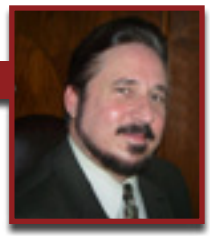
technical® SUPPORT

Supporting Enterprise Networks and Operating Environments

JUNE 2010 VOLUME 2, NUMBER 2

VERBAL and Written Communication Skills for Technology Professionals

Leveraging Virtualization to Automate Your Help Desk



Message from the President

NasTeC Conference is Coming to Chicago in October

In case you're wondering, NaSTeC stands for the NaSPA Technical Conference and we've been having them since 1987. This year NaSTeC 2010 is being held in the Chicago Ohare Airport area at the Westin Airport hotel. The event is being held on Saturday, October 16 and we'll have location information available on the NaSPA website very soon.

As has been the case for many of the last few years, the event is designed to be inexpensive and be held on a weekend so that your employer doesn't need to be involved. Since education/conference budgets have been very lean the last few years we've made this easy for you to pay for and attend.

This years' theme is "Career Development" and is designed for the job seeker, novice and veteran IT Technical Professional and the event will feature two tracks. Track one is for the "new" or "novice/entry level" IT professional to develop their career skills or to directly find a job. Track two is for veterans to better hone their skills to be better at their job and get the most out of their career. In addition to the two tracks there will be many opportunities for face-to-face interactions with other members, employers, staff and NaSPA board members and officers, hands-on workshops, door prizes, mentoring opportunities and a few fun surprises. More details to come soon!

NaSPA has always shined brightest during these events and we are excited, happy and proud to host it again this year. Look for more details inside, in upcoming issues, on the NaSPA website and in NaSPA e-news. I'm looking forward to meeting you in Chicago in October. Be there!

Leo A. Wrobel
Editor in Chief Technical Support Magazine
President, NaSPA, President@Naspa.com

NaSTEC

technical SUPPORT
Supporting Enterprise Networks and Operating Environments

NaSPA

June 2010
Volume 2, Number 2

Published exclusively for NaSPA, Inc.
Network and Systems Professionals Association

www.NaSPA.com

7044 South 13th Street, Oak Creek, WI 53154
(414) 908-4945, (414) 768-8001 Fax

June 2010 Volume 2, Number 2

FEATURES

ARTICLES

DEPARTMENTS

NaSPA Mission Statement:

The mission of NaSPA, Inc., a not-for-profit organization, shall be to serve as the means to enhance the status and promote the advancement of all network and systems professionals; nurture member's technical and managerial knowledge and skills; improve member's professional careers through the sharing and dispersing of technical information; promote the profession as a whole; further the understanding of the profession and foster understanding and respect for individuals within it; develop and improve educational standards; and assist in the continuing development of ethical standards for practitioners in the industry.

NaSPA serves Information Systems technical professionals working with z/OS, OS/390, MVS, VM, VSE, Windows Operating Systems, Unix, and Linux.

7044 S. 13th Street, Oak Creek, WI 53154-1429.

Verbal and Written Communication Skills for Technology Professionals

By Jeff Snyder

In high school, math, science and computer classes were easy classes for you. In college, you concentrated on science and math classes and worked through them with ease. Now, you're in the business world working in a technology related job and all that hard work previously devoted to math and science classes during your educational years is translating into a paycheck. So far so good.

But wait! Did anyone ever tell a computer science student when they were in school that verbal and written communication skills would become critically important skills to master in the workplace? Stated another way, what does it matter WHAT you know if you can't illustrate it in writing or the spoken word to your superiors, subordinates and peers in the workplace?

The Corporate View

Technology professionals who one day wish to stop writing code or who wish to stop administering networks need to develop verbal communication skills that enable them to provide clear communication to others. Chances are that this message was not communicated to you in college or you didn't hear the message when it was communicated.

When major corporations call on executive recruiters to recruit technology professionals for their organizations, more often than not the reason an external recruiter is called upon is to help their client to identify candidates who have both the required technical skills and exceptionally strong verbal and written communication skills. Technical skills alone are not that difficult to find. Add the requirement of exceptionally strong verbal and written communication skills and the search for talent just multiplied in complexity.

Companies place a high enough value on exceptional verbal and written communication skills to engage executive recruiters to assist in identifying candidates who possess such skills.

Verbal Communication

While you concentrated on math, science and computer related classes in college, odds are that nobody told you to also give your best effort in a speech or debate class.

Why is verbal communication so important? The answer should be apparent: Technology professionals who wish to progress to team leadership and managerial roles will eventually spend much more time interacting with their team and with line of business owners across the corporation in verbal communication settings than they'll invest into working with bits and bytes.

In many IT departments today, the ability to get funding for a proposed project is largely dependent upon a technology professional's ability to present the business value behind a technology project in a group setting. Failure to properly communicate in a group setting where your audience is generally made up of non-technology professionals will frequently result in a lack of funding.

Written Communication

Whether you think about it or not, you communicate in writing every day. Every time you send an email or a text, you leave a statement on a social networking site or you initiate a corporate memo, you're sending out impressions of who you are, what you do, and how you do what you do in a traceable written form.

When communicating with a human resources person on the inside of a company you wish to work for or when communicating with an external executive recruiter for the first time, the written communication you choose to deliver first will serve as a first impression that can't be taken back.

Technology professionals frequently fail to understand the impact of their verbal communication. When sending an initial email to a recruiter for example, take the time to write in complete sentences and to check spelling and grammar.

Be sure that the message you share presents a business case. Make it clear as to how the recruiter or human resources professional can most easily reach you, when they can reach you and most importantly, leave a first impression that will make the recruiter want to reach out to you.

Improving Communication Skills

Technology professionals who are serious about seeing their technology career elevate beyond the level of bits and bytes will do things their peers choose not to do.

For example, technology professionals who wish to overcome a fear of public speaking or who wish to learn to speak in front of groups for the first time might consider joining a local Toastmasters International chapter. These chapters are available across the country and meet on different days at different locations. Chapters exist to help members to improve communication and leadership skills and build self-confidence.

These are precisely the skills and traits technology leaders need to master in order to progress.

Technology professionals who need to improve their written communication skills might consider taking a college level business writing class or two.

Executive recruiters say that the difference between senior level technology candidates who are considered for "C" level jobs and those who receive offers is frequently quality of verbal and written communication skills.

Isn't the cost of a refresher college class or the cost of joining a professional speaker's organization worth it to see your career and future compensation elevate?

Jeff Snyder is the President of SecurityRecruiter.com, a search firm highly specialized in information security recruiting. Jeff's recruiting career started in 1990 in the general IT recruiting space. His first information security recruiting assignment landed on his desk in the 1995 - 1996 timeframe. SecurityRecruiter.com provides full-time and contract recruiting services, job placement services and professional resume writing services and is a gateway to various kinds of security education, security certifications and security training opportunities.

With Group Savings Plus®, NaSPA members can get more from their auto and home insurance.

Responsibility. What's your policy?™

Liberty Mutual

Savings of up to $327.96 or more a year on auto insurance*
with a special group discount and other discounts**

12-month Rate Guarantee
unlike the six-month policies that some other insurers offer

Help when you need it
with 24/7 Emergency Roadside Assistance and 24-hour claims service

Additional coverages for added security
including Umbrella Liability policies, Accident Forgiveness† and Home Insurance with optional Identity Fraud Expense Coverage

Chances are, Liberty Mutual's Group Savings Plus program may be able to offer you more savings and benefits than your current auto and home insurance provider.

AUTO

HOME

Get More. Save More.
Find out just how much more today.

- **Call 800-524-9400 and mention client # 101282**
  M-F 7:00 a.m. – 12:30 a.m., Sat 7:00 a.m. – 11:00 p.m., Sun 9:00 a.m. – 10:-00 p.m. (ET)
- **Go to www.libertymutual.com/naspa**

This organization receives financial support for allowing Liberty Mutual to offer this auto and home insurance program.

***Figure based on a February 2008 sample of auto policyholder savings when comparing their former premium with those of Liberty Mutual's group auto and home program. Individual premiums and savings will vary. **Discounts and credits are available where state laws and regulations allow, and may vary by state. To the extent permitted by law, applicants are individually underwritten; not all applicants may qualify. †Accident Forgiveness coverage subject to terms and conditions of Liberty Mutual's underwriting guidelines and is not available in all states. Coverage provided and underwritten by Liberty Mutual Insurance Company and its affiliates, 175 Berkeley Street, Boston, MA. A consumer report from a consumer reporting agency and/or a motor vehicle report, on all drivers listed on your policy, may be obtained where state laws and regulations allow. Please consult a Liberty Mutual specialist for specific details.**

Leveraging Virtualization to Automate Your Help Desk

by Ravi Gururaj

IT managers frequently work with limited resources and budgets, forcing them to prioritize the time dedicated to and money spent on their organization's critical needs. Often, these managers find themselves overwhelmed with the volume of demand from help and support desks servicing software customers.

Many organizations provide remote help and support services for their software applications over the phone, through email or on the Web. Much of the support team's time is spent trying to recreate the customer or user environment in order to offer the most appropriate solution to any problem the customer is experiencing. The level of software complexity, how software is used and the number of applications an organization supports can all contribute to the speed at which customer issues are resolved.

One technology that organizations can use to shorten support resolution cycle time is virtualization. While many companies have turned to virtualization to consolidate underutilized servers and save on additional physical server infrastructure investments, virtualization has also been used by software support teams to replicate images of customer machines as well as allow customers to share their images with support teams to help expedite solutions. However, server virtualization used in this context should only serve as the beginning of a support organization's foray into virtualization. Prior to deploying virtualization technologies, it is essential for support teams to develop deployment plans because without a management system, and given the relative ease at which a virtual machine (VM) can be created, virtualization may create more problems than it solves. VM sprawl and issues surrounding VM lifecycle management can wreak havoc for a support organization.

