that should be applied to the organization's IT infrastructure. This company's IT department had developed in a piece-meal fashion over a number of years of slow but steady growth. The company now has potential new work that would cause them to double in size over the next year to eighteen months, with the continuing expectation of increased growth. Company management wanted to learn more about how a viable IT infrastructure should be created and how to implement a solid computer security position as a basis for making viable business decisions. The following paper was presented to the company as a working tutorial. It has been reformatted to comply with the SANS GSEC requirements; company-specific references have been removed.

Information Technology and Security Topics
As Applied to a Small-Business Environment

Abstract

When evaluating Information Technology (IT) and security issues in the current economic climate, corporations must balance asset protection with avoidance of unnecessary expenditures. By carefully evaluating, analyzing, and addressing its corporate IT position, a business can increase its viability while maximizing its return on IT investment. On his website, Marcus Ranum writes: "…computer security is nothing but attention to detail and good design." (Ranum) As a company builds its computer infrastructure, it can inadvertently neglect those two elements of good computer security. This document focuses first on the details that make up an IT infrastructure, then emphasizes good design by discussing best practices that will strengthen a company's IT position and security posture.

This paper is broken into three sections: Section I describes the evaluation and assessment of the current position and future needs of the IT infrastructure; Section II demonstrates the application of industry best practices and the deployment of security solutions to the information obtained in Section I in order to enhance the overall security posture of the organization; Section III addresses cost considerations and trade-offs to aid in the decision-making process.

Section I. Evaluation and Assessment

Many IT infrastructures start small then expand over time to meet new demands and requirements. Since this expansion often takes place in a non-structured manner, an organization may eventually find it beneficial to step back and reassess current and future corporate needs, how well the current IT infrastructure is meeting those needs, and what should be done to position corporate IT for future growth.

In order to perform a thorough evaluation and assessment of the existing IT infrastructure, one must first obtain the "big picture" with respect to the various components of the IT infrastructure, computer security, and corporate planning and directions. The following list is not exhaustive, but represents questions that will present an overall view of corporate IT practices. The questions below are intended as points of reference and should act as starting points for more detailed queries if the situation so warrants.

- Corporate-specific Issues
  Does the corporation have a Business Continuity Plan (BCP) and a Data Recovery Plan (DRP)? What growth is currently planned in business

areas and in IT support services? What is management's expectation of the IT department? What additional corporate requirements (i.e., ISO 9001 certifications) is the corporation seeking? What role does the IT department play in helping the corporation meet these goals? Is corporate-proprietary information kept on the systems? How about sensitive customer information? How is this information protected? Is there other information that should be protected?

- Policies and Procedures
  What corporate IT policies are in place? Which are written and which are merely "understood"? Which IT processes have been deemed significant enough for written procedures? Who writes, and who signs off on, the policies? the procedures?
- Computer Hardware
  What IT hardware is being used for servers? for the desktop? for remote access? Are there additional systems (i.e., hot spares) to cover system failures? What peripherals are used? Is there any "special purpose" hardware? Is there a hardware database; if not, how is the hardware documented and tracked?
- Computer Software
  What computer software is being used in the corporation? Is it site licensed? If not, is each installed copy licensed? Is a given software package server-based or is it installed on each individual system? What is the patch level (if applicable) of each software package? What operating systems are installed? What are their patch levels? Is there a software database; if not, how is the software documented and tracked?
- Networking Equipment (including Firewalls)
  Does the facility have a router or are routing functions provided by the ISP? Which vendor's products are used and what IOS version is being run? What network equipment is in use at the facility? Are there special configurations (i.e., virtual networks on the switches)? What is the bandwidth of the devices (i.e., switches, system network cards, etc.)? Is there one bandwidth for the entire organization, or are some system (i.e., servers) configured at a different bandwidth? Does the network have a firewall, and if so what is its configuration?
- Services
  What services are provided by the IT servers (i.e., e-mail, web services, DNS, anti-virus server)? What are the primary support services provided by the IT Department (i.e., server, network, desktop, VPN, application, database support)? How are the various service functions prioritized and supported? What services are not provided? Are there services that should be provided but are not because of staffing (or other) limitations? How are backups handled (i.e., server, desktop)? How are operating systems patches handled? What authentication methods are in place? How are permissions and access privileges handled? Is remote access being provided? If so, what is being used for this access (i.e., PDAs, laptops)? How are those systems being protected? Is a VPN being used?

