Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Systems Maintenance Programs – The Forgotten Foundation and Support of the CIA Triad
C. Farley Howard
GSEC v1.3
January 10, 2002

Abstract:

Much has previously been written on the importance, relevance, and critical application of the CIA (Confidentiality, Integrity, Availability) Triad security model. However, operational emphasis on the CIA model has historically been placed primarily on "hard" or widely addressed topics relating to prevention, auditing, and enforcement. This type of emphasis addresses issues such as policies and procedures, training and awareness programs, encryption, access controls, and hardware or software based security management tools. Where "soft" issues such as maintenance procedures have been addressed as a security function, it has been almost solely in the areas of Change Management. There are some areas of overlap, however. Items such as backups and anti-virus protection are often addressed in both maintenance and security documents. What is usually not recognized is the symbiotic relationship between maintenance and security.

During the current economic downturn, organizations are making every possible attempt to extend the life expectancy of their existing systems. A well engineered maintenance program that takes advantage of correlations between maintenance procedures and the CIA Triad will not only assist in operational readiness, but can also provide an invaluable supplement and enhancement to any existing security program. Where no comprehensive security program is yet in effect, a properly instituted maintenance program can provide the basis of initial security for systems and associated data, as well as continuing security support throughout the systems life-cycle. It can also provide opportunity for audit, assessment, remediation, and improvement throughout the organization's security program.

What is a systems maintenance program? (or….let's define our terminology)

The old paperback dictionary gathering dust on many IT professionals desks contains multiple definitions for the word "maintain". The first is relatively obvious - "to keep in an existing state (as of repair)". **(Mirriam-Webster, p. 441)** This is the one we most often think of in relation to a computer maintenance program. Keep the systems up, running smoothly and efficiently, and little else. This is undoubtedly the most commonly presented requirement and justification for instituting a formalized maintenance program. The overall purpose addressed here is ensure that systems operate at maximum efficiency for conducting the normal course of business, and to extend the life expectancy of those systems.

While maintaining the operational status of information systems is a major function of all IT departments, Information Security is of just as great a concern. As such, we will also deal with the less well known, but for our purposes just as important, second definition of the word. "Maintain – to sustain against opposition or danger". **(Mirriam-Webster, p. 441)** The steps we take to protect our

information assets from opposition or danger is the core and purpose of the CIA Triad model, and the basis for any organization's information security program.

Turning semantics into working terminology while maintaining security focus, we arrive at the following definition:

Systems Maintenance Program: A set of policies, procedures, and actions designed to support, promote, and implement the following four maintenance objectives:

1. Keep IT related hardware in good working order
2. Keep IT related software, operating systems, and system environments in good working order;
3. Assure that the status of these systems meets existing organizational, industry, and other accepted "best practices" as they relate to operational and security requirements;
4. Leverage the program as a tool to enhance overall security posture in relation to the CIA model

Within this definition, we can also identify three major categories of maintenance. These are:

1. Preventive Maintenance: Tasks performed on a system to correct or prevent degradation of performance, and to correct other minor issues prior to them becoming larger problems. For many systems, this would include tasks such as disk defragmentation, file system cleanup, minor physical cleaning, anti-virus scanning, and backups. For desktops and laptops, this is often a user level responsibility, although some organizations may assign some portions to in-house IT personnel or outsource vendors .

2. Scheduled Maintenance: This is a system of performing on-going, routine maintenance procedures at periodic scheduled intervals. The purpose behind scheduling routine maintenance tasks such as upgrades, patches, cleaning, and installs is to provide a measure of predictability and to move any expected downtime to off-peak hours. Maintenance of this sort is often required for servers and other infrastructure systems, and is usually the responsibility of in-house IT support personnel.

3. Corrective Maintenance: Maintenance of last resort. The system is broken, and must be repaired or replaced. Yesterday or sooner, will be the users preference. Corrective maintenance can range from a simple component swap to replacement of an entire system. Corrective maintenance may be performed by in-house personnel, outside vendors, or a combination.

Each of these categories will be explored in further detail shortly. In addition, direct links and correlations will be drawn from each in support of all three legs – Confidentiality, Integrity, and Availability - of the CIA Triad security model.

Why is a well-defined maintenance program of even greater importance today?

During the economic boom of the 1990s, many organizations were investing heavily in their information systems infrastructure. Larger corporations instituted programs for mass-deploying new

hardware platforms at 2 to 3 year intervals. Network and desktop operating systems were often refreshed at similar intervals, with many applications being upgraded as soon as new versions were available. As these companies often purchased extended warranties for these systems, the perceived value of formal preventive, scheduled, and corrective maintenance programs became greatly diminished.

But even in the best of economic times and in situations as described above, there have always been a certain number of systems that were either not replaced or were trickled down to others in the organization. We are all familiar with the old 386/486 class machine that was never replaced; it has been held solely to run that single "mission-critical" Windows 3.1 application. We are also aware of the many situations when management gets new "top of the line" computers, and the others roll down to less fortunate users. These situations have always been a support, security, and maintenance nightmare.

In the economic downturn which began in late 2000 and accelerated after the events of September 11, 2001, far more older systems will remain in working inventory for the foreseeable future. Just one year ago, a Computerworld Magazine survey showed that 59% of companies of at least 400 employees planned to increase their IT budgets for 2001. These increases were estimated to average 10%. **(Ulfelder)** However, Computerworld and GIGA are now estimating that 2001 IT budgets will be down by approximately 5% overall, and by as much as 20% for computers and telecommunications hardware. **(Verton)**

As more machines are being kept in service longer, the need for a well-engineered maintenance program becomes critical – both in keeping older systems operational as well as keeping them secure. Initially, an increased maintenance workload may be perceived as a distracter - tapping critical resources away from a security role. However if maintenance functions are properly formulated and oriented, they can and should be a solid foundation and support structure for an overall security program. The initial challenges of designing and implementing a comprehensive maintenance program actually offers a number of opportunities to create or enhance the overall IT security posture of the organization.

How should a maintenance program be designed and implemented in MY organization?

Designing a specific and detailed maintenance program for any particular organization is not the goal of this presentation. To cover the myriad possibilities involving potential hardware and software platforms alone would result in just one more "maintenance, upgrade, and repair" book, and there are already many very good ones. It is also impossible to create a "one size fits all" program, as individual organizational issues, existing policies and procedures, and objectives must all be taken into account. The starting point for any particular set of circumstances would be to refer to the four maintenance objectives described earlier. These, in conjunction with a close examination of your operating environment, maintenance needs, and organizational structure; you will be well on your way to developing the basis of your own maintenance program.

The goal here is to introduce and emphasize the basic but critical principles of maintenance, and how they relate to and support a comprehensive security program. Awareness of these principles, and applying them to your specific environment, while keeping a focus on requisite security, will allow you to engineer a maintenance program that fits your specific needs and requirements. Following the principles of the "Campaigner's Computer Maintenance Mantra" can be an inspirational guide:

> *I must maintain my computer to keep it operating efficiently.*
> *I must regularly conduct system maintenance to prevent errors.*
> *Every month I must check my system for viruses.*
> *I will scan the file system for errors. I will de-fragment the drives if they need it.*
> *I will check the operating system for itinerant temporary files and delete them.*
> *I will delete or copy onto disks unwanted or surplus files in my work area.* **(Mobbs)**

What are the links between a maintenance program and information security, and how does this program support the CIA Triad model?

To establish a direct correlation between specific maintenance concepts and security concerns, we will now examine some specific examples. While this exploration is by no means all-inclusive, it demonstrates the significant impact that a solid maintenance program can have on security issues. Proper maintenance procedures are the method to assist in securing an insecure system, and to assure that a system that is secure today will remain secure tomorrow.

> *No computer system can be considered truly secure if the basic hardware and software mechanisms that enforce the security policy are themselves subject to unauthorized modification or subversion. The continuous protection requirement has direct implications throughout the computer system's life-cycle.* **(DoD 5200.28-STD Req. 6 – Continuous Protection)**

1. Preventive Maintenance. Since this class of maintenance is normally performed by the end user, it is imperative that any training or guidance provided stresses the security ramifications as well as the operational impact on their systems. This could be accomplished via hands-on orientation, instruction provided through manuals or CBT, or a website dedicated to standard user level maintenance. The most critical thing to consider when allowing or recommending that users perform the types of actions outlined here, is to provide adequate and appropriate tools to perform them effectively.

   Newer operating systems may contain utilities which will perform or assist with some of these functions. Windows 98, ME, 2000, and XP for example, contain disk defragmentation, cleanup, and backup utilities. In many cases these built-in tools may be sufficient. In other cases, self-contained tools may not be available, or may be insufficient to meet specific requirements. In these situations, there are many third-party utilities to provide or supplement operating system tool functionality. Packages such as Diskeeper, Norton Utilities, McAfee Office, or OnTrack SystemSuite can provide increased usability for many preventive maintenance procedures, and are available in versions compatible with various platforms. **(Keizer, Mueller p. 1094)**

At a minimum, user level preventive maintenance policies should address the following six general procedures, and orient them toward the applicable hardware and OS platform: **(SFSU, SFSU 2)** (note that many of these processes will be applicable to scheduled and corrective maintenance procedures as well)

A. System Backups: Backups are one item often addressed in both maintenance and security documentation. The importance of regular backup of systems and data is probably the topic most stressed by maintenance and security personnel, yet receives the least actual use from the user level. When both security and maintenance policies reflect a common perspective and provide common procedures, the user will be more likely to finally "get the point" and pay more attention to this critical function. Maintenance and security organizations must then ensure they provide users with adequate software tools, appropriate backup devices and media, storage, and on-going support.

Relationship of backup procedures to the CIA Triad Model:

Confidentiality: To maintain confidentiality of data, backup procedures should address the following areas – access to file systems, secure storage of backup media, protection of media from environmental hazards (water, fire, ESD, etc), encryption or password protection of media, as well as physical and logical access controls.

Integrity: To assure integrity of data, backup procedures and policies must include verification methods for the backup files. This often entails file comparisons made during or upon completion of the backup process (i.e. CRC, hashing, or bit-matching) Provisions should be made for testing the restore process; to ensure users are aware of the procedures, and a final verification that backup media and files are useable and of the expected revision.

Availability: Backups are the last line of defense in any information security and protection program. When everything else fails, the availability of reliable backups is the final measure of comfort and recovery. If no current backups are available in a catastrophic situation, all may be lost (including the job of a system administrator or two!). An adequate backup execution and media rotation schedule is critical for ensuring that an adequate level of availability protection is provided. This schedule should be designed individually for each system, based on the criticality and volatility of the data.

B. File System Maintenance: This procedure can potentially involve several tasks, based on the type of system, and how it is used. A file system or data maintenance policy should address issues relating to cleanup of temporary files and folders, defragmentation of hard drives, clearing cache files, deletion or archiving of outdated files, evaluating the current classification level of data, and file/folder organizational structure. Disk Cleanup in Windows based systems, or a commercial utility package can assist in identifying and clearing unnecessary system and temporary files.

Relationship of file system maintenance procedures to the CIA Triad Model:

Confidentiality: Regular file maintenance provides an opportunity to ensure that files are located in areas which are protected to the level of the data's classification; i.e. not in publicly shared folders, are placed in encrypted or hidden folders, or subject to archiving to removable media. It is also a cleanup opportunity; to clear cache, temporary, or outdated files which may contain confidential information which would present a serious risk if the system is compromised in some way.

Integrity: Periodic disk defragmentation, in addition to improving the performance of a system, can also enhance the integrity of the files on the disk, as subsequent read/write processes involve less movement of disk heads. (note: an unsuccessful or interrupted defrag routine can also corrupt data – a good backup prior to this process is essential). File maintenance also presents an opportunity to scan for any suspect files; which may contain Trojans or other hazardous malware.

Availability: During file system maintenance, files which may have become damaged are identified for restore. Data cannot be considered "available" if it cannot found – organizing files during these procedures makes data easier to locate, and therefore more available. File organization also streamlines processes such as backups and data classification.

C. Basic Hard Drive Maintenance: At the user level, hard drive maintenance seldom involves more than the basic defragmentation described earlier, and the use of basic utilities such as chkdsk, scandisk, or third party utilities such as Norton Disk Doctor. The purpose of these tools is to identify potential defects on the drive itself, attempt to relocate data from those sectors to safer areas of the disk, then marking the defective sectors to prevent their reuse. **(Mueller, p. 1093 – 1095)**

Relationship of file system maintenance procedures to the CIA Triad Model:

Confidentiality: Drive maintenance assists in ensuring that data resides on accessible areas of the disk, and helps prevent premature drive failure through repeated access attempts to defective tracks. In turn, this could prevent the removal of a "dead" drive, which could then be obtained and accessed by unscrupulous technicians with more advanced data recovery tools.

Integrity: Integrity levels are increased by moving data away from defective tracks on the media, helping prevent corruption or loss.

Availability: Marking defective tracks and sectors to prevent their use for file storage helps circumvent potential loss of data due to hardware failure at this level.

D. System Cleaning: Physical cleaning of information systems is usually not considered a maintenance procedure, but can be critical for the health of the system and it's associated

data. At the user level, this usually entails only basics – screen cleaning; input devices such as keyboards and mice; removable media drives such as floppy disk, tape, or CD drives; and removal of dust from internal components. Some concerns with user level cleaning include: availability and use of appropriate cleaning materials, preventing unqualified users from any work inside system enclosures, and potential "wear and tear" damage to components due to over-cleaning. These concerns must be addressed on a case by case basis.

Relationship of system cleaning procedures to the CIA Triad Model:

Confidentiality: As cleaning systems is a necessary maintenance task, yet is relatively simple, the confidentiality of data stored on the system is better maintained if the system user performs this task. Ideally, support personnel are capable and trustworthy, but the more people who use the system, the greater the chance of a confidentiality or other security breach.

Integrity: Proper cleaning of removable media drives, such as floppy drives, tape drives, CD-ROM drives, etc., will increase the lifespan of these devices, and will greatly reduce the likelihood of read/write errors on those devices. A schedule of cleaning these types of devices based on usage levels and environmental conditions should be developed and adhered to. As the cleaning tools for these components may include cleaning fluids and/or abrasives, overuse may result in unacceptable "wear and tear". Periodic cleaning of screens and monitors will also assist in increasing data integrity. Dirty screens produce higher levels of data entry mistakes, due primarily to decreased clarity and increased eyestrain.

Availability: One of the greatest threats to the actual "life" of a computer system is heat. Dust and dirt inside the system case acts as an insulator, interfering with airflow and heat dissipation. Overheating can damage many components, possibly bringing down the entire system and reducing availability to nil. Periodically opening the case and blowing out accumulated dust will greatly reduce overheating potential and increase hardware lifespan. (**Groth p.360**) (note: this also provides an opportunity to verify that cable connections, RAM, inline chips and cards are not loose from "thermal creep" – however this involves a risk of ESD damage, and is not recommended for casual users **(Mueller p. 421 – 422))**

E. Software and Operating System Updates: Patches and updates are released for applications and operating systems on almost a daily basis (especially with Microsoft products, which are by far the most prevalent). These patches may add functionality, repair bugs in the system, or close security holes. Security policies often address the issue of patch management due to the incidence of fixes released due to security issues. However, as many patches are released for other reasons, it should also be addressed within the systems maintenance arena. Within either of these areas or as an overlapping function, there should be a "patch management" program. The purpose of this program would be to evaluate and test patches prior to mass installation, as well as educate users on when and from where to

install updates. Social engineering has repeatedly been shown to be effective in enticing users to load malware under the guise of a "patch". **(Cornetto, Lyman)**

Relationship of patch management procedures to the CIA Triad Model:

Confidentiality: proper and prompt installation of patches assists in closing security holes which allow Trojans to capture and transmit passwords and other confidential data; allow remote access, viewing, or control of a system; or allow other compromise of data.

Integrity: Many patches are released which repair operating system or application errors capable of causing corruption of data. Other patches are released to repair problems in software which could cause various levels of failure, entailing possible data loss or corruption. Prompt installation of these fixes will mitigate this risk.

Availability: Both bugs and malicious software have the potential to destroy data. When fixes are available to correct software malfunction, or to close security holes which allow malware into the system, a procedure for prompt installation is critical to prevent data loss.

F. Virus – Malware Prevention: Like backups, anti-viral strategies are another area that is often currently addressed in both security and maintenance policies. The fact that these areas of interest are already addressed under multiple policies indicates both the high level of concern, and the logical overlap in responsibilities for security and maintenance programs. As there are over 55,000 currently identified viruses with hundreds more each month, this concern is not misplaced; especially considering that the overall cost estimate due to virus outbreaks in the year 2000 is in excess of $17 billion. **(Hansmann)**

The good news is that only about 200 viruses cause the majority of damage, and most can be prevented or stopped by the proper implementation of a well-engineered anti-virus policy. There are several major anti-virus software vendors; Network Associates, Symantec, F-Secure, and Sophos among them. As they are all highly respected and evaluate well in virus detection and removal, the choice of software is not as important as it's proper implementation within security and maintenance programs.

The software should be a standard within the organization for maintenance and support purposes. The application should be patched and updated regularly, and run religiously. Ideally, virus definition files should be "pushed" to users as they are released; alternatively, clients should be set to automatically "pull" new versions from a standard location. Software should be configured to scan all potentially hazardous files.

Relationship of virus/malware prevention procedures to the CIA Triad Model:

Confidentiality: many Trojans and spyware applications are specifically designed to compromise the confidentiality of systems; either by capturing and transmitting passwords or other sensitive data, opening back-door control of systems, or to set systems up as attack

zombies in a Distributed Denial of Service attack. Anything that keeps these types of programs out of systems is support for confidentiality.

Integrity: An infection by a remote control Trojan such as Back-Orifice opens a system up to many possible integrity hazards. A cracker could surreptitiously alter data on the affected system, or use that system to access others on its network for purposes of data diddling. Alterations of this sort may not be discovered for some time, and could potentially be more costly than the actual destruction of the data – the changing of financial or payroll information, for instance. If systems are susceptible to this kind of attack, data integrity can never be assured.

Availability: The great majority of destructive viruses currently found in the wild carry a payload aimed at corrupting or destroying data. Depending on the particular circumstances such as backup availability and value of the data, this loss can range from a mere nuisance to a catastrophic event.

2. Scheduled Maintenance: Scheduled maintenance normally entails routine procedures aimed at upgrades, patches, cleaning, and installs for servers or other infrastructure equipment; but can apply to "personal" systems as well. As this class of maintenance is usually the responsibility of IT support personnel, it should normally be accomplished at a higher level of control, detail and documentation than user preventive maintenance. This allows a much tighter integration with existing security procedures, but can present some potential security risks as well.

3. Corrective Maintenance: Corrective maintenance can range from a simple component swap, to replacement of an entire system in order to bring a broken system back on line. Corrective maintenance may be performed by in-house personnel, outside vendors, or a combination of the two. In most respects, the security ramifications of this type of maintenance are very similar to scheduled maintenance, so they will be dealt with here together.

Upgrades and replacements, whether software or hardware, should be evaluated and tested prior to installation for any potential security ramifications. This evaluation should be done along the lines of a life-cycle assurance program; to ascertain that changes being made are authorized, performed properly in accordance with manufacturer's instructions and any other applicable recommendations, do not degrade the security posture of the platform, and do not introduce any new security risks into the system.

> *Life-cycle assurance refers to steps taken by an organization to ensure that the system is designed, developed, and maintained using formalized and rigorous controls and standards. Computer systems that process and store sensitive or classified information depend on the hardware and software to protect that information. It follows that the hardware and software themselves must be protected against unauthorized changes that could cause protection mechanisms to malfunction or be bypassed completely.*

(DoD 5200.28-STD 5.5.3 Assurance)

In addition, procedures should be in place to maintain data integrity during the work process itself. This may involve performing backups prior to commencement of work, documentation of settings prior to change, recovery checkpoints to use in event of failure, or "fail-safe" procedures that may be platform or system specific. In the event of disruption or mistakes during the process, these protection mechanisms could make the difference between recovery and catastrophe.

> *As appropriate, the computer installation will have defined procedures for maintaining data integrity during hardware repair, will set up a schedule of preventive maintenance for the computer system, and will maintain a log of hardware malfunctions.* **(UNT)**

The importance of proper documentation during scheduled/corrective maintenance must also be stressed. Any changes made to systems could have an effect on existing security and operational parameters or on future enhancements. Without adequate system documentation, other technicians will be at a great disadvantage for any changes need later.

Confidentiality Issues to address with Scheduled/Corrective Maintenance:

A. Technicians may be exposed to data to which they would not normally have legitimate access. They must be keenly aware that they are obligated to protect that data from further disclosure, and they are not to "explore" any further than necessary to accomplish their tasks.

B. Outside vendors may be involved in these types of maintenance as well. Policies and procedures must be in place to prevent any unnecessary disclosure of sensitive information to these personnel. The procedures could include physical escort, non-disclosure agreements, and physical and logical access controls.

C. Established procedures must be in place and followed for the proper disposal of any removed or replaced components, especially hard drives or other media. Just because a drive is "dead" in the current system configuration, does not mean that data cannot be recovered from it by a skilled and dedicated technician/hacker.

D. In-house and outside technicians should be monitored for any malicious activity which could present a threat to data, system, or process confidentiality.

Integrity Issues to address with Scheduled/Corrective Maintenance:

A. Many types of maintenance may result in damage to data if performed improperly, or if the system "hangs" during the process. To prevent corruption or destruction of data, system

settings, or other parameters; procedures should be in place for backups prior to implementing the changes, and for fail-safe checkpoint mechanisms during the work.

B. Strict adherence must be maintained with manufacturer instructions, organizational policies and procedures, and industry "best practices" to prevent improper maintenance work from causing further problems in the system.

C. Pre-existing configurations should be well documented prior to commencing work, including both hardware and software settings. This is necessary both for rollback, updating final system documentation, and for preservation and recovery of settings in event of problems.

D. Whenever possible, hardware and software changes should be tested thoroughly for potential risks to data integrity and other security issues prior to being implemented on a production system.

E. Technicians should be monitored for any accidental or malicious activity which could result in a compromise of data integrity.

Availability Issues to address with Scheduled/Corrective Maintenance:

Scheduled and corrective maintenance procedures are normally implemented for the express purpose of enhancing or reestablishing the availability of systems and their associated data. As such, availability could be considered the "Prime Directive" of these types of maintenance. Taking the proper precautions outlined earlier, and verifying that documentation is completed to prevent future problems, will ensure continued availability.

How else can a well engineered maintenance program support a security program?

WARNING: the acceptability and legality of some of the actions suggested here may be contingent upon the wording of other existing policies, regulations, or statutory restrictions applicable to your organization. Prior to implementing any of these actions, verify that they are legal and acceptable in your particular setting, and make sure that *management approval is granted in advance, in writing*. Performing these actions in the absence of a concrete policy and management approval could result in legal exposure for the technician.

In addition to the inherent qualities described above, in which maintenance bears a direct relationship to security, proper orientation of a maintenance program may provide many other opportunities to augment and supplement security policies and procedures. An opportunity is presented for verification of adherence to standard security practices, installation of proper software, and audits of varying levels. It must be emphasized, however, that most support technicians would not be capable of, nor expected,

to perform some of these functions. Only proper attitude, training, assignment of responsibility, and management support would provide the proper justification and guidance.

Auditing opportunity: Anytime that a computer system is due for maintenance of any type, a prime opportunity is presented for audit of that system. This audit could entail a simple verification of standard software load, a check for any unauthorized/unlicensed software, an in-depth inspection for the presence of unacceptable software, files, or malware, or an audit of access and traffic logs. Audits anywhere in this spectrum could be performed as a standard procedure or under conditions of "probable cause". It is *essential* that policies be in place to address any "unfavorable" results of these audits..

Verification opportunity: When systems are undergoing maintenance is an excellent time to verify that all necessary software, updates, and patches are installed. Verification of backup status, current virus definition files, and installation of critical security "hot-fixes" would be the focus of this type of check. Correction of discovered deficiencies could also be addressed at this stage.

Training opportunity: Often, the reason a system is down for unscheduled maintenance is because of user error or misuse. As such, an opportunity is presented for informal or formal training of the user – both for maintenance and operation of the system, and for the security "focus of the day".

Summary:

In the preceding sections, we have examined six sets of procedures, all commonly associated with user level preventive maintenance. Each has demonstrated a direct correlation to all three legs of the CIA Triad – Confidentiality, Integrity, and Availability. All provide critical prevention and remediation capability to mitigate various security risks, and to correct and recover from active threats.

We have also looked at scheduled and corrective maintenance, and examined the effect that these programs can have on an overall security program.   We can see that this type of maintenance also has a major impact on the CIA model, and in the case of Availability – actually *embodies* the model.

What can be gathered from this? If an organization has absolutely NO official security program in place, then a well engineered user level maintenance program will provide a solid security foundation to build upon. Where there is a security program in place, these maintenance procedures, if properly implemented and executed, can provide an invaluable adjunct and support structure to that program.

The keys to making this work to the advantage of security are awareness and training. Users must be trained to perform their tasks as they relate to the systems they use, and must be constantly and consistently reminded of the benefits they derive. A "normal" user will not take the time to perform a full disk defragmentation based on the concept that it makes data more secure. Demonstrate to that same user the 5 to 10% performance gain that can be realized by periodic defrags, and they will do it twice as often as necessary! Similar approaches can be utilized for many standard maintenance tasks.

By the same token, support personnel must be made aware of the potential security ramifications of modifications which may be made in the course of their duties. Failure to follow established maintenance procedures and best practices or failure to properly document system changes could introduce unnecessary security risks into the system. Proper adherence to accepted standards, however, provides on-going support to security as well as to operational readiness.

By no means has a comprehensive plan or program been outlined here. These are merely the basics; which must be oriented, expanded, tuned, and customized for a specific environment. At that point the beginning of a real maintenance program will begin to take shape. If properly designed, properly oriented with emphasis on the relevance of the CIA model, and properly implemented; that plan will be both a firm base and strong support for a solid security program. Then systems maintenance will no longer be the "forgotten foundation", but the "active foundation" of the CIA Triad security model.

Source References:

Cornetto, Jon. "Bogus E-mail Patch Reported for Microsoft Outlook". (13 Aug 1998).
http://www.pcworld.com/resource/printable/article/0,aid,7768,00.asp (2 Jan 2002)

DoD 5200.28-STD. "Department of Defense Trusted Computer System Evaluation Criteria Security"
(Orange Book). (26 Dec 1985). http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html
(4 Jan 2002)

Groth, David. A+ Complete Study Guide. Alameda, CA. Sybex Inc. 1999.

Hansmann, Bob. "Lessons Learned – New Security Threats Change Anti-Virus Software for the
Better". http://www.ispworld.com/bw/nov01/Lessons_Learned.htm (5 Jan 2002)

Keizer, Gregg. "OnTrack System Suite 3.0" (review and comparison). (11 Dec 2000).
http://www.cnet.com/software/0-806176-8-4059554-1.html (4 Jan 2002)

Lyman, Jay. "Bogus Alerts Highlight Phony Security Postings". (18 July 2001).
http://www.newsfactor.com/perl/story/12084.html (4 Jan 2002)

Mueller, Scott with Zacker, Craig. Upgrading and Repairing PCs Tenth Anniversary Edition.
Indianapolis, IN. Que Publishing. 1998.

Merriam-Webster. The New Merriam-Webster Dictionary. Springfield, MA. Merriam-Webster, Inc.
Springfield, MA. 1989. P. 441

Mobbs, Paul. "The Campaigner's Computer Maintenance Mantra". (7 Dec 2001).
http://security.tao.ca/mantra.shtml (5 Jan 2002).

SFSU – San Francisco State University. "Recommended Computer Maintenance for Windows
95/98/ME/NT4/2000". (31 May 2001).   http://www.sfsu.edu/~helpdesk/maint/pc-maint.html
(4 Jan 2002).

SFSU 2 – San Francisco State University. "Recommended Computer Maintenance for Apple
Macintosh Systems 7.x-9.x". (10 Dec 2001)
http://www.sfsu.edu/~helpdesk/maint/mac_maintenance.html (4 Jan 2002).

Ulfelder, Steve. "Paying for IT 2001". (18 Dec 2000).
http://www.computerworld.com/storyba/0,4125,NAV47_STO55252,00.html (26 Dec 2001).

UNT – University of North Texas. "Policy Manual - Computer Resources Security Standards".
(August, 1997). http://www.unt.edu/planning/UNT_Policy/volume2/3_7.html (4 Jan 2002).

Verton, Dan. "Conservative year ahead for IT budgets". 26 Dec. 2001.
http://www.computerworld.com/storyba/0,4125,NAV47_STO66958,00.html (26 Dec 2001).