On the other hand, virtualization can also offer a number of strategic benefits from the shared resource pool that a virtual server infrastructure creates. This shared resource pool can be consumed across an organization, from the software support division to the help desk. Virtualization coupled with virtualization management software can enable support services to focus on fulfilling specific customer needs with increased quality and timeliness, rather than on how to manage or create customer environments. Virtual lab automation, a type of virtualization management software for virtual labs, can manage resource pooling and provisioning, which includes the support of complex multi-machine configurations, the management of VM lifecycles and the reporting and monitoring of virtual lab access and use.

With its low cost of ownership and high level of efficiency, virtual lab automation reduces the capital costs required to build software test labs and shortens support resolution cycle times while maintaining software license agreement (SLA) integrity. Whether a support organization is employing best practices or developing a support strategy from the ground-up, it needs a virtual lab design that takes advantage of the cost savings, flexibility and agility of virtualization, while managing virtual labs in a way that is beneficial to all stakeholders.

Central Management and Provisioning Using Virtual Lab Automation

Support engineers are responsible for debugging and troubleshooting any customer issues that arise. When a software issue occurs, engineers are usually faced with resolving the problem over the phone or online. Ideally, on any given day, these support engineers would have a library of pristine customer-like configurations modeled and readily available to troubleshoot customer issues remotely. This may not always be the case, requiring these engineers to recreate their customer environment from scratch, a timely process that detracts from the quality of service a support team is able to provide.

Software organizations that do maintain configuration libraries often use home-grown applications. Of course, as the number and complexity level of possible customer environments grow, so does the diffi-

culty in preparing and maintaining these libraries. A company servicing hundreds of software applications must be cognizant of the multiple problems that could arise – from the possibility of re-creating multiple configurations when the stored ones become difficult to locate to conflicts enabled when multiple users try to access the same configuration.

With a virtual lab automation solution running within the data center, organizations can easily build a library of multiple product versions and customer-like environments. Support teams can test a supported Web-based Java application against different versions of Java and different Internet browser types (such as Internet Explorer, FireFox, Opera, etc.) on every supported flavor of Windows against multiple Web servers (such as IIS, Apache, Domino, etc.). More importantly, virtual lab automation allows them to centrally manage and share configurations so that an environment cannot be brought up without being aware of other active running environments. This avoids problems such as IP address and hostname conflicts, eliminating the time spent dealing with these types of issues.

In the case that an in-house library configuration of a customer environment is not available, support engineers also have the ability to easily and quickly replicate customer environments to reproduce and resolve defects within a specified SLA timeframe. Support engineers can then save, snapshot and share with other staff members their configurations as they work with them and debug customer scenarios. All of these altered configurations can then be saved in the central library.

Another benefit of virtual lab automation is that it does not create full VM image copies which often result in massive amounts of storage utilization. With virtual lab automation, configurations are saved and VMs are deployed on the fly as needed. Engineers are then able to access a web portal that provides customer configurations and setups. These can be complete configurations (including full stack setups) that are deployed through a self-service model where support engineers choose and deploy the required configurations, without any additional manual intervention to resolve IP conflicts and other issues. With often limited resources, software support teams can optimize the use of their hardware.

The central management of virtual lab automation also prevents VM sprawl. Once a running configuration, or VM, has been deployed and used, resources can be reclaimed allowing them to be reprovisioned. Reclamation of resources can be triggered by the users or by a predefined job lease time, which is a defined length of time which an environment can exist on the lab infrastructure. Central management is crucial to keeping track of these VMs as well as the captured snapshots of provisioned systems. Snapshots capture and share multi-machine configurations currently in use from the configuration library. Captured configurations preserve memory and CPU state and can be redeployed instantly. Without the ability to take snapshots and then save and access them at a later date, support organizations often keep configurations provisioned for days or weeks – contributing to VM sprawl and inviting possible conflicts.

With so many users accessing resources, security is obviously a top concern for organizations deploying virtual lab automation. To address this, these solutions often come with a number of features to prevent misuse of the infrastructure. One of the most powerful security features is user access control, which enables IT managers to define strict access control policies which determine what users can do, see and execute within a virtual lab. IT managers can also set user quotas, which help eliminate resource abuse by ensuring that resources are used equally among users. To avoid hostname, IP or MAC address conflicts, most solutions will also use fencing – a network isolation technology that allows users to deploy identical environments simultaneously in their own private network. IT managers also have access to an audit trail which maintains a detailed log of all the activities and actions performed manually or automatically within the virtual lab automation solution. In addition, IT administrators can also control through a central management console which UI features and resources the support users have access to by defining user and team share permissions.

Conclusion

As software support teams turn to virtualization to leverage their resources, they should carefully plan how they will manage the virtual labs they create. With most organizations needing to run efficient and lean IT shops, virtual lab automation can be greatly beneficial in meeting the continual demands – of both time and hardware resources – placed on the support and help desk teams. Virtual lab automation can eliminate multiple inefficiencies that exist with the access and use of a software configuration library –shortening issue resolution times and helping deliver better customer service.

Ravi Gururaj has over nineteen years of technology product development, management and marketing experience. Prior to VMLogix, Ravi was managing director of Trilogy E-Business Software Pvt. Ltd., the Bangalore based offshore development center of Trilogy Inc. of Austin, Texas. Previously, Ravi was director, E-Commerce Initiatives at Trilogy, Inc., Austin and general manager of UberWorks Inc., a Trilogy incubated universal wallet and shopping cart infrastructure software. He has also been at Dialogic Corporation (an Intel subsidiary), New Jersey and founded two software start-ups that designed and licensed reusable software components for application developers worldwide. Ravi received an MBA with high distinction from Harvard Business School, where he was elected a Baker Scholar, and graduated with honors from the University of Pennsylvania, as a Benjamin Franklin Scholar in the Management and Technology (M&T) program, receiving a BSE in Computer Science & Engineering from the Moore School and a B.Sc. in Finance from the Wharton School.

BCDR: It's a big acronym where *business* comes first

by Ron Williams

Business Continuity and Disaster Recovery is a hot topic today. And rightly so. As the Insurance Information Institute notes, the number of declared major disasters doubled in the 1990s compared to the previous decade. When adjusted for current dollars, the top ten most costly catastrophes in US history occurred since 9/11/2001.

The top ten most costly catastrophes in US history occurred since 9/11/2001—Insurance Information Institute

In the decade of the World Trade Center disaster, we've witnessed significant upheavals in actual disasters as well as the threat of disasters. They come in the form of hurricanes, terrorist attacks, blackouts and brownouts, floods, ethics violations, and system failures. Government has responded with increased regulations and compliance directives: Sarbanes Oxley, HIPAA, FFEIC, and more.

Forrester counsels that many of these regulations mandate a company or organization present proof of disaster preparedness to auditors, industry authorities and government agencies. Proof can't be a simple insurance policy or an ability to recover from a one-time event, but a disaster recovery framework that sets standards for refreshing business impact analysis, risk assessments, developing thorough plans, testing plans, training employees, keeping plans updated and reporting meaningful metrics.

It's a tough world today—even for executives

There are many ways to approach BCDR, and there are many decisions to make. The SEC prohibits making false or misleading statements about internal operations. Sarbanes-Oxley section 404 requires that enterprises have a security policy and classify data for security, risk and business impact.

Executive and board-level decisions made incorrectly, could mean liability lawsuits. Disaster Recovery Journal notes, "Senior management decisions don't have to cause the damage for senior management to be sued, however even if the directors' and officers' decisions are exonerated, the company may still have to bear the cost of legal defense." That said, can you still afford to look at BCDR as an IT plan? No. While IT is absolutely mission-critical to the BCDR plan, it's the mission of the business itself that should prioritize, align and manage the continuity and disaster plans on an ongoing basis.

What's your mission?

For most businesses, IT isn't the mission today or during an emergency. For grocery stores it's keeping the community fed . For hospitals, it's about saving lives. For banks, it's about keeping money flowing. Granted, there are significant and complex IT plan to support those missions, but maybe IT doesn't have to recover *everything* as priority-one, but just those very important things to support the mission. So how do you assess priority? By integrating the BCDR plan in with the executive direction of the company that is managed through governance, risk and compliance.

Governance , Risk and Compliance

By looking at BCDR from a governance, risk and compliance standpoint, executives can more easily and quickly gauge and rank the elements critical to maintaining the business mission throughout any kind of disaster. They can weigh the business's core mission and risk tolerance against three objectives:

- To keep the business alive and the brand thriving
- To minimize the cost of getting back to normal
- To maintain compliance with regulators

Align that with your core services and your core business processes, and you are on the road to creating a BCDR plan that really does put business first.

The Hard Facts

"A company denied access to mission-critical data for more than 48 hours will be out of business within one year."—DisasterRecoveryPlanning.org

"93% of companies that lost their data center for 10 days or more due to disaster filed for bankruptcy within one year of the disaster"—National Archives and Records Administration

"25% of all companies that close due to disasters—hurricanes, power failures, acts of terror and others—never reopen."—Institute for Business and Home Safety

"Every year, hundreds of businesses that carry adequate insurance against direct property losses fail because they are not insured for indirect losses. After 9/11, 33% of dollars paid out for commercial claims were for lost income and extra expense claims for getting business back on track."—Insurance Information Institute

"92% of respondents said it was very important or somewhat important for businesses to take steps to prepare for a catastrophic disaster; but only 39% said their company had a plan in place."—Ad Council.

Ron Williams is the managing director of Clearview's Consulting Services Line of Business; focusing on business and IT strategy, business process improvement, and applications selection, implementation, and integration. As the lead strategist, he co-developed the IT outsourcing "go to market" plan for both MCI Systemhouse and Bell Atlantic Business Systems Services. Mr. Williams has extensive call center, data center, and infrastructure management experience. During the past 15 years he has become a thought leader in the area of applying business and IT integration to CRM, ERP, SCM and EIP. He has developed proven and effective models for justifying ROI through business case development and internal executive sales strategy development. http://www.clearviewfocus.com

Grooming The Next Generation of Data Center Professionals

By James I. Nelson, Chairperson, ICOR

You start your day as a data center professional by driving to work. You meet up with your chief engineer and lead electrician in a morning meeting, slip out at lunchtime to get a haircut and on your way home the phone rings. You are asked to stop at the butchers to pick up some steaks for the weekend. Just another typical day. What you are missing is right there in front of you.

You need to be licensed and certified to drive a car, cut hair, cut meat, or operate as an engineer or an electrician. As a data center professional this is not necessarily required. Hmmmmm, that's interesting. And not particularly uncommon.

People just like you are responsible for the care and operations of millions of dollars of physical plant, technical infrastructure, and equipment. It's a tall challenge. In fact, it can be difficult to calculate the precise value. After all, it's not just the physical equipment, but the value of the data that resides on it. The impact of any bad move can be pronounced.

This leads to the "way we have always done it syndrome" where inaccurate information, bad habits and misconceptions are shared.

Here is another scenario. Tomorrow is looking to be much busier. You are meeting on the feasibility of building a new data center to replace the existing 20 year old facility you have now. You have worked your way up to a senior position with the company over the last 10 years and you have been asked to take the lead on this effort. What do you know about designing and building a new multi-million dollar investment to meet the company requirements for the next decade or two? How do you even go about selecting the proper vendors and consultants to accomplish this project? Let me share a little with you from my personal experience.

I am in my early 50's and my peer group was amongst the first to actually pursue degrees in computer science. Our seniors were generally selected and trained because they had an aptitude for math or could think logically. Suffice it to say the over 50's have not been in school for a long time.

The "under 50 somethings" on the other hand have a variety of technical training. The younger crowd often looks to technology itself for solutions. They embrace the geek factor. The more experienced crowd has the scar tissue and experience garnered through their careers. The younger crowd embraces technologies and is not afraid to try new things. There is no right or wrong here, in fact, the happy medium probably lies between the two.

The majority of professionals do not have the opportunity or work experience to become familiar with all of the complex aspects of design, build and operating a critical data center or server room facility. Instead, we have a tendency to silo and become proficient at specific functions, disciplines or aspects of the data center. There is also an unrealistic expectation that you may learn or pick up "best practices" throughout your career. This leads to the "way we have always done it syndrome" where inaccurate information, bad habits and misconceptions are shared.

There are solutions and alternatives available in the marketplace, including vendor training to use products and equipment that focuses on the diverse specialties in the technical field. Many providers offer training on how the optimize the use and performance of *their* products. These are useful when considered in context. It's a good way to stay current on new technology, but obviously a vendor will not tell you if a competitor has a better product or service. Your peers however will tell you. Therefore you can also attend local user groups or conferences and seminars in the discipline. Join organizations like NaSPA!

When looking for more formalized training, alternatives are also available. (Albeit far fewer than a generation ago – many formal training companies and seminar houses are gone!) As a principal in one of the "survivors," the International Consortium for Organizational Resilience (ICOR) let me tell you what to look for when you look for formal training. First let me preface that like the vendor example above, you should take this advice with a grain of salt. We are a vendor, but like to think we know a thing or two about training.

ICOR provides a number of training options, but we will discuss the Certified Data Center Professional series of courses. These courses are specifically designed on how to design, build, operate and optimize a critical data center facility. These courses were developed by EPI Asia Pacific and are certified and delivered in the western world through ICOR. The benefit and market differentiator of the ICOR training is that these course are standards-based and vendor-agnostic and taught by instructors who know how to both teach and who have experience managing and building data centers. The training is of very high quality and is designed to meet the needs of the fast paced challenges of the

present professional. The standards-based design provides benefits in review and audit of a new design or a risk assessment of an existing facility that must continue to operate.

The focus is on high availability and encompasses all of the issues that face the data center professional, the facilities professional and the business continuity professional. The standards-based design also means the design is repeatable. It means that key decisions can be analyzed and assessed based on facts - not on opinions and recommendations of design professionals that do not have the responsibility to continue operations for the life of the facility.

The standards-based design and delivery of these courses also allows you as the business owner to make informed decisions on which consultants, design firms and solutions you select to meet the unique needs of your project.

There are obvious benefits to the consultants and design-build firms also. They have the opportunity to review their offerings and best practices, align these to standards, improve their credibility and delivery mechanisms, and better meet the needs and requirements of their clients.

The materials that are takeaways from the course itself are excellent reference tools rather than just a set of PowerPoint presentations that you receive in other training offerings.

Another testimony is that students return to take additional courses in the series. They recommend the course to their colleagues. They enroll in other courses offered by ICOR.

ICOR has recently seen some competition with some very similar offerings entering in the market place. We welcome the competition. There is an old saying that this is the highest form of flattery. Adding a letter here and there to the trademarked certification does not deliver quality. The requirements to continue to stay current to developments in the profession are a must to protect the integrity of the credential and the profession as a whole. ICOR is a non-profit 501c3 certifying body – this is also a differentiator. Anyone can print a certificate. The value, integrity, quality and recognition of the certification is assured through ICOR.

If your intent is to pursue high quality professional development, deliver quality to your employer and clients, operate at a high ethical level and contribute to the future of the profession there is only one question. When can you start?

James I. Nelson is the Chairperson of ICOR and an instructor of the data center series of courses. He is also the President of Business Continuity Services, Inc., a consulting company in the disciplines of business continuity, crisis management, data center management, and disaster recovery planning. For more information go to www.theICOR.org and www.BusinessContinuitySvcs.com.

Exploiting Software Vulnerabilities

By Maura A. Van der Linden

Software attacks are regrettably a fact of life for the I.T. professional and it is important to stay vigilant and informed. This article discusses the many ways for software exploits to be delivered as an attack, and some of the issues that surround specific delivery mechanisms. In addition, this article should help you then garner an understanding of the identity, goals, and motivations of potential attackers. It's not meant to be a comprehensive overview of every type of vulnerability. The most clever and talented of attackers with an innovative exploit can still in many cases get that exploit to the systems they wish to attack. Because these are only the delivery mechanisms however, and because the actual content delivered varies greatly, we discuss each below and offer a few tips on what you can do about them. Let's start with the basic terminology:

Trojan

A Trojan in software security means a seemingly attractive or innocuous program that hides malicious software inside. Trojans aren't typically capable of spreading themselves, but instead they require a separate method of distribution, and that usually consists of the file containing the Trojan being transmitted to potential victims using methods like e-mail, instant messaging, IRC, ICQ, etc. When the potential victim opens the file, the Trojan is installed. Trojans can also be staged on download sites and disguised as utility programs, games, etc., and the victim is tricked into downloading them because they look like a useful program the victim might want to use.

Trojan Horse Virus

This is a hybrid between a Trojan and a virus. Most Trojan horse viruses infect like a Trojan in that they need to be run or executed by the victim (still typically by opening a file), and then the virus behavior takes over and the Trojan horse virus automatically spreads itself to other systems. So, it spreads like a biological virus. Sometimes it sends itself to your address book or your IM contact list, etc.

Virus

A computer virus is a program, typically malicious, that reproduces by adding itself to other programs, including those belonging to the operating system. It cannot run independently but needs a "host" program to be run in order to activate it. The source of the name is a reference to biological viruses that are not considered alive in the usual sense and can't reproduce independently, but rather invades host cells and corrupts them into producing more viruses.

Boot Sector Viruses

A boot sector virus is one that infects the boot sector of hard disks, floppy disks, CDs, DVDs, USB drives, etc. Despite the infection being located in the boot sector, these do not require that the victims boot their system from the infected media to infect it. These viruses often stay resident in memory and infect floppies and other media when they are being written by the infected system. Once relatively common, such viruses are becoming ever more rare as the use of floppy disks continues to decrease.

Master Boot Record (MBR) Viruses

A master boot record virus behaves very similarly to the boot sector viruses, except that it infects the master boot record instead of the boot sector.

File Infector Viruses

The file infector viruses infect executable files such as .EXE and .COM files. Some of these viruses will stay resident in memory and carry on continuously infecting files, but others only infect the system when their host file is executed.

Macro Viruses

A macro virus uses some sort of scripting language, often Visual Basic or JavaScript, and infects types of datafiles from applications that support that scripting language. This is most well known from the incidents of infections among the various datafiles of Microsoft Office suite.

Multi-Partite Virus

This is simply a virus that exhibits the characteristics of more than one of the types of viruses.

Worm

A worm is a program that can copy a fully functional version of itself to other machines across a network without intervention. It doesn't

usually require another program in order to run, but worms can, and do, sometimes hide behind other programs. The source of the name is a derivative of "tapeworm," which is a parasitic organism that lives inside a host and saps the host's resources in order to maintain itself.

Logic Bomb

This is a piece of code that sits and waits for some piece of program logic to be activated and then activates the bomb's payload. Date bombs are the most common type of logic bomb, but the trigger could be anything from a message to the deletion of a file or directory, or a file size. Logic bombs don't replicate themselves but instead have to be specifically targeted to the recipient. These are sometimes attached to a delivery mechanism that will install the logic bomb on a user's system. Although this is really a trigger rather than a delivery mechanism or method of spreading, I've listed it here because it's generally delivered with one of the other listed delivery mechanisms.

The Role of Social Engineering

There are probably as many definitions of what "social engineering" is as there are security specialists, maybe more. My own favorite definition is that social engineering is a clever manipulation of the natural human tendency to trust in order to persuade people to do as the manipulator wishes them to.

All trust is misplaced.

It's a human tendency to grant trust far too easily, and that makes the human factor the weakest link in the chain of security. The goals of social engineering, as applied to software security, are similar to that of the various programs and tools - to gain unauthorized access to systems or information to commit data theft, disruption, industrial espionage, etc.

Social engineering plays a huge role in many security exploits, often as the initial attack vector. There are multiple psychological reasons why social engineering is so successful and most of them simply boil down to aspects of human nature. The quandary with social engineering is that user education only goes so far, and you can't issue a patch for people to insure they cease whatever risky behaviors they have been exhibiting or to increase their skepticism.

At its core, social engineering is really a confidence (con) game. It's an age-old criminal approach that has now moved into the electronic age with a vengeance and at great benefit to the con artist. The costs to run the con game are far less. The chances of the con artists getting caught are much less because the victims and potential victims don't actually meet the con artists face to face. In fact, they may not even be in the same country as their victims. There is a much larger pool of potential victims that are far easier to approach, and it only takes one or two potential victims to fall for the con to make it all worthwhile.

Social engineering attacks and, really, all security attacks, are not usually a single event that strikes like a bolt from the blue. The attack pattern may include a succession of more and more complex attacks that serve to gather information or probe for weaknesses and lead up to the culminating major attack. If you think of social engineering in particular, you can see that even the release of minor amounts of information that are not seemingly of much use on their own could be used later to form and carry out other information gathering attacks or even damaging attacks.

Imagine that someone persuades you to give him the last four digits of your social security number to "verify your identity," and then you get a call from a very convincing man who says he is from your bank and who tells you that the bank has intercepted a case of suspected identity theft using the social security number it has on file for you. He tells you the last four digits and then asks you to repeat the entire number so he can verify that your number is indeed the one being used and the bank can take action. By the end of the call, if you've fallen for the con game, the con man has your entire social security number and certainly already has your name, address, and phone number. Now the con man has a set of data that can result in identity theft. There are two basic types of social engineering - active and passive.

Active Attacks

In active social engineering, the con artist has direct contact with the potential victim. This could take the form of telephoning the victims to talk them into revealing a password or other private information, and in many ways this resembles one of the more classic telephone scams. This could also be an in-person attack where the con artist shows up at the office door and pretends to be a representative of your company's software vendor, and needs to install an emergency patch on your system. Almost all active attacks depend on one or more of the following methods to gain the information and access the con artist needs:

- Authority - We are all taught to respect and bow to authority.
- Befriending - It's human nature to want to trust, and especially to trust those we feel are, or are becoming, friends.
- Blackmail - We've all done wrong or an impression can be created that we've done wrong, even if it's not actually true.
- Deception - Flat out lying is always a staple.
- Flattery - Who doesn't want to think they are special or somehow better?
- Impersonation - Most often combined with another method, especially authority. Just pretending to be someone they aren't or to represent someone they don't.
- Intimidation - When in doubt, play on people's fears by intimidating them.
- Pressure - Don't want to give you any time to think so you're less likely to see through the con.
- Sympathy - This applies to both seeking and giving sympathy. Who doesn't want to help someone who is in need or in trouble? Who doesn't soften toward someone who seems to sympathize with our own predicament?

Passive Attacks

Passive attacks attempt to obtain information with stealth. They tend to be carried out in bulk so as to maximize the return. After all, why send one or two e-mails (or even fifteen or twenty) when you can send tens of thousands for not much more of an investment? This is true especially if you are using someone else's e-mail server or account.

These passive attacks use some of the same methods as the active attacks but aren't nearly as specific as the latter. They don't have as high a percentage of success, but with the quantity involved and the relative

NaSTEC Convention returns to Chicago on October 15-16, 2010

To Register or for further details, visit NaSPA.com. This year's theme, Employment and Career Development!

Be an active part of this focused one-day event!
If your organization is interested in presenting or providing a speaker for this year's intense NaSPA Systems Technical Education Conference (NaSTEC 2010), please contact Leo A. Wrobel, President, at president@naspa.com. For securing an exhibit display space, to get full exposure for your products and services, get in touch with NaSPA's Don McMurray at (414)908-4945 ext.111 or dmcmurray@naspa.com. NaSPA members and partners get special consideration and discounts on exhibit space purchases and preference as speakers. Make your mark on many NaSPA members at what promises to be a lively and eventful NaSTEC 2010!

(L-R) past NaSPA board member presenting Ron Fischer with the "Member of the Year" Award

Mainline exhibitors at a past convention

Think NATURAL DISASTERS are Beyond Your Company's Control? Think Again.

Since 1996 the Pacific Disaster Center (PDC) has delivered solutions to disaster and humanitarian assistance communities worldwide. Now many of the same tools previously used only by Governments are available to YOU.

PDC provides comprehensive, multi-hazard early warning and risk analysis platforms:

- **Timely and Actionable Disaster Warnings**
- **Vulnerability Analysis and Visualization**
- **Business Impact Analysis**
- **Proactively Mitigate Risks and Take Preventative Actions**
- **Know precisely where your company is at risk – from world renowned experts.**
- **Click HERE for a FREE LOOK NOW:**

- **Improve Situational Awareness *before and during* Disasters**
- **Make capital construction and spending decisions based on HARD FACTS.**
- **Conduct Meaningful Business Impact Analysis (BIA) with the goal of reducing risk to lives, livelihoods, and the organization's economic assets.**
- **Scalable to organizations of all sizes, from a low-cost server to enterprise-wide multi-server platforms.**
- **OEM Partners Welcome to Inquire.**

PACIFIC DISASTER CENTER

*As seen in **"Disaster Recovery Planning for Communications and Critical Infrastructure,** © 2009 Artech House Books. Click HERE to Order Your Copy:*

For more information contact Leo A. Wrobel, President, b4Ci Inc.
Executive Outreach Consultant for the Pacific Disaster Center. (214) 888-1300 / Email Leo@b4Ci.com.

inexpensiveness, only a few successes are needed for them to pay off. They are also more anonymous than the active attacks.

Phishing

Passive attacks include items like phishing, where many thousands of emails are sent to potential victims claiming that the person needs to change a password or verify a credit card number, and includes a helpful link to click on to do so. This link typically leads to a look-alike site, many of which are quite cleverly done, but entering data on these look-alike sites is the equivalent to handing the attacker your information.

A lot of these links are titled in a way intended to conceal the truth of their origin or exact nature. The hyperlink title may be "eBay Password Change," but if the potential victim hovers over the text to see the URL, they may be able to tell that it doesn't even have a similarity to eBay. Some of the URLs themselves are designed to deceive. A phisher may use a domain very similar to that of the legitimate entity they are masquerading as, for example, "www.ebaysecurity.com." These links are, however, similar enough to deceive the potential victim who only gives it a quick glance.

Lately, I've even seen some look-alike sites place a false "lock" symbol on their web page to pretend to be an HTTPS site. Because users are taught to look for this lock symbol as a sign that a site is safe, they may see that lock and never even look at the address and see it's not an HTTPS site at all, but rather an HTTP site using a bitmap to deceive them. There is also a play on trust if the e-mail you get happens to claim to be from a company or entity you already use. Most of the time, that is merely a random event because phishing e-mails tend to be "blanket" mails rather than specifically targeted e-mails. E-mail headers are notoriously easy to spoof, but despite that fact being rather well known, many people still believe that the e-mail they receive is indeed from who it claims to be from.

These passive attacks can also include pop-ups and redirects that the potential victim can't verify the source of and which may lead them to believe that they need to enter their name and password again, but that information is really being sent to the phisher instead.

Urban Legends

Although not technically a security risk, a look at how urban legends begin and are subsequently spread is an interesting study in some of the aspects of social engineering. Urban legends are cautionary tales couched as tales of actual events that always seem to happen to someone only slightly removed from the alleged writer. Some are true and some are fictitious, but they all share the fact that they play on human fears. Most urban legends are also modern tales - supposedly taking place relatively recently.

These are often spread in e-mail and are typically forwarded to us by a friend, family member, coworker, or online acquaintance. I often see them spread in newsgroups and e-mail lists as well. Although many of these tales seem dubious at best, a surprising number of people will look at the e-mail and immediately begin forwarding them to their friends and e-mail lists without ever attempting to verify the information they contain.

When these people are confronted with information that the e-mail they forwarded is an urban legend and that they should check their information before passing it on, they almost inevitably became defensive. They immediately claim that it has to be true because it came from so-and-so who would never send them something that isn't true. Their defensiveness seems to be dual edged - part "how dare I cast doubt on the integrity of so-and-so" and part feeling embarrassed that they fell for the story and didn't ask questions.

However, the point doesn't seem to get through that I am not casting doubt on so-and-so's integrity. I'm sure that the people who forwarded that mail, all the way up the line to whoever first received it from the original author, sincerely believed that it was true and the cautionary tale, picture, warning, etc., should be passed on to their friends and relatives. Each person in the chain trusted the information's source. The motives of the original author, however, are often a different matter.

All trust is misplaced. Just because someone you know forwards an email to you, never trust that the e-mail is true.

Nigerian (419) Scams

Another case study in social engineering is that of the Nigerian Scam -also called the 419 Scam or the Nigerian Advance Fee Fraud. The 419 refers to a section of the Nigerian penal code that applies to these types of cases. Various sources claim different dates for the start of this fraud - ranging form the late 1970s to the early 1990s. They do agree that it began with paper mail and fax but migrated to e-mail and the Internet relatively quickly. It is now sent almost exclusively by e-mail with occasional cases of instant messenger transmissions.

This well-known and well-publicized con game typically claims that it is from a person or a representative of a person who needs help to transfer large sums of money out of the country or to claim inheritances. There are numerous variations that have different stories such as being the beneficiary of an estate or needing help to claim an unclaimed estate. These are also not at all limited to Nigeria anymore.

If the potential victim asks questions, the con artist always has an answer, typically very apologetic and heartfelt. The con artist will continue to string the potential victim along with a variety of ploys until the potential victim either says no or gives in. Once the victim agrees to whatever deal that particular con artist is trying to pull off, the victim is sent official-looking documents or e-mails, then delays are claimed, and the perpetrators begin to request a transfer of a relatively small amount of money (in comparison to the promised payoff) to do things like bribe officials, set up an appropriate bank account in the local country, etc. As long as the victim pays, the delays and more additional costs are added while the perpetrators keep the carrot of the large payoff in sight. However, the promised payoff will never happen because the funds just do not exist.

All trust is misplaced. If a deal appears to be too good to be true, never trust the sincerity or honesty of the person brokering the deal. The entire 419 scam is a con game - a social engineering scam at its purest.

Lost in the Cracks

A prime place to look for security bugs is in all the "cracks" in and around your product. I consider a crack to be anywhere that control is passed or data is moved between separate functions, modules, applications, or even hardware. You'll see that this is also an area that is focused on in the section on threat modeling. In a way this also goes back to trust. If data has been brought into the system somehow, an implicit trust exists that this data has been validated somehow by whatever brought it into the system in the first place.

All trust is misplaced. Data being passed, even between subsystems of the same project, is not inherently trustworthy. This is especially true as programs, operating systems, and even accessories become more and more interconnected. There may or may not actually be any way to tell how any piece of data entered the system.

Vulnerabilities are also found in between areas of functionality in the same application or product. One module may take data from the UI and pass it to an application programming interface (API) to process. The API doesn't check the incoming data before using it because it trusts that the UI has validated the data and only passed it on to the API after validation. However, if the data was sent to the API by a method other than the UI, that data may be untrustworthy for multiple reasons, including:

- Business logic rules violated
- Data boundaries not enforced
- Unexpected data passed through
- Source may be spoofed or otherwise untrustworthy

Vulnerabilities are often found in areas of interface between different applications, products, or hardware. One system may take direct user input and save it in a file that is then consumed by another system. In this case the secondary system may not check the file before using it because the first system has been trusted to produce only valid and usable files.

However, the file that was consumed by the second system may be untrustworthy for multiple reasons both inside and outside of the control of the first system. Some examples are:

- Formats not respected
- File crafted with malicious code
- Version changes
- File modified before use
- Generator of file unknown

We hope this article was helpful and provided some food for thought about protecting your systems from many kinds of issues, intrusions and malfeasance. For more information please feel free to order my book below with your NaSPA discount by clicking the Auerbach link on the home page, http://www.naspa.com.

Call for Authors

Each month Technical Support Magazine brings you an eclectic collection of articles, of interest to Information Technology professionals of all types. Do you have valuable insights and ideas that can be shared with NaSPA members? Fresh, timely ideas are important to our members, even if you have never published before. Our editorial staff is here to help and welcomes your submission. It's never too late to start. Contact president@naspa.com for more information or to submit your article for review for possible inclusion in a future edition of Technical Support.

Upgrade Your Business Along with Your Software

By Dan Wilhelms

The recent announcement by SAP reminding customers of the approaching deadline for discontinuing mainstream maintenance has created a flurry of activity. Enterprises that don't want to move into the costly "extended maintenance" mode and pay an annual surcharge to continue receiving support are now scrambling to make sure they move up to SAP ECC 6.0 by the appointed deadline.

When the upgrade is complete, no doubt many will issue a collective sigh of relief at having dodged that expensive bullet. Yet in the end, if all you've done is change the version number of your software, you've really missed an opportunity. Because a software upgrade presents the perfect time to move your enterprise onto a better business platform.

If all you've done is change the version number of your software, you've really missed an opportunity.

Why? Consider how much work goes into a software upgrade, especially in the SAP world. You have all the planning that goes into it. You have the technical upgrade, which essentially resets any custom code you've developed back to SAP standard – which means you'll have to put all the custom code back into it afterwards. There's all the testing to make sure everything still works. And finally, there's upgrading and testing all the functionality, which can take months to complete.

Throughout this long, arduous procedure, you will be opening up your business processes and back-office operations to make the changes. Rather than simply converting them to the new version, it makes sense to examine them closely to ensure that the things you set up yesterday still make sense for where the business is today – and where it's headed tomorrow.

Following are a few of the areas you should look into as plan your upgrade.

Streamlining business processes

Business processes have a tendency to grow and evolve over time. Sometimes, for the better, sometimes not. While there was, no doubt, a good reason at some point for every process you have and the way it has been built, that may no longer be the case.

A version upgrade is the perfect time to look at your business processes and determine which should stay, which require modification, and which should perhaps be retired. After all, you will be exposing these processes as part of the project planning process. Instead of just accepting them as-is, why not take the extra time to make sure they make sense.

For example, you can look at how purchases are initiated and how the approval process for payment works. What are the steps? Are there any that are unnecessary or redundant? Are there any that violate compliance regulations? Could certain things be shifted elsewhere to provide a more balanced workload?

Again, you will be looking at the business processes anyway to make sure the transition from one version to the next goes smoothly. Why not look at them with a critical eye to help you optimize the business?

Reducing complexity

Just like business processes, systems also have a tendency to grow in size and complexity over time. An unmet need here, a special project or requirement there, and suddenly your SAP landscape is so complex it takes more time and resources to operate than it should.

The planning phases of a software upgrade create an opportunity to take a step back from your SAP landscape and see where the complexity can be reduced. In some cases, it may be a matter of simplifying or even eliminating certain procedures. In others, it may be a matter of leveraging a new capability that is being added as part of the upgrade. Or it may be in consolidating two or more operations into one more all-inclusive process.

SAP is complex enough on its own. The more you can do up-front to simplify its use, both for your business users and your internal team, the better value you will gain out of it.

Reducing ongoing support and maintenance

It has been estimated that the average IT department spends 70 percent to 90 percent of its time and budget on maintaining the hardware and software it already owns. That leaves very little time to develop innovations or contribute ideas to advance the business.

A software upgrade creates an ideal environment in which to examine current support contracts and history to determine if the level of support being paid for matches the organization's needs. Is there redundant support? Do the current contracts align with the going rates at this time? Has the performance met expectations? Are you still paying to support systems that no longer require that level of support?

An upgrade is also an opportune time for IT leadership to look at which support functions absolutely must be handled internally, and

which can be outsourced to an outside firm. If even half the current support and maintenance load can be reduced, it frees internal IT resources to focus on more profitable projects from which the enterprise can derive real business value.

There is a human tendency to allow low-visibility activities such as support and maintenance to just roll along over time. Place those activities under the microscope during an upgrade and make adjustments as-needed.

Increasing productivity

Software upgrades, especially significant ones such as SAP ECC 6.0, generally introduce major improvements and capability additions. Yet enterprises may fail to gain the full value if they don't leverage those improvements by re-examining their operations and making adjustments accordingly.

Instead of looking at how you can transition current processes into the new software, enterprises should see if the software lends itself to new, better processes that increase productivity. Even several small improvements can have a cumulative effect. And if there's one "Aha!" change, it can help justify the cost of the software upgrade over the long term.

Instituting better practices

Although they're not intended to be, institutional best practices are often looked at as a project to be completed instead of living, breathing guidelines that need to be re-examined and updated constantly. As a result, what may have once been a "best" practice may no longer be.

Since a software upgrade is heavily process-oriented, it is a great opportunity to go through the organization's best practices to ensure they really are the best way for the enterprise to operate. A good place to start is change management (especially documentation) since it will have the most direct effect on the success of the upgrade itself. Tightening up change management and documentation procedures will help minimize the risk during the change itself while positioning the enterprise for better operations going forward.

Once those best practices have been established (or confirmed), IT can then proceed to review and improve technical procedures followed by functional uses within SAP. With the upgrade going on, there should be ample opportunity to test the new practices to be sure they truly are optimal, and once the upgrade is completed, the organization will be well ahead of where it would have been if it merely undertook a technology/version upgrade.

Conclusion

While the upgrade to SAP ECC 6.0 may be driven by what are perceived as negative conditions, the opportunity exists to gain a more positive outcome than merely the continuation of regular maintenance. Use it to move the enterprise to a better business platform overall, and you'll reap the rewards many times over.

Dan Wilhelms is President and C.E.O. of Symmetry Corporation (www.sym-corp.com), an SAP® hosting partner that provides technical managed services, security administration and project consulting for SAP customers in the U.S. and around the world. He can be reached at dwilhelms@sym-corp.com.

Enterprise User Identification and Authentication Challenges

By Dobromir Todorov

During the time of centralized computing when users had to use terminals connected by means of serial links to a mainframe or central computer, authentication was centralized and there was only one place where it could be performed - the only intelligent component was the central host. Later on, when minicomputers were connected to the first networks and started communicating with one another using protocols such as TCP/IP, the authentication model started to change and became relatively decentralized. Users now needed an account on every host to which they wanted to connect.

Apart from interactive sessions, however, because of the small number of networked hosts and therefore authentication databases, accessing resources that resided on one host from another host was a matter of a simple model of trust where authentication was not really vital. The model of trust at that time was based on the UNIX r* commands (such as rsh and rlogin) that provide for an authorization file with a list of remote users who are allowed equivalent access to the one a local user has on a particular host. Authentication was not really involved; it was simple identification, wherein the user ID of the requesting user, as well as the name or IP address of the requesting host, could be deduced by the r* request.

In the early 1980s, the IBM Personal Computer and Apple Macintosh started the personal computer (PC) revolution, and now every user had a microcomputer on his desk. UNIX workstations also became popular and now even UNIX users could have their own dedicated host on their desks. Personal computers meant (somewhat) decentralized computing; and in order to be able to share resources in a decentralized world, networking advances were required by the industry. Among the main requirements from the network infrastructure was the ability to authenticate in a network of micro-hosts. As a result, many authentication systems were developed.

This article (and my book described below) present some of the commercial and industry systems that have survived for the past 20 years. However different these systems might be, they fall into two main categories: (1) centralized and (2) decentralized authentication systems.

The decentralized authentication approach (Figure 1) allows each network host to maintain its own user authentication database and policies. UNIX hosts have their own and are independent from other hosts' /etc/passwd file and may potentially use PAM but will still maintain an independent database of users. Windows hosts maintain their own local security accounts manager (SAM) database and authenticate users against this database.

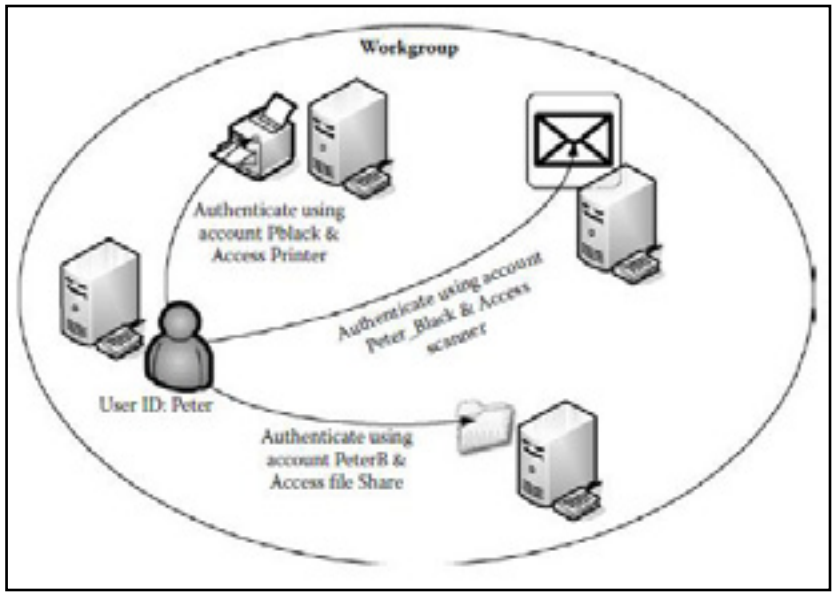


Figure 1 Decentralized authentication workgroup model.

The centralized authentication approach (Figure 2) requires hosts to trust and follow the policies defined by a central authentication authority. This may be just one host, or it may be a set of hosts that form a logical authentication authority. The authentication authority has an authentication database that can be used by all the hosts participating in the centralized authentication system.

An advantage of the decentralized approach is that it allows for user authentication autonomy. In systems that require a very high level of security, designated hosts may be hardened and configured in a secure way to allow access to highly sensitive information assets. Such high security hosts or workstations are not likely to trust other parts of an information system which have a lower level of security. Another advantage of the decentralized approach is that there is no dedicated hardware required for centralized authentication authority servers, so this makes this model appropriate for home networking and small organizations of a couple of networked computers.

The disadvantage of the decentralized approach is that it requires authentication every time a user from one host needs to access resources on another host. Every user needs to have an account and associated credentials, such as a password, on every host on which there are resources that this user may need to access. A separate account should

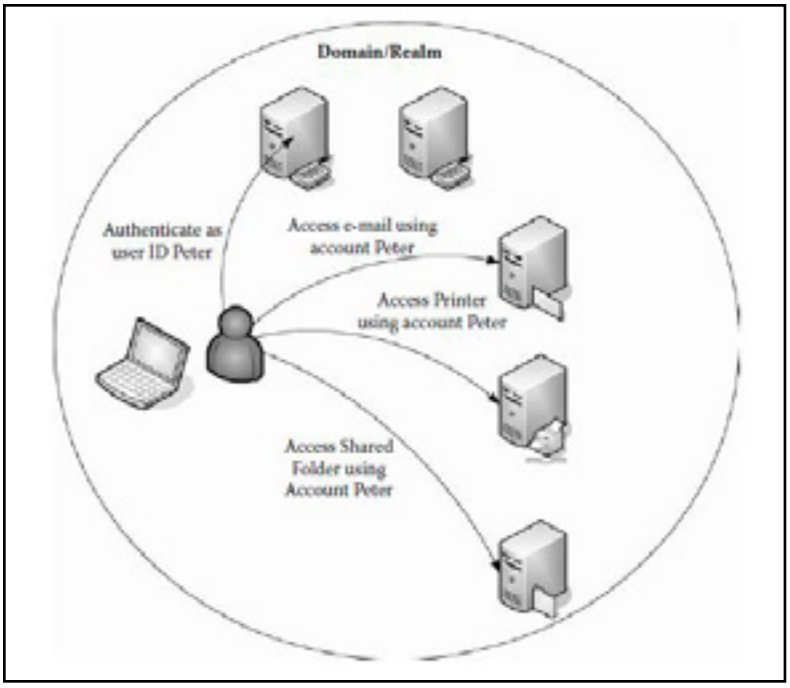


Figure 2 Centralized authentication workgroup model.

be created on every host. Unfortunately, this does not scale well for more than a few computers.

In a network of ten computers where each user has his own computer, and administers his own authentication database, for a complete trust between all the users so that every user can access resources on every other computer, 10 x 10 = 100 accounts will be required: every user has an account on his own host, and a separate local account on every of the other nine hosts. Every time a user needs to access a resource on a remote host, he might potentially need to use a different username assigned by the administrator of the remote host. Potentially, he may also need a different password. If the user wants to maintain the same password on all hosts, then every time the password is changed on one host, it should also be changed on all other hosts. The whole maintenance of this otherwise simple model takes a lot of user and administrative time and effort.

The advantage of centralized authentication is that authentication information is stored in a central authentication database and one or more servers play the role of an authentication authority. If a supplicant trusts the centralized authentication authority, it can become part of the centralized authentication system. Because the centralized authentication authority is trusted to provide authentication information, all participating hosts can authenticate any user who has an account in the central authentication database. Therefore, each user only needs to have one account, stored in the central authentication store, and he can log in from any host in the centralized authentication system, and then access resources to which he has been granted access on any host in the centralized authentication system without the need to re-authenticate. This approach gives significant advantages to enterprise information systems in terms of user account management, and centralized security.

A disadvantage of the centralized approach is that if a user account is compromised, the attacker has access to any resource to which the user account has access. For some information systems, this model may be unacceptable.

An example of decentralized authentication is the Windows Workgroup authentication model (Figure 1). In this model, each computer stores authentication information locally in a portion of the machine registry called the Security Accounts Manager (SAM). Each computer in a workgroup defines its own local authentication policies and user accounts. To log on interactively from such a workstation or to access resources on this workstation over the network, users must have a user account defined locally in the SAM for this workstation.

Examples of centralized authentication are Windows NT and Active Directory domains (see Figure 2). In both cases, information is stored centrally in a user database, which is made available by set of authentication servers known as domain controllers. In the case of Windows NT, authentication information resides in the SAM. For Windows 2000 and later, user authentication information is a subset of the information stored in Active Directory.

Centralized authentication is a generic term for Single Sign-On (SSO). In today's information systems, organizations invest money and effort to make sure that users are authenticated only once (sign-on only once) but then are able to access resources anywhere on the network. SSO implies unified authentication for access to both the infrastructure using port access control technologies, or remote access, such as dial-up or VPN, as well as services: e-mail, file services, Web portals, management information systems, etc. Unfortunately, at the time of this writing, true SSO is rarely possible.

In an ideal world, all the applications and services in an organization will use a single centralized authentication database to provide for user authentication. Unfortunately, services at the infrastructure layer, as well as applications and services at upper layers, have their own authentication methods and databases.

One of the approaches to SSO is identity management. Organizations - especially those with legacy applications and information systems - may have a multitude of directory services with information about users. For example, many organizations have a human resources database, a phone directory, and legacy plaintext files in the file system for user authentication. Users in the phone directory may be listed by their full names, and plaintext authentication files may use user IDs. The human resources database may use employee IDs as the primary way of identifying users. Identity management solutions typically provide for directory replication or synchronization so that system designers can create relationships and effectively use information from all the directories. This is often achieved using a metadirectory: a centralized, consolidated directory with information from all potential sources. Once data has been consolidated in the metadirectory, it can then be replicated to each and every directory, and updated as necessary or on a regular basis.

I hope this article was helpful to you. For more information, why not consider ordering my book below using your NaSPA discount. Just click the link on the home page, http://www.naspa.com and select the Auerbach discount prompt.

This article has been adapted from Mechanics of User Identification and Authentication: Fundamentals of Identity Management by Dobromir Todorov. © Auerbach Publications, New York, 2007. Technical Support thanks Auerbach for this thoughtful contribution.

Looking for an extraordinary opportunity for your firm? Look No Further. NaSPA wants your company!

Technical Support™, NaSPA's 24-year old, award-winning, flagship publication is working toward solid growth. NaSPA membership is already growing at a renewed pace and this captivating publication needs to advance to meet the organization's membership expansion. NaSPA is seeking one or two long-term sponsors to assist in this upward progression. Here's an invitation for your firm to partner with NaSPA. Together we can accomplish development goals that, individually, are unavailable!

NaSPA is looking for two special firms with which to form partnership agreements.

The NaSPA partners will receive a number of valuable benefits. Among them are:

- A full-page *Technical Support*™ ad in each issue
- Exclusive sections of *Technical Support*™ and NaSPA website dedicated to your firm
- Quarterly e-blast to 100,000+ *Technical Support*™ readers and association members
- Free exhibit space at NaSTEC, NaSPA's annual conference in Chicago in October
- Free distribution of your marketing brochure at NaSTEC conference
- 25 Gold NaSPA memberships for your staff and customers

This opportunity offers a high level of value in NaSPA services for your firm. For more information contact NaSPA President, Leo Wrobel, president@NaSPA.com.

NaSPA®
NETWORK AND SYSTEMS PROFESSIONALS ASSOCIATION

Are SAP® Organizations Living on Borrowed Time?

By Dan Wilhelms

In every movie involving a natural disaster or an invasion by space aliens, there is always one scientist or person of authority who spots the impending calamity early and sounds the alarm. Of course, everyone ignores them – it wouldn't be much of a movie if they didn't – until it's too late. Then, once catastrophe strikes, the rest of the world turns to that person to solve the problem, which he or she proceeds to do.

Hopefully, life doesn't always imitate art – because there is an impending cataclysm in IT that can be avoided if we act now. The alarm is being sounded today. The question is, "Will anyone listen?"

The question is, "Will anyone listen?"

What is this event threatening such upheaval? Essentially, many organizations that depend on SAP for ERP, PLM, HR and other functions are living on borrowed time. Especially for thinly staffed mid-size enterprises.

To understand why, you first have to look at how SAP is integral to the enterprise. It is a very large and complex system that is thoroughly ingrained into the operations of those enterprises. It may have taken a while for organizations to fully harness its power, but today it is the enterprise's most mission-critical system.

Despite SAP being an integral part of the fabric of business, when the economy took a downturn, enterprises began making deep cuts into IT budgets. IT staffing and operations budgets have been pared to a minimum. Especially hard hit are the internal SAP support teams. Many original core team members have gone back to their business units or moved on. Too many IT organizations are supporting their mission-critical SAP applications with under-staffed, poorly trained, cobbled together internal teams.

So now you have a situation where business units rely heavily on SAP for day-to-day operations and strategic information, yet there is now too often only a skeleton crew – in many cases without adequate knowledge and training – to support their most mission-critical IT application. In these environments, urgent system maintenance is being deferred, or worse, simply overlooked. Enterprises with loosely coupled IT "silos" of operations bear a greater risk as the cumulative sum of critical competencies in multiple SAP-related IT disciplines (e.g. OS, SAN, database, Basis & functional) are lost or diluted.

It is all too likely that these factors are creating an environment where SAP is going to go down, and down hard. Enterprises have grown so used to trouble-free SAP operations that manual work-around procedures in the absence of SAP are lost. A prolonged outage of SAP can affect hundreds of users, and bring the enterprise to a grinding halt. And given the Just in Time (JIT) nature of business these days, one company having an issue can affect everyone else up- and downstream.

On any given day, these enterprises deal with a combination of factors that could lead to a disaster scenario. SAP is a dynamic, constantly growing system that must be proactively monitored for changes that impact its stability. For instance, sizing must be monitored to ensure the system has enough disk space to operate; otherwise, the enterprise risks SAP stopping. System performance also changes over time as new applications are added. While a performance issue isn't likely to stop the system, it will cost the organization in terms of lost productivity and frustrated end users.

SAP security is another overlooked area that requires constant maintenance due to staff turnover and job function changes, as well as constant monitoring for security breaches.

At the majority of enterprises, staff is given or accidentally receives too much access to the SAP system, leaving the enterprise open to fraud and embezzlement. Publicly traded enterprises are required by law to undergo regular compliance audits, although this doesn't guarantee that their security controls are being proactively monitored. Privately held enterprises often put themselves at even greater risk because they don't believe they need controls and argue that they can't afford the investment in tools or expertise. In reality, both public and private enterprises can benefit from the more affordable second generation of governance, risk and compliance (GRC) tools on the market. These tools proactively monitor the environment for security breaches, and help cut costs and free up IT teams with time-saving task automation features.

IT departments that try to cut costs by having a single staff member perform multiple job functions are not only setting that person up for failure, but they also are setting up their enterprise for a true disaster. SAP is complex: One person simply cannot possess all of the application specific expertise necessary to manage an environment. And unfortunately there is no "undo" button in SAP. Inexperience has resulted in mistakes ranging from deleting critical data to shutting down the entire system.

When an issue does arise, enterprises find that a lack of staff continuity has left them without access to expertise, and more critically, knowledge of their own environment. For every hour an SAP environment is nonfunctional, an enterprise can lose thousands of dollars in revenue. When support continuity is fractured, the enterprise bears the "cost of discovery" as staff try to determine why something was originally configured or coded the way it was, and research the fix.

Every good disaster movie has a twist in the plot. In the case of the SAP enterprise, the twist comes when a disaster is declared and the enterprise's disaster recovery (DR) plan fails. Disaster recovery is one of the first areas to be affected by resource cuts. The result is that many plans are never properly tested. Often, the enterprise grows and implements new applications or acquires new business, but the DR plan and DR environment haven't kept pace with the changes. Or, it may not cover everything necessary to run the business e.g. SAP, email, faxes, EDI and warehousing.

As with any good disaster movie, however, there is a solution. It's a technical managed services model designed for the realities of 21st Century business.

Unlike the managed services models of the past, which took an all-or-nothing approach to managing SAP, the 21st Century model provides a flexible approach that allows enterprises to blend outsourced management of their SAP technical services with internal IT staff to provide reliable, cost-effective SAP operations. This yields an optimal combination of knowledge of your business and access to deep, broad SAP expertise.

Having a dedicated team is a key factor. In the past, technical managed services providers would have a pool of SAP experts who would field calls as they came in. Often, there would be a lag in responsiveness as the expert familiarized himself with the client's specific SAP system. Hours of frustration would be lost explaining and re-explaining a SAP production issue to some stranger(s) half a world away.

In today's JIT world, that lag-time is no longer acceptable or practical. When a client calls with an issue, it needs an immediate response from someone who knows her SAP environment intimately. This is not to say the front-line expert can't tap into a deeper pool of knowledge as-needed; that is both advisable and desirable. But quality support must start with someone who knows the particular SAP landscapes, and knows the client-side team.

The real benefit of this approach – and the ability to avoid disaster – comes not with specific issues but in the day-to-day management of the SAP environment.

Let's face it. No one really likes doing day-to-day SAP production support, like monitoring systems. It is necessary, but isn't as exciting as a major project initiative. It's also not the most efficient or profitable use of an already minimal internal staff. Yet keeping the SAP environment running, and averting preventable outages, is critical to any enterprise.

By engaging with a 21st Century technical managed services provider, enterprises can offload day-to-day SAP production support, freeing the internal team to support more value-add, business facing innovation. The goal is to convert internal IT staff's time from just "keep the lights on" operations to supporting more strategic initiatives.

At the same time, because the provider works with multiple SAP systems, they have the critical mass to build a world-class SAP support organization; to create automated tools to monitor them; and then supplement that with pro-active human assessments to see what the business rules didn't catch. It is this combination of technology and human decision-making that yields superior results – and minimizes downtime, which is sure to please the CFO as well as the rest of the C-suite.

Of course, while that all sounds well and good, enterprises today must also be conscious of budget considerations. Fortunately, the 21st Century model for technical managed services is less expensive than 20th Century models for total out-sourcing, or conversely, fully staffing with internal resources. There are documented cases where enterprises which moved to a 21st Century SAP model were able to fund an upgrade from the savings in production support costs. In others, they were able to bring innovations and ideas to the table – all because they had the time to pursue innovation rather than "just keeping the lights on" managing their existing SAP landscapes.

One other financial consideration is how the partnership is structured. In the 20th Century model, technical managed services providers were paid by the hour. They could afford to quote minimal hours to achieve a low price, because they could always claim "scope creep" later to justify a higher total cost.

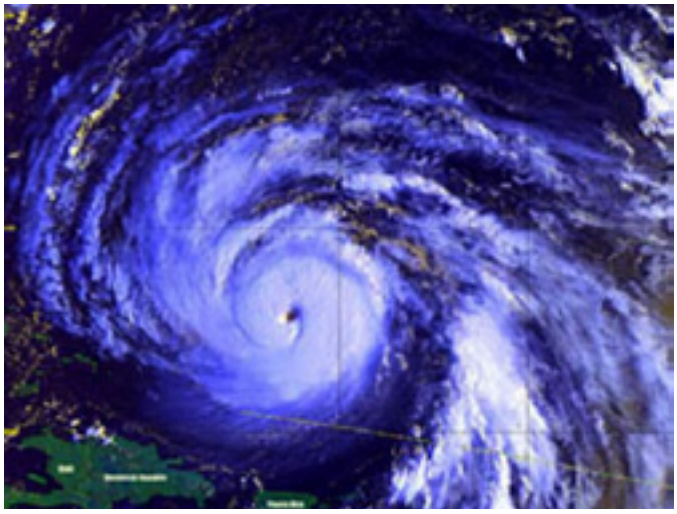
In the 21st Century model, however, providers offer, and are held to, flat fees. As a result, the true cost is predictable, and the provider is incented to complete the work quickly. They are also incented to do the job well since any fixes to a Band-Aid solution will come out of their own profitability, not the enterprise's IT budget.

For SAP enterprises, it really comes down to one of two choices: They can either follow the disaster movie formula, and ignore the very serious warning signs facing them today. Or they can listen to the rumblings now and move to a 21st Century technical managed services model before the Big One hits. Because it's not a question of "if"; it's only a question of "when." And you can bet the "when" will happen when it hurts the most.

Dan Wilhelms is President and C.E.O. of Symmetry Corporation (www.sym-corp.com), an SAP® hosting partner that provides technical managed services, security administration and project consulting for SAP customers in the U.S. and around the world. He can be reached at dwilhelms@sym-corp.com.

Call for Speakers

NaSTEC is returning to Chicago October 16 and still has available slots for conference speakers and moderators. In addition to the superb exposure you and your organization will receive at this year's NaSTEC, we are offering other incentives and promotional opportunities that would complement your participation. This year's theme is IT Career Development for the Novice, Practitioner and Veteran. That's a very broad canvass that offers significant opportunity for compelling presentations. If you are prepared to speak about professional development, and/or a timely and relevant technical topic of interest to IT, professionals, please contact NaSPA President Leo A. Wrobel, president@naspa.com.
See you in October!



Part II of III: Understanding and Mitigating Severe Weather Events

By Sharon M. Wrobel

Figure 1 Photo courtesy of NOAA/NCEP

In the last issue of *Technical Support*, we were getting ready for tornado season and as predicted it has already been a very active season. In part II of this series we will delve into the realm of hurricanes. We will discuss how they are formed, how they are named and how you can protect yourself as well as your business. Not to be outdone by tornado season, FEMA predicts that this will also be an unusually high season for hurricanes.

What is a Hurricane?

Depending on where you live determines what this non-frontal system is called. It's identified as a hurricane if one lives in the Northern Hemisphere, which includes the following bodies of water: Atlantic, Caribbean, Gulf of Mexico and the Central Pacific. The season runs from June through November and the storm takes on a counterclockwise rotation. If one lives near the Pacific Ocean north of the Equator and west of the International Dateline, it is called a typhoon. Rotation takes on a clockwise motion and goes from late October until early May. A cyclone occurs in the Arabian Sea and the Bay of Bengal. This occurs mostly in the Bay of Bengal as the waters are normally warmer than those in the Arabian Sea. The rotation in these cyclones appears to go in a counterclockwise motion.

How are Hurricanes formed?

Hurricanes form over tropical areas of the ocean when the temperature of the water hits 80º F. Several thunderstorms form together creating a tropical disturbance that starts to organize and move in a circular rotation. When the winds are less than 38 mph the storm is classified as a tropical depression but once wind speeds of 39 mph are maintained it is given a name to identify and track it. A hurricane forms when enough energy from water vapor is pulled up from the warm ocean surface by upper level winds. At 74 mph it develops into a hurricane. The "eye" of the hurricane forms in the middle where there is no weather and is surrounded by intense winds and a rotating cloud mass. The smaller the eye, the stronger the storm. The hurricane loses energy once it crosses land or cooler waters. They have been known to last as long as two weeks.

The Saffir-Simpson Hurricane Wind Scale

The Saffir-Simpson Hurricane Wind Scale determines the impact on the United States coast utilizing five categories based on wind speed. In this newly adopted hurricane scale, storm surge and flooding effects will no longer apply as they did in the original Saffir-Simpson Scale.

- Category One hurricanes have maximum sustained winds of 74-95 mph creating minimal damage. Hurricane Gaston is an example of one such hurricane that hit South Carolina in 2004.
- Category Two hurricanes have maximum sustained winds of 96-110 mph creating moderate amounts of damage. Hurricane Isabel hit North Carolina in 2003.
- Category Three hurricanes are more intense carrying wind speeds of 111-130 mph and creating extensive damage. Hurricane Katrina was a category three hurricane that impacted Louisiana in 2005.
- Category Four hurricanes have maximum sustained wind speeds of 131-155 mph creating extreme damage. An example of this storm is Hurricane Iniki when it hit Hawaii in 1992.
- Category Five hurricanes have maximum sustained wind speeds of over 155 mph creating catastrophic damage. Fortunately, only a few Category Five hurricanes have been recorded in the United States. Two of these were Hurricane Camille in 1969 and Hurricane Andrew in 1992.

How are Hurricanes named?

First, tropical depressions are numbered from a weak Category 1 to a catastrophic Category 5. 80-100 tropical storms form annually and only half of those actually become hurricanes.

Tropical storms or hurricanes are issued a name. In 1953, hurricanes only had female names. Both female and male names were alphabeti-

A little trivia for you: The name hurricane comes from the Central American deity of wind called Huracan.

cally used in an alternate fashion by 1979. These names are dispersed on six lists that are used in rotation. This year, 2010's list, was last used in 2004. Names of hurricanes are deleted when a devastating storm occurs and replaced by others in consideration of the affected people. You will note that Ivan is not used this year and next year's list does not have a Katrina or Rita on it.

What can you do to protect yourself as well as your business against a potential Hurricane?

You need to know what type of damage results from hurricanes. The leading cause of death is the storm surge, which we know can be as little as 3 feet to over 18 feet. People love to go out to the water to see the surf forgetting that it has the potential to knock one over especially combined with wind gusts. Or they drive into a flooded area thinking they can get through it. As you've been taught over and over; turn around don't drown! Next is wind damage, which can begin at 74 mph for a Category One Hurricane and increase to over 155 mph. Finally, heavy rains can break levees, overflow riverbanks and dislodge bridges as seen in the aftermath of Katrina. So, what should one do?

FEMA recommendations:

1. **Permanent storm shutters #1 best overall protection**
2. **5/8" marine plywood cut to size; ready to install**
3. **Tape is a waste of time as windows still break**
4. **Keep trees and shrubs trimmed back**
5. **Unclog gutters and downspouts so water has a place to drain**
6. **Install a safe room**
7. **Generator**

Protect Your Property from Flooding

- Build With Flood Damage Resistant Materials
- Dry Floodproof Your Building
- Add Waterproof Veneer to Exterior Walls
- Raise Electrical System Components
- Anchor Fuel Tanks
- Raise or Floodproof HVAC Equipment
- Install Sewer Backflow Valves
- Protect Wells From Contamination by Flooding

Protect Your Property from High Winds

- Maintain Exterior Insulation and Finish System (EIFS) Walls
- Protect Windows and Doors with Covers
- Reinforce Double Entry Doors
- Reinforce or Replace Garage Doors
- Remove Trees and Potential Windborne Missiles
- Secure Metal Siding and Metal Roofs
- Secure Built-Up and Single-Ply Roofs
- Secure Composition Shingle Roofs
- Brace Gable End Roof Framing

Summary

We hope that this hurricane season is light especially with the Gulf oil spill still not completely cleaned up at the time of this writing. But in the event that nature doesn't cooperate and Murphy's Law is alive and well, we hope that you have come away with something you didn't know about hurricanes and the ways to ensure your safety in and about your workplace and home. For more information please go to: http://www.weather.gov/om/hurricane/index.shtml. Another useful resource for hurricane and other disasters is the Pacific Disaster Center (www.pdc.org) and their Global Hazards Atlas (www.pdc.org/atlas).

In the last of the three part series, through no "fault" of our own, we'll take a "crack" at earthquakes. Anyway…..☺

Sharon M. (Ford) Wrobel conducted extensive publishing and regulatory research for her former employer, (a 50 state telephone company), a function she continues today as Vice President of Business Development for b4Ci Inc. Sharon was a major content contributor to Leo's 2009 book "Business Resumption Planning Second Edition" © Taylor Publishing Inc, and was co-author of Leo's latest book "Disaster Recovery for Communications and Critical Infrastructure" © 2009 Artech House Books Inc. She has published over a dozen trade articles in 2008-2010 alone. Sharon attended the University of Maryland and El Centro College in Dallas where she trained as a registered nurse before joining Leo in his businesses. Sharon is a member of NaSPA, the Association of Contingency Planners and the Community Emergency Response Team. Sharon also served honorably as a public official, accepting appointments to the City's Planning and Zoning and Historical Commissions. For more on Sharon, including her Disaster Recovery articles, click http://www.informit.com/authors/bio.aspx?a=cc5bc70e-b2fe-44ff-bad9-2c174d2a9533

The NaSPA Community is looking for you.

Don't wait for your picture to appear on the side of a milk carton. Take advantage of a special "Back to the Future" opportunity that NaSPA is offering to REACTIVATE your NaSPA Membership.

Don't miss out on all the exciting services and benefits that NaSPA has to offer. Reactivate your NaSPA membership today.

To reactivate your NaSPA membership, click here for www.NaSPA.com, and come back to the NaSPA Community.

For information call our Missing Member info line 414-908-4946, Ext. 450.

To find out more about the services and benefits that NaSPA has to offer, go to www.NaSPA.com

NaSPA
NETWORK AND SYSTEMS PROFESSIONALS ASSOCIATION

Careers | Connections | Skills | Success

JOIN NaSPA TODAY
www.NaSPA.com

Please complete this form and fax it to (414) 768-8001

❑ **Yes, I want to become a NaSPA member!**

Name_____

Signature_____ Date _____
required

Title _____ Company _____

E-mail Address _____

Address _____

City _____ State/Province _____ Zip _____

Country _____ Phone (____) _____

Address shown is: ❑ Home ❑ Work

System software you work with: (check all that apply)

1. ❑ MVS-IBM 2. ❑ VM-IBM 3. ❑ VSE-IBM 4. ❑ Windows Workstation
5. ❑ Windows-Server 6. ❑ UNIX-All 7. ❑ UNIX-Linux 8. ❑ NetWare-Novell
A. ❑ AS/400(OS/400)-IBM B. ❑ Macintosh-Apple
C. ❑ VMware Z. ❑ Other_____
please specify

Payment Method:

❑ Check ❑ MasterCard ❑ Discover ❑ Visa ❑ American Express

Card # _____Exp. Date _____

ADVERTISER DIRECTORY

ADVERTISER	URL	PAGE
Appsense	www.appsense.com	6
b4Ci, Inc.	www.b4ci.com	18
Clearview	www.cvglobal.com	25
CRC Press	www.crcpress.com	28
Liberty Mutual	www.libertymutual.com	5
Pano Logic	www.panologic.com	7
PDC	www.pdc.org	14
Security Recruiter	www.securityrecruiter.com	16
Symmetry	www.sym-corp.com	10

SERVICE DIRECTORY

MEMBERSHIP INFORMATION
- Address Changes
- Dues Payment
- Membership Status/Applications
- User ID/Password Inquiries
- Publication Back Issues

Contact Carrie Banacin
Membership Manager
(414) 908-4945, Ext. 116
NaSPA_membership@NaSPA.com

PUBLISHING INFORMATION
- Article Submissions
- *NaSPA E-News*
- Letters to the Editor
- Copyright Inquiries

Contact Leo A. Wrobel
Editor-in-Chief
President@NaSPA.com

CUSTOMERCARE CENTER

Contact Bonnie Kuchinski
(414) 908-4945, Ext. 450
customercare@NaSPA.com

MEMBER SERVICES/CHAPTERS
- Chapter Start-up Kit
- NaSPA Direct
- Discount Programs

Contact Alex Llanas
Marketing Coordinator
(414) 908-4945, Ext. 123
a.llanas@NaSPA.com

ADVERTISING SALES
- Advertising in *Technical Support*™
- *NaSPA E-News* sales
- *Reprints*

Contact Don McMurray
Sales Director
(414) 908-4945, Ext. 111
dmcmurray@NaSPA.com

NaSPA INFORMATION
- Board of Directors
- NaSPA Focus and Direction
- Industry Issues and Trends

Contact Leo A. Wrobel
President
president@NaSPA.com

MEMBERSHIP CATEGORIES (CHOOSE ONE)

❑ **Subscriber**	• *Technical Support*™ magazine • NaSPA luggage tag • *Rate per year: $40 U.S., $45 International*
❑ **Gold**	• *Technical Support*™ magazine • Member ID Card & Certificate of Membership • Members only web access • All member discounts and services • One e-mail account • NaSPA luggage tag • *Rate per year: $45 U.S., $60 International*
❑ **Platinum**	• *Technical Support*™ magazine • Member ID Card & Certificate of Membership • Members only web access • All member discounts and services • Two e-mail accounts • NaSPA luggage tag • *Rate per year: $95 U.S., $110 International*
❑ **Faculty**	• *Technical Support*™ magazine • Member ID Card & Certificate of Membership • Members only web access • All member discounts and services • One e-mail account • NaSPA luggage tag • *Rate per year: $20 U.S., $20 International*
❑ **Retired**	• *Technical Support*™ magazine • Member ID Card & Certificate of Membership • Members only web access • All member discounts and services • One e-mail account • NaSPA luggage tag • *Rate per year: $20 U.S., $25 International*
❑ **Student**	• *Technical Support*™ magazine • Member ID Card & Certