NETWORK AND MANAGEMENT ERRORS

Ali Daneshmandnia
71 Willow Gate
Roslyn Heights, NY 11577
daneshmandnet@gmail.com

Abstract: Having a robust, dependable, adaptable, and secure network is fundamental requirement of any Information Technology infrastructure. Errors can have devastate consequences on the entire IT of the organization. Error by an IT professional can have major consequences for the entire organization. In this paper I have presented various types of human errors in relation to computer networks and their possible causes. I have discussed possible solutions and preventive measures for each category of the errors.

Keywords: Human Error, Network Error, Errors by Network administrators,

Making error by an IT professional can have major consequences for the entire organization. I have tried to explore the types of errors that we would encounter in a computer network environment of an educational organization. To make this paper more meaningful, I conducted interviews with some of the personals of two different colleges in New York. In search of answers I tried to interview some technical and non-technical staff. All individuals that I interviewed, work with students, faculty and, staff of the college either directly in IT departments or indirectly as lab supervisors, test proctors and academic advisors. I have presented the areas that I have seen human errors and I discussed the solutions to each problem through research and interviews.

Developing a friendly user interface

Jetona Levnug, an aptitude and admission test administrator at Globe institute of technology located in New York City, believes that 50% of the human errors in the assessment of prospective students are related to giving the wrong type of exam. She says, "When a new prospective student approaches me for an aptitude test, I can give her/him two different tests, usually referred as form one or form two. Most of my mistakes take place here and I end up choosing the wrong test." As Jetona explained, form one is given to a student who is taking an aptitude test for the first time while form two will be given to the students who have already taken the test and did not pass. She added "I make error while choosing different object from the menu." Milosh, another test administrator from Globe says that "After giving the wrong test to the applicant, I might realize so I would apologize and I would give them the correct test, forcing students to retake the exam. This makes them frustrated." According to Jetona, the cause of not giving a correct test to prospective students is due to design of interface software and partly because of not looking at the admission application that the student hands in to be tested. When the test proctor gives the wrong admission test to the prospective student, S/he has to interrupt the student and asks him/her to retake the test. This causes many problems such as having more than one result for student, and making the student frustrated and tired which leads to receiving an inaccurate test score. Milosh Suggest that to correct such problem we have to redesign the forms so the proctor can distinguish the main part of the form, such as students name, type of test and number of times that the student have taken the test already.

Errors made by network administrators

In the Microsoft network environment, users are usually associated with a domain. A domain can be associated with other domains as a child domain or parent domain. However, when an active directory domain controller is upgraded to a newer release or when we try to recover after a crash, a complete test of new active directory server will ensure that we will not have any surprises such as corrupted accounts. Antonio Solano, the network administrator at Globe Institute, thinks that the human error can cause many unnecessary corrections. He says "in one situation, I had to migrate user accounts from a crashed MS domain controller 2000, to a MS 2003 domain controller. Instead of copying my documents and desktop for all users, as a precaution, I copied the entire users' data including the data base to the new Primary Domain Controller (PDC), not knowing that the data base was corrupted. This resulted in copying corrupted database to the new domain controller which corrupted many accounts. According to Antonio Solano only user desktop and My Document folders needed to be copied. These types of errors which are happened everyday can be avoided if research or consultation with the vendor is done prior to engagement of such projects. Periodic training for Network ministers are extremely important to keep up with new versions of network operating systems.

Password Security

Some times network administrator try to make the work environment very user friendly by allowing the users (often mid to high level management) stay with a very easy password, such as their name, for ever. In reality the network administrator is not following basic security policy of a network which requires users to use strong password quality with the minimum length, composition and a limit on the age of password. When I raised this issue with Boris Kuminesky, a network administrator from School of
Manhattan Technology located in New York City, he believed that novice users are often confused as to what the network prompt means. He says that "when the network server forces them to change their password after 90 days, many of the users will get confuse. He explains "when Domain Controller ask for the old and new password, end users tend to reenter their current password as new password and the Domain Controller does not allow that and as a result I have to stop enforcing strong password in password policy."

According to a new report form DTI (Department of Trade and Industry of UK) most people never change their passwords and a third write them down on a paper.(Millman, 2007 1) The IDT study also found that about two third of the 1800 adults questioned never changed their password. Malcolm Wicks, the minister of Science and Innovation in UK, maintained that in a survey that was done, they found that the UK lost ₤ 440 million to credit card fraud last year and 62 percent of companies experienced network security incidents. He believes that "large number of people was careless with passwords, unwittingly exposing themselves and their company to fraud and theft" (Millman 3). This brings up the need for ongoing training for the users. End-user enrichment in working with computer must be ongoing. The IT department should conduct training classes in various areas such as security, messaging, group collaboration, and application software. In a survey that was done by CompTIA (Computing Tech Industry Association) only 29% of 574 organizations surveyed said that information security training is required at their company. (McCarthy 2006). Among those about 84% said that such training has resulted in a reduced number of major security breaches. System administrators should never overlook security policy under any circumstances and grant additional privileges to certain employees based on job titles.

Lack of documentation

Lack of documentation can lead to initiate human errors on the computer networks especially by the administrators. When an administrator solves an issue, they should take time and write about the problems and solutions. Compiling and organizing these issues and their solutions in a knowledge base would help the organization to expedite their trouble shooting procedures by looking up the knowledge base. Many technical staff get involve with solving the problem and they do not take the time to document their findings and solutions. Error reduction intervention includes: clear documentation practice such as employing a knowledge base system to log all events and solutions which must be implemented by all IT staff starting from help desk all the way up to the manager and directors. Other areas that cause human errors due to lack of documentations are lack of proper labeling of network devices and cabling systems, and absence of updated network diagrams.

Using Systematic Human Error Reduction and Prediction Approach (SHERPA) to predict errors and reduce them

Donald Norman (1981), who wrote many books and article on psychological research on human-computer interaction, performed a research to determine the psychological theory behind why professionals make mistakes. According to Norman " if action is directed by schema(organized a memory units), then faulty schemas or faulty activation of schemas will lead to erroneous performance."(qtd. In Stanton 374) According to his theory errors can take place if we select wrong schema for misinterpretation of data, or because of similarity in the triggering condition or, finally if schema activated because of wrong timing. According to Jacob Stoller, who is an independent writer and researcher based in Toronto, sequential step-by-step checklist-type tools will clearly prevent much of these kinds of errors. (Stroller 79) Barry Kirwan (1992), who researched human error identification for air traffic control and human reliability assessment, feels that SHERPA is the ideal approach to predict human errors. Kirwan says: "combination of expert judgments, used together with SHERPA's technique produces the best available approach to confront human errors." (qtd. In Santon 378). I have used the SHERPA method to create an error predication approach for installation of Network Operating System of a MS server 2003. Two tables have been developed: table 1 shows the errors and what category they belong to and table 2 shows the SHERPA table predicting the errors of a typical network server installation. In Table 2 common task in a networking environment was used to predict errors that might happen and present solutions for each case. The solution for each case is based on MS 2003 server installation guide and consultation with various network administrators who were interviewed earlier on this paper.

Errors associated with Email servers

EMAIL Services

Email servers are one of the most important components of an organization. When the email server is "down" that can spell trouble for the IT group. Email services must be reliable and operational on a 24/7 basis. There are many measures that we can take to ensure email servers' functionality and high availability. Following are a small list of suggestions on how to plan to confront possible human error and to be ready if the email server failed:

- We must have a robust backup system in place which is tested weekly (just part of the backed up data) Tapes should be kept off site in case of any problem such as flood, fire and so on.
- We must use fault tolerant server with fail over solutions. Fail-over could be in form of a cluster of servers, so if the main one fails another one will take over.
- The fail over solution must also be highly available. There are many products in the market which synchronizes two identical servers via point-to-point T1 or T3 lines and ensures that if a server becomes unavailable due to human error or any other reason, an exact one will be on line remotely, preventing any loss of service or data.

Even if there is a delay in which there is no email services available, all email send to the server while the server is down, can go to the internet provider's (ISP) servers. When the company's email server goes back on line all diverted emails will be copied from the provider (ISP) server back to the company's email server. In some other application software, we may prefer consistency of operation of the server over lost of data. So deciding how to cope with human error is based on application. Aaron Brown, a researcher in Adaptive Systems department at IBM, developed a prototype of human-error-undo mechanism for email servers which all IMAP and SMPT traffic were logged. When a human error is discovered, the email is rolled back to a latest snapshot, and then replays the logged mailbox update stream. (Brown 5) There is several software such as Symantec System Recovery 7.0 which takes snapshot of a server and can restore it on a different hardware platform. (www.symantec.com)

Since we use email on daily basis, we must take the initiative to educate users as an ongoing basis and enlighten the users about do's and don'ts. According to Chad Dickerson from Info Week online journal, one of the UK largest bank send an email to 2,600 customers where all recipients email addresses were visible to everyone else on the list. (Dickerson 34-41) This error can be easily avoided if the users had regular training on sending out mass emails on company wide email system. Of course, we don't know if the person who sends the email was being supervised or the manager just left the task to a staff member. If the latter scenario was the case, then the manager is at fault. Such important task must be handled by a manager who's technically savvy and will be able to evaluate all possibilities for error in advance.

Inappropriate Access privileges for users

In regard to access privilege sometimes certain ordinary users may have extra ordinary privilege on a network. This is extremely dangerous. According to CERT and US Secrete service, 87% of insider security breaches were achieved by simple unsophisticated users who happen to have much more privilege rights that they needed. (Dickerson,2004 36) TO avoid such problems, IT must have clearly defined guidelines and policies, which is applied to all employees regardless of their job titles. These guidelines will be followed by the IT staff that is ultimately responsible for any breach of security. According to Security Director Report publication, the IT or Information Security of an organization should conduct a comprehensive audit of how employees interact with security. Timothy Brandon, Security manager of a US army installation believes that security can not succeed without the active support of the users of the system. (qtd. In Security Director's Report) He says "There are countless cases of modern high technology security systems …that turn out to be worthless because the user doesn't know how to operate them, becomes frustrated and end up ignoring or circumventing the system."(3).

Once again, we are reminded about the importance of training for the new technologies, which the organization has acquired.

An important measure regarding security of data and program of a company is not to assign password to users that never expire. Instead as a matter of policy there must always be some type of deadline for the password accounts. Network administrators should not rely on the memory to remember to disable staff's access upon their departure from the company. Instead, removal of users' account must be handled via software. When an employee depart from a position, the supervisor must notify the IT department by executing certain programs that is available to the supervisor, so the IT department will be notified and all privilege of departed users will be terminated or suspended.

Typical management errors

IT staff and engineers must adhere to rules and guidelines of company when they want to administer mission critical events. IT engineers should never test their ideas on production servers. No matter how talented a senior engineer is, he/she should not be allowed to implement new changes without consulting the manager and other technical staff. Testing a newly developed system is job that must be done by Quality Assurance (QA) testing team and not by the developers. Leaving the job of testing to those who developed the system would not get the usual evaluation that we would get from the QA staff (Dickerson 38). Paul Eisen director of the consulting services group at CIBC which helps banks to confront human errors believes that human error reduction begins when you first purchase an application. (Stoller). He says "Step number one include usability issues, which include effectiveness and minimization of errors as key criteria in your purchase decision." (2) Eisen insists that Vendor who is selling the application should show how and where the software was tested and what were the results. Perhaps the key factor behind accurate testing is that designers, operators and/or end users think differently. According to Graham Creedy, a senior manager of responsible care for the Canadian Chemical Producer's Association: "Typically, when something new is being designed, the designers are operating at the knowledge based level. They're got the knowledge to know what's going on, but they're sort of exploring themselves to work out how best to operate it." (Stoller)

Releasing a network project for use without adequate QA testing could be disastrous, and it could cost a manger his or her job. In case of security implementation, an outside security company can be hired to properly test the system and effectively report their findings and make appropriate suggestions to the management.

When we want to determine network performance, we should perform different types of tests to determine the network performance while focusing on ports, links, and client utilization. We can then use the result from tests to arrive at a calculated judgment to measure the network status on various ports of switches, routers, and evaluate whether we have to increase bandwidth or balance the loads on the switches and other network equipment instead.
Important security update must be done during the time that the network is least busy. Sometimes IT managers misinterprets the slowness of IT activities to lack of bandwidth while all it is needed is to shift certain activities such as update of servers to a low traffic time slot. It is not wise to delegate tasks continuously to subordinates and relying on them that they do the job without any need for close supervision.

Professional IT administrators will make errors

In a test that was done by Arron Brown, a simple experience was carried out using RAID (Redundant Array of Inexpensive Disks) by strong savvy network technicians who were trained as system administrators and were assigned to the test systems and were given the responsibility of repairing any disk error as it happened. (Brown 1) The experiment was set up as series of trials and simulated stop failure on one disk in the RAID volume. The result showed that 10% of all Linux OS system ended up with a fatal error. For systems that had Window and Solaris the result was from 8 to 23 percent for fatal and non-fatal error. (7) One way to try to reduce these types of errors is by designing wizards and user friendly programs for many of network tasks, such as creating new employees, which includes creating user accounts, creating email accounts, and so on.

According to Reason, psychologists report that 70 to 80 percent of errors can be detected immediately after they are committed even if they can not be anticipated (Reason). As Arron Brown indicates in his article titled, coping with Human Error, buffering build-in email system is a good solution to allow users to correct themselves even after they click the send button. Although this allows the sender to self-correct or cancel the email if error occurred, but this kind of solution will work in a synchronous environment and it will not work when the application is interactive. (Brown, 2-5). One way to confront the human error is to have replica of the computer system that is running. RAID is a perfect example where if a disk set is damaged or encounters fault, another disk can take over. Other example would be implementing a cluster of servers so when the server fails the other in the cluster takes over. An example of this is Micro Soft Exchange environment. Another protection against error is to have replication of server's snapshots stored on the network file server. This type of software, can make regular replication of servers and desktops based on a schedule and store them on a network file server. Once a server fails we can restore the exact image of the server, even on a different hardware platform than the original one. The down side is that the replicated server lacks accurate up-to-date data so it should be combined with backup solution. If a server crashes we can restore the newest snap shot of the server and then update the restored server with real time data from differential backup.

Disaster Recovery

Disaster recovery is undoubtedly one of the most important, if not the most important, step that an organization should design and implement as a multi line of defense philosophy to combat human error in a computer network environment of an organization. Although this is a vast topic, but I will try to explore it since it is vital to have a well constructed disaster recovery plan in place at all time. Following are summary of few different measures that I think will impact how we can recover effectively with no loss of data if a human error or equipment failure caused one or more server in our LAN to malfunction or to shut down:

- A through plan which identifies all mission critical application servers and the bulk of information that are updated constantly. The plan should be developed in a way that it addresses servers based on the balk of data and frequency of the server update. Some servers such as data base are constantly being updated while other servers such as DHCP may not get updated constantly.
- Multiple solutions should be implemented such as local and remote replication and snapshot images of servers that are done locally and remotely must be saved and available upon need.

- There is also software available from Computer Associates, EMC Corporation, and others which can be used for fail over for high availability (HA) servers over the WAN. With lower cost of T1 and T3, it has become very affordable to implement these kinds of solutions. According to Mehran Hadipour, former VP of marketing at Kashya (which was aquired by EMC in 2006): " A next generation data protection application such as Kashya's achieve no data loss by making an up to date copy of the data available at the remote site…" (Had pour 4) With a reduction of cost of bandwidth for T1, T3, and cost of servers, these solutions have become very affordable now.

A company should really examine this software before adopting them since that startup and operational cost could be high. Chris Woods points out using a Highly Available (HA) failover protection solution provides the cost of a joined-up disaster recovery strategy and its cost will pay off when a disaster occurs. (Wood)

Training

The mission of an organization in confronting and controlling human error, should be installing measures in place to address it at the root level. As I have discussed in this paper, an effective, frequent, and robust training philosophy is a key to control human error. In a survey which was conducted in 2002 by Ill-based global association of Computing Tech Industry Association (compTIA) discovered that human error defined mainly as a lack of adequate certification and training, is the root cause of lax IT security at most corporations. (Dwyer) This survey which was titled "Commitment to security Benchmark Study" found that even though as organization placed more emphasis on security practices and procedures; as well as spending more fund on preventive measures (on human errors), but because of lack of investment on training, the overall return on investment was not realized and security improvement did not happen.

The result of this survey revealed that 60% of 900 organizations which participated in the survey indicated that lack of training led to at least one major IT security breach which resulted in loss of confidential information or interrupted business operation. (Dwyer)
John Ventor, president and CEO of CompTIA says that "human knowledge and action are critical to making networks and IT infrastructure secure. "(Dwyer) A proper training which should lead to certification should be robust, increase awareness, make use of organizational investment in new security technology to the fullest and ultimately reduces the human error.

Voice over IP systems

VOIP have become very popular because of the saving on the telecommunication costs as well ease of management and convenience that they offer. VOIP requires a broadband internet line such as T1 or T3 lines as well as one or more dedicated voice T1 line. They offer server-based Voice mail system with many possibilities such as:

- Unified messaging, which allows user receive their voice mail in form of wave file in his/her email.
- Call accounting system: This is a comprehensive call accounting system which can be used by sales managers, for example. The sales manager can determine if their sales team are meeting minimum call quota, and can generate reports on calls that were made from different extensions for various purposes such as conducting survey, generate various phone related analysis and many more.

- An elaborated caller id interface which appears in the desktop of the user as s/he receive and make calls.
- An IT staff can install IP-phone for any employee as long as s/he has a desktop with network connection, eliminating the need for running phone lines and installing phone jacks.
- Installation of phone extensions at several remote sites which eliminates the need to install PBX at the remote locations.

On a typical phone system we will have a PBX system with computer processors which contain IP cards, to which all IP phones connect to, and computer servers which manage all phone applications including Voice Mail (VM), caller ID application and other special application specifically for phone communication management. The down side to VOIP is its dependency to internet , unlike the digital phone which requires POTS lines. Quality of voice outside of the company location may not be optimum because we depend on internet, unless we install dedicated channel (such as T1) on all locations. As with any other IT field, human error can create disastrous results. VOIP vendors who deploy phone equipments and computer hardware and software which go along with it, usually manage the entire system exclusively without getting the clients involved. This includes installation of phones, computer hardware, software, and support. But this affair does not always go smooth. In one case that I was directly involved, I learned that the local dealer of the VOIP system mishandled the installation by ignoring to secure the Voice Mail (VM) server by antivirus and antis Pam software. In this particular case, the vendor agreed to install a VOIP system by upgrading an existing PBX with a much newer robust processor, while reusing the older phones, and adding new LIPU cards for new IP phones. While this was a smart choice because we would not rely solely on IP phone (the digital phone does not depends on company's LAN), we left the installation of phone system and its subsequent maintenance to the vendor without being involve in either phase. Unfortunately vendor used public IP address on all equipment, LIPU cards, and on the servers that used for voice mail and other phone applications. The vendor did not install any anti virus, antispam or any other security feature on the servers. Moreover the vendor did not have any solution in place for the backup of VM server. After some times the VM server was infected with viruses and Trojan horse and it became extremely slow which affected the voice mail. Although the system was cleaned and firewall, anti virus and backup systems were installed, but the organization experienced many instances of disabled VM which caused the lead (main) number of the organization which is usually pointed to the VM server, to ring busy for all caller, not a good situation to be in peak of the work day hours. Lesson learned form this ordeal is that the Network engineer and managers must make sure that services which is maintain by vendors are secure and client must be inform of how the vendors is protecting data and securing it. In the above case the error which was made by the telephone vendor was as result lack of planning and human error.

Conclusion

Undoubtedly human error is and will be the cause of many incidents in network environment. Our goal in protecting computer network resources should be design and implementation of networks with multiple lines of defense to confront human error. First and foremost defensive strategy is to avoid making mistake. To enforce this we can use automation, as much as possible, clear and error-free interface and most of all continues and robust training. Next we should use variety of methods to combat and cope with human error without loss of

operation and data. These techniques includes implementing buffering in certain applications such as email, where users have chance to rectify themselves even after submitting their works; creating images or snapshot of servers and saving them for rollback if need arises; using virtual Machine to run multiple copies of servers; using cluster of servers to run multiple copies of same servers simultaneously, and implementing verifiable high availability solution for crucial servers. Finally an extensive reporting mechanism should be in place in order to inform all concern individuals and to get them involve in improving the techniques and measures of coping with the human errors.

References

Brown, Aaron. "*Coping* with Human Error*." Error Recovery* November 2004 2:8

Dickerson, Chad "The Top 20 IT Mistakes", *Infoworld.com* November 22, 2004

Dwyer, Steve. "Lack of training: Root causes of most IT security lapses." *Insurance*

Networking News Executive Strategies for Tech Management 7-10 May 2004

Haddeus, Jude. "Disaster Strategy: Bring continuity from Calamity." *Computerworld,* February 12, 2001.

Hadipour, Mehran "Addressing the challenges of data protection; key data must be 100% reliable, accessible and up-to-date". *Computer Technology Review*. Jan 2004: 34(2).

Kirwan, B. "Human error identification in human reliability assessment." *Applied Ergonomics*, 1992

McCarthy, Brian, "Close the security Disconnect between awareness and practice" *Electronic Design* Sept. 2006

Millman, Rene. "Human Error biggest threat to computer security", *Information security News*; 19th June 2007.

Reason, J. "Human Error." Cambridge: Cambridge University Press. 1990.

Rist, Oliver. "Enterprise Windows: Top six steps toward disaster-recovery" *InfoWorld.* April 2006

Stanton, Neville A. "human computer interaction handbook" London: Lawrence ERL Baum Associate.

Stoller, Jacob "IT downtime: assessing thee human factor; A number of recent studies cite human error as the largest cause of centralized IT failures." *CMA Management* November 2005.

"Tactics to prevent human error from thwarting security". *Security Director's Report* October 2004: 4.

Wood, Chris. "Analysis- It's time to go back to backup. Businesses are being forced to tale a second look at their storage solutions" *Computer Reseller News* January 16, 2006.

Wood, Scott, Kieras, David. "Modeling Human Error for Experimentation, Training, and Error-tolerant Design" *University of Michigan* .

TABLE 1- Error Modes and their descriptions

Error Mode	Error description
Action	
A1	Operating System CD not readable
A2	Computer name not unique
A3	Static IP address not unique
A4	IP address assigned by DHCP Server not recommended, for server must assign static address
A5	Hard Disk format fails
A6	Raid controller driver not available
A7	Security update is not installed
A8	updated service pack is not installed
Information Retrieval	
I1	Proper Driver not available (for devices such as NIC, sound card, video card, chipset)
I2	Device manager of OS shows error associated with a particular device by placing "?" next to device, information not obtained
Checking	
C1	Check for correct CD inside
C2	System freezes during copy system files
C3	Check for bootable CD inside CD ROM
C4	Wrong BIOS setting, wrong boot order for boot device
C5	Check if the server must be added to Domain OR designate as stand alone
Selection	
S1	Not bootable CD inside
S2	Correct networking protocols not selected
S3	Wrong selection of format used for User ID and Password
S4	Wrong date and time Zone is selected

Using the SHERPA approach, I have developed the following table which shows what actions to take when we encounter problems during installation of a network server:

Table 2 The systematic Human Error Reduction and Prediction Approach (SHERPA) for installation of a network server

Error Mode	Error Desc.	Consequences	Recovery	P	C	Remedial Strategy
C1	Fail to insert CD into CD Rom	Can not proceed	Immediate	L		Make sure the proper installation CD is in the CD ROM drive
C4	Bios fails to Boot from CD Rom	Boot order may be incorrect	None	L	!	Restart system, boot to BIOS, set boot order to CD, then HD
A5	Faulty Hard Disk	Can not continue	None	L	!	Replace HD with new HD (raid, hot swappable)
I1	NIC device driver not available on NOS installation disk	Can not continue	Immediate	H	!	Download NIC driver from manufacturer web site
A1	CD not Readable	Can not proceed	none	M		Replace the damage installation CD with a correct CD
A2	Server name not unique	Duplicated name exist in the network	immediate	L		Change the server name to a meaningful unique name
A3	IP address duplicate exist	Can not proceed	immediate	M	!	Use static address that does not conflict with existing IP addresses consult DHCP for list of all Static addresses
A4	IP address must be static	Will be able to continue	none	L		A server must have static address and not dynamic.
A5	Hard Disk format fails	Can not continue	Immediate	L	!	Perform an extended format and if problem persist HD must be replaced
C3	Server does not boot using CD Rom	Can not continue	immediate	M	!	The CD that is left in the CD ROM drive is not bootable CD. Replace with bootable CD and restart.
S2	Server does not respond to network command	Certain network function may not work	None	L		Certain network protocol may not be installed during the installation of server. Must use custom install not express install to select all intended network protocols
S3	Wrong format of password used	Can not proceed	Immediate	L		Proper format must be selected. Certain special characters may not be used, space bar may not be selected, A strong password should be used
I2	Upon completion of NOS device managers show error on certain devices	Will be able to continue	None	M	!	Certain devices within the server may not work; ex: sound card, modem, etc. Troubles shoot all devices with “?” reload device drivers and confirm the functionality of these devices from device manager
S4	Proper date/time/time zone is not selected	Will be able to	none	L		Ensure that correct time zone is selected for the server

		continue				
A7	Security update not installed	Will be able to continue	none	H	!	Consult the Network OS web site and update the latest security patch for the server
A8	Updated service pack not installed	Will be able to continue	None	H	!	Ensure that the latest service pack (for MS OS) or any necessary patch is installed
C5	Server was not added to the domain controller	Will be able to continue	Immediate	L		Using Domain administrator privilege join the server to an existing Domain controller or similar enterprise server

Legend: P= Priority L=Low M=Moderate H=High