- IT Support Personnel
  How many full-time and part-time IT support personnel are there? What are their primary functions? How heavily does the organization depend on "ask your neighbor" as a support tool? Are additional personnel needed either full-time or part-time? If so, to fulfill which functions?
- Documentation
  What formal documentation is in place? Is it printed, web-based, or both? Who is responsible for creating the documentation? How is staff advised of the availability of documentation?
- Training
  What are the provisions for user training? Is the IT department expected to do specific training (i.e., application training, computer security training, one-on-one user training, etc.)? Is training formalized, ad hoc, or a combination? What training is available and/or provided to IT personnel?
- Outsourcing Issues
  What is outsourced? What is the level of dependency on the outsourced services? What Service Level Agreements (SLAs) are in place? What contingency plans are in place? How is the company protected in the event of the failure of an outsourced service?
- User-Level Considerations
  Based on user interviews, what are users' opinions of existing services? What's working well? What can be improved? What is needed but unavailable? What "would be nice"? What would help users be more effective in their jobs?

Whether an assessment of this nature is done by an outside organization or by in-house staff, it must be understood that this is only the first step. Section II continues with the next step in this process.

Section II. Best Practices and Recommendations

Once an assessment has been completed, the strengths and weaknesses of the corporation with respect to its IT infrastructure and security posture can be evaluated. By establishing a more formalized IT infrastructure, a business can position itself for future growth while at the same time securing and protecting business assets. Although this section will of necessity mention specifics in some areas, it is not intended as a procedural or implementation document. More detailed specifics would be defined in response plans that would be created by analyzing the assessments from Section I of this paper, and then applying best practices to that data. New risks constantly threaten the IT security infrastructure; therefore, the entire process must be considered a cycle to be repeated and refined over time. (Briney)

Corporate-specific Issues

Two of the most critical documents that address risk mitigation within an organization are the Business Continuity Plan (BCP) and the Data Recovery Plan (DRP). These plans provide the means to address contingency, reliability, confidentiality, integrity, and recovery issues that would be necessary for the survival of the business and its IT resources in the event of a critical event. Although reports of terrorist activity lead one to consider critical events of a catastrophic nature, these plans would also cover situations such as a building fire or water damage to computer equipment.

Although these plans are serious undertakings in terms of staff time, there are numerous templates available to facilitate the process. The Business Continuity Plan provides for the continuity of critical business resources and processes in the event of a disruptive event and ensures that the corporation will be able to continue operations during the recovery process. It can encompass a variety of other plans such as an Emergency Planning and Response Plan, Specific Service (such as the phone system) Recovery Plans, and Data Recovery Plans. (unknown author)

The Data Recovery Plan addresses computer and IT infrastructure and computer security related issues that would facilitate recovery from a disruptive event. It identifies the critical IT support processes that a business requires and addresses ways of resuming IT operations to provide those processes in the event of a disaster. Additionally, it addresses longer-term recovery processes that will restore the business to its original position. (Bit Solutions, LLC)

Both plans are designed to allow the business to continue operations in the event of, or at least recover quickly from, disruptive events. Besides providing a level of confidence in effective disaster recovery within the organization, they also provide customers and stakeholders with the reassurance that the organization has a plan in place to effect an immediate response to a disaster or disruptive event. It is not unreasonable to assert that failure to prepare plans of this nature could, in the case of a disaster, be the difference between the viability and the failure of a business.

Policies and Procedures

Although policies and procedures are often thought of as “just documentation”, they are actually the backbone of the IT infrastructure as well as the means by which protection is provided for the corporation, the equipment, the capabilities, the support personnel, the users, and the data. Because procedures are more commonly used and better understood than policies, this discussion will focus on policies.

Policies address “who, what, where, when, why” while procedures address “how”. Lack of written policies leaves the corporate IT infrastructure open to misuse and abuse, as well as the consequences of the failure to safeguard IT resources and critical information. To provide good security policies, risks and

vulnerabilities must first be assessed, then policies developed and implemented to comprehensively cover the corporate and IT infrastructures.

There is a wide range of the type and level of coverage of various corporate IT policies. While there are certain policies that every organization should have, an organization's policy concepts, development, and implementation are tailored to its particular environment. All IT policies should have the approval of and be signed off by corporate management and other key personnel. Corporate IT policies serve several purposes: they define areas that need clarification and set guidelines; they protect company assets by outlining acceptable and unacceptable conduct, behavior, responses, and functionality; they protect IT support personnel by defining roles and responsibilities, establishing clear guidelines, authorizing performance of duties, and defining the means to protect IT information; they protect IT users by delineating acceptable and unacceptable usage of IT equipment, establishing guidelines for access and privileges, and describing the consequences of lack of compliance; they protect data integrity, confidentiality, and availability by establishing a protective framework for that protection. (Lipson)

There are numerous IT security policies that should be considered. High-level program policies are often written at a corporate level; they can also be the "policy policies" that describe how other policies are created and implemented. Issue-specific policies address areas such as an acceptable use policy, antivirus policy, password policy, data backup policy, and the proprietary and sensitive information policy. System specific policies cover systems that perform specific functions, such as the firewall.

Computer Hardware

Computer system hardware is the physical backbone of a corporation's IT infrastructure. Often, however, the addition of hardware over a period of time leads to weaknesses in the areas of standardization, redundancy, and even reliability. When computer hardware is purchased, consideration should be given to both short-term and long-term planning. In the short-term, meeting the needs of immediate goals and needs while addressing cost limitations, is paramount. However, long-term planning should address needs for interchangeability, flexibility, and migration of hardware as it ages and is upgraded, shifted to other support functions, or replaced by newer systems.

With the proper long-term planning, design and implementation issues will address standardization, interchangeability, and cost-effective solutions. Although it is often tempting to purchase the "latest and greatest" hardware, doing so should not hinder an organization's ability to address hardware failure issues in a cost-effective manner. Ensuring that standardized systems are purchased will allow failed parts on critical systems to be replaced with those from non-critical systems (and even allow the replacement of entire failed systems with non-critical systems). Standardization will allow the IT department

to stock fewer parts and will also allow the IT staff to provide upgrades in a systematic and cost-effective manner. (Burry)

The potential for catastrophic hardware failure can be mitigated by both the standardization mentioned above and by other practices. While not an exhaustive list, the following practices are a few methods to lessen the effect of hardware failures. RAID disks on major servers can provide protection against disk failure; hot-swappable disks on RAID systems will further minimize or eliminate disk-based downtime. Entire computer systems can be set up as redundant or hot-swappable servers; lower-cost solutions include mirroring critical disks and using backups to restore critical data in the event of a system failure.

IT support is also simplified when computer systems are well documented. The hardware database should include individual system information (i.e., model and serial numbers, configuration, location) as well as a list of the software installed on the system (i.e., operating system, application software, and patch levels). There are various programs available that will obtain this information, and other application programs that will store the information in a database, often in conjunction with network diagrams and other network information.

Computer Software

Software also benefits from standardization. Licensing is a critical factor from a legal standpoint; software companies often strongly pursue licensing agreement violations. Standardization can allow an organization to take advantage of multiple-use licensing agreements at a reduced cost. From an IT support perspective, standardization of computer software minimizes IT support costs by allowing the IT staff to become proficient in fewer versions applications (i.e., word processor or spreadsheet). Standardizing on one version of an operating system helps minimize IT staff time in vulnerability tracking. (Burry)

IT computer software planning should also consider the location of application software packages. It is often possible to install a single copy of an application on a server then license its use to the various desktop systems, thus minimizing the number of installations that must be performed. In doing so, the cost of support personnel time is minimized for initial installations as well as for later patches and upgrades.

From a computer security standpoint, application software standardization, operating system version standardization, and server-based application installations increase the IT staff's ability to quickly address problems. With server-based application software installations, application software patches do not have to be installed on individual systems and can be quickly applied to the server-based copy. Operating system version standardization allows the IT staff to efficiently monitor vulnerabilities and apply necessary patches.

Networking Equipment (including Firewalls)

In addition to providing the connectivity that enables communication between systems, networking equipment also presents a first line of defense in IT protection. The importance of good network security practices cannot be overemphasized.

Routers may be provided and maintained at the Internet Service Provider (ISP) or may be a part of a corporation's network. In either instance, router maintenance and configuration is critical. It is often easy to forget that a router can present a single point of failure; therefore, contingency planning must include how a router failure will be addressed (i.e., redundant routers, hot spares). Router configuration is essential to the security of the network it supports. Router operating systems and firmware must be kept up-to-date to minimize risks from known vulnerabilities. Router Access Control Lists (ACLs) must be routinely reviewed and adjusted to support corporate business needs while providing maximum protection.

Switch settings and configurations should also be reviewed periodically. While network switches do not present the same level of vulnerability as routers or firewalls, improperly configured switches can affect network connectivity and throughput. As a company grows, special switch configurations such as virtual LANs that consolidate and isolate high-traffic segment of the network may also be an effective way to maximize the overall throughput of the company backbone. Similarly, switches may be used to provide high-speed throughput on some sections of the network (i.e., between servers) while allowing other systems to operate at lower bandwidths. This is a cost-effective way to introduce higher-speed network cards and devices in a staged migration. As with routers and firewalls, switch vulnerabilities can be minimized by installing the latest updates.

Firewalls must also be considered as potential single point of failure items. As with routers, plans must be in place to minimize downtime due to a firewall failure. Configuration of firewalls is one of the most critical, yet often least understood areas of a corporation's security posture. Firewalls protect an organization by denying both internal and external access and capabilities. Of course, certain ports must be opened and services must be allowed so that an organization can accomplish its goals. Allowing these capabilities (also known as "opening holes in the firewall") can also introduce vulnerabilities and threaten an organization's security. It is critical that firewall security policies be carefully scrutinized then reviewed on a regular basis. Because it is often necessary to "open a hole" temporarily to accomplish a specific task, regular reviews of the firewall configuration will ensure that those holes do not inadvertently remain open instead of being closed down again.

Services

IT services can range from the highly visible (i.e., a system on a user's desktop) to the invisible (i.e., backups). An IT department should have a clear understanding of what services are being provided to an organization and how those services can affect the organization's bottom line and security posture. Many IT departments define three categories of services: those that are used and supported, those that are permitted but not supported, and those that are denied. By clarifying its roles and responsibilities with respect to various user services, the IT department not only gains some kind of control over what must be supported, but also clarifies for the users what services are not available and the services the user must support. In determining what services fall into those three categories, the IT department must understand the impact on support costs as well as on IT security issues.

The "used and supported" services are the reason that the IT department exists. Under this heading are three categories: services that are critical to the basic structure of the business and that protect the IT availability and integrity (i.e., servers and individual systems and their operating systems, communication and network services, applications and data); services that are needed but cannot have a negative affect on critical systems (i.e., updates, expansions, additions); and services that are desired but may not conflict with critical systems (i.e., enhanced capability and ease of use services).

The "permitted and unsupported" services should be those that represent low cost and low risk, which means that an organization allowing these services must choose carefully when identifying them. These can be conveniences (i.e., media players), company-cultural (i.e., the occasional use of a graphics package for entertainment purposes), and environment enhancements (i.e. screen savers and backgrounds).

The "denied" services represent those that may be high cost, high risk, or simply unacceptable. This includes many attractive Internet 'services' (i.e., questionable websites), personal use and abuse (i.e., using company resources to maintain a home business), inappropriate hardware or software (i.e., personal dial-up devices), and testing on or experiments with the systems (i.e., installing code to override system settings).

In all instances, the final decision about the support of IT services rests with upper-level management, although they should strongly consider IT department feedback, recommendations, and reservations.

IT Support Personnel

IT support personnel are the single most important investment an organization can make in its IT infrastructure and overall computer security planning. Levels of capability and competency vary among IT support staff, and most organizations have a need for staff with varying levels and areas of knowledge. IT support positions do not lend themselves to a "one size fits all"

approach, and organizations would be well-served by breaking down corporate IT support requirements into various areas such as application support, desktop support, server support, network support, and computer security support. By identifying the areas critical to its business operations, an organization can then address obtaining the necessary support for those areas.

An organization must also decide which IT support areas to maintain in-house and which could be outsourced or handled by support contracts. Because many IT support personnel issues come down to cost considerations, it is also important to keep in mind that the most cost-effective way of providing support in the short-term may not be the best solution for the company in the long-run, particularly when factoring in computer security issues. (See Section III for an additional discussion of cost issues.)

Documentation

Saying that documentation is critical to the operation of an IT environment appears to be stating the obvious; however, based on the lack of documentation within a large number of IT environments, the issue bears some discussion. In an effort not to belabor what is apparent, documentation must cover all of the important aspects of the IT infrastructure including but not limited to policies, procedures, contingency plans, contact information, and informational handouts. Location of documentation is also an important consideration. If documentation is web-based, what happens if there is a system failure? Organizations must not only provide printed documentation, but must also make sure that staff members who could be potentially affected by a failure know where the printed copies are located. In addition to covering critical functions, contact names and addresses must also be available, particularly for emergency situations. In providing those names, do not forget contact information for any outsourced IT functions.

Computer security is enhanced by sufficient documentation to allow response personnel to perform whatever tasks are necessary when responding to a disruptive event. When an effort has been made to both create the documentation and to keep it updated, an organization has a much better probability of addressing critical events successfully and in a timely manner.

Training

A formalized computer security training plan is essential to the overall security posture of an organization. Regularly scheduled user training is one of the most cost-effective ways to minimize security risks because many of the entry points for malware is via users (i.e., clicking on e-mail attachments, downloading destructive code, clicking on e-mail attachments). Ensuring that users are aware of current threats and how to avoid them will go a long way toward curtailing those types of risks. This is particularly applicable to personnel who use laptops off-site and connect to company resources.

IT staff training is also important in maintaining a strong security posture. This training can be as simple as providing time for (and expectations that) IT staff to spend some time each week maintaining a current level of knowledge about computer security threats and vulnerabilities. Specialized training classes are also valuable, as is supporting IT staff members who desire computer security certifications in areas that will help support overall business goals. (Duigan)

Outsourcing Issues

Outsourced IT services introduce another level of risk management. Every organization is dependent at some level on outsourced services; for instance, Internet connectivity requires the services of some type of Internet Service Provider (ISP). The organization must have a clear picture of what services are outsourced and the criticality of a failure of any of those services. The organization must also define an acceptable level of impact. For an outsourced website, for instance, website unavailability be a minor inconvenience (in the case of informational websites) or a major catastrophe (in the case of commercial websites that receive customer orders).

Service Level Agreements (SLAs) should be in place with the providers of outsourced IT services clearly outlining contingency planning, critical response time guarantees, and operational commitments. For instance, if in addition to Internet connectivity the ISP provides and maintains the router for an organization, the SLA should provide a commitment on updating the router operating system and firmware to address vulnerabilities. The SLA should also clearly describe the responses an organization can expect in the event of a router or connectivity failure and a commitment as to maximum downtime. If Domain Name Service (DNS) functions are outsourced, there should be a commitment as to server redundancy and server failure contingency plans. In the case of an outsourced website, the SLA should not only address server and connectivity failures, but should also describe how frequently the website is backed up.

While outsourcing can be a cost-effective means to provide IT support solutions, it can also open an organization to additional risks and vulnerabilities that are outside its immediate control. Solid SLAs and a clear understanding of what an organization can expect from the outsource providers can go a long way toward mitigating those risks. (Barbee)

User-level Considerations

Interviewing users may at first glance seem counterproductive. Because IT staff interacts with the users on a regular basis, it is easy to think that the users have communicated all of their wants and desires and that interviews will only elicit complaints and more work. Doing formal user interviews, however, has several benefits. First, one-on-one interviews involve the users in the overall planning process. Well-prepared interview questions as well as conversations

during the interview can act as a training device to help users obtain a view of the high-level issues being dealt with. Second, one-on-one interviews provide an opportunity for the IT staff to really listen and quantify user concerns, needs, and desires. Analysis of the acquired interview data can often indicate trends that are not visible on a day-to-day basis. For instance, are users asking for services that are not necessary to support business directions and that may have a detrimental affect on the network (i.e., instant messenger services, unauthorized shareware, etc.)? If so, that can indicate a need for additional user training (or even informational memos) to explain why the services are not allowed. Third, one-on-one interviews provide the opportunity for users to seriously contribute to IT functionality and security. Perhaps a user has noticed issues that could lead to vulnerabilities in the system; often the IT staff is so busy that users will not bother to bring those issues forward, or users will believe that IT staff is already aware of the issues. Finally, one-on-one interviews help users see that the IT staff is involved in their needs. Even if users are not provided with functionality that they desire (but which could cause corporate security vulnerabilities), they know that the IT staff can be approached and will explain decisions instead of simply saying no.

The "people factor" is a critical part of the overall security structure of an organization. While user interviews are not something that will be (or can afford to be) done on a regular basis, occasional data-gathering initiatives can often provide insights and foster a stronger working relationship between users and IT staff. In doing so, it addresses the "people factor" in a positive manner. (Briney)

Security Testing and Maintenance

A final best practices area that should be mentioned is that of testing, detection, scanning and auditing. These areas are often used once most of the other computer security issues have been addressed and are methods for determining the success of the computer security initiatives. Penetration tests and vulnerability scanning are performed to determine the effectiveness of security defenses and to determine which areas (such as patches and updates) have not been sufficiently addressed. Intrusion detection systems are sometimes placed in an IT infrastructure to allow monitoring of security breaches that might otherwise go undetected. Security auditing is used as a means of assessing security vulnerabilities as well as undetected violations.

Industry best practices in computer security and IT infrastructure can only go so far in addressing the needs of a corporate IT environment. As with most areas of a business enterprise, the people are both the strongest and the weakest links. Preparation, education, and constant vigilance can go a long way to ameliorate the potential for damage to an organization and to protect an organization's assets and viability.

Section III. Cost Considerations, Trade-offs, and Corporate Directions

Assessing, maintaining, and growing the IT infrastructure is a progression of efforts that are never fully completed. The saying “life is a journey, not a destination” also applies when addressing a corporation’s IT infrastructure and security practices. One of the most important services provided by a company’s IT support staff is to provide the information that will enable company management to evaluate the trade-offs between computer support, computer security, and bottom-line costs.

Calculating costs can be a very complicated area. Issues such as lost business, late deliveries, loss of customer confidence due to IT infrastructure problems must be factored into the bottom line costs. Any downtime in an IT service can have an impact that reaches far beyond that of a simple system failure. In addition to the time and effort required for IT staff to repair a failure, an organization must also consider how the downtime will affect users (i.e., an hour’s downtime that affects 40 users means 40 man-hours or a week of lost work). Additionally, system downtime can mean cascading costs in project delays, overtime costs, and potential for late deliveries, loss of customer confidence, or lost business.

Lack of policies can also result in costs to the business. Just to use the acceptable use policy as an example, lack of such a policy can increase costs due to improper usage of equipment, wasted employee time, and legal issues that may result from damage caused. (Duigan)

An oft-quoted calculation when dealing with IT security issues is

Risk = (Threat x Vulnerability) / Countermeasure

This is a good way for management to evaluate the relationship of risk, threat and vulnerability in order to determine which solutions are cost-effective and which are not. It can be challenging to apply specific values to these components, but doing so can be enlightening when deciding where to best spend money on IT security measures.

There are also quantitative and qualitative analyses that can be done that are outside the scope of this paper. These are a part of the calculations that should be done when creating a BCP and a DRP, and are available in documentation about that subject. (A Google search for ‘Business Continuity Plan’ or ‘Data Recovery Plan’ will provide numerous references as well as templates that can be purchased to simplify the writing process.) Simply stated, these analyses provided a means to calculate annualized loss expectancy based

on a company's exposure factor, asset values of threatened resources, and the potential rate of occurrence of a disruptive event.

Additional costs that must be considered are those of IT support staff including on-site personnel and outsourced contracts. Evaluating this topic often requires that trade-offs be made in the level of support, convenience of support, capabilities of personnel, and relative cost of each. IT security concerns must also be considered in this evaluation because sometimes less expensive solutions actually increase the potential for IT security incidents. While many of the calculations of this nature are subjective, a thorough analysis of all of the potential costs in the event of an incident (including the intangibles such as loss of customer confidence) must be made in order to understand the possible cost of an incident to the organization.

IT hardware and software costs are yet another area that must be considered. Redundancy in essential hardware (i.e. hot spares, RAID systems) can certainly add costs to the enterprise. However, calculations of potential costs in the event of downtime may indicate that these are justified expenses. Investment in software packages (i.e., monitoring systems, backup systems, etc.) must also be evaluated in light of their potential to minimize downtime.

Conclusion

Ultimately, corporate management must make the difficult decisions will affect the IT infrastructure, IT security concerns, and even business viability. It is up to the IT staff to ensure that management is provided with all available information to facilitate effective and efficient solutions. A carefully designed, implemented, and maintained IT infrastructure, properly security solutions, and well-trained users and IT staff can ensure that the corporate IT environment properly supports the organization's business goals.

References

Ranum, Marcus. "Computer Security." Personal website. 14 Oct 2003 http://www.ranum.com/security/computer_security/index.html

"BC 010102 Benefits of Developing a BCP." Complete Work: Business Continuity Planning / Disaster Recovery Planning An Online Guide. 14 Oct 2003 http://www.yourwindow.to/business-continuity/bcp3_1_2.htm

"Creating a Disaster Recover Plan." Bit Solutions, LLC. 14 Oct 2003 http://www.bitsolutionsllc.com/Create a Disaster recovery Plan.pdf

Briney, Andrew. "The Risk Lifecycle." Online version of Information Security Magazine. June 2003. 14 October 2003 http://infosecuritymag.techtarget.com/2003/jun/risklifecycle.shtml

Lipson, Adam. "Placing Strategic Security on the Front Burner." SC Infosecurity News. August 2003. 14 October 2003 http://www.infosecnews.com/opinion/2003/08/06_03.htm

Burry, Christopher. "Increasing Value from Fixed IT Costs." Computerworld Online Magazine. 04 March 2003. 15 October 2003 http://www.computerworld.com/managementtopics/roi/story/0,10801,78025,00.html

Burry, Christopher. Ibid.

Duigan, Adrian "10 steps to a successful security policy." 08 October 2003. 15 October 2003 http://www.computerworld.com/securitytopics/security/story/0,10801,85583,00.html?SKC=security-85583

Barbee, Mike. "SLAs: How to buy the best IT performance." Computerworld Online Magazine. 22 September 2003. 15 October 2003 http://www.computerworld.com/managementtopics/outsourcing/story/0,10801,84806,00.html

Briney, Andrew. "The Four P's." Online version of Information Security Magazine. September 2003. 15 October 2003 http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss81_art198,00.html

Duigan. Ibid.

Last Updated: July 22nd, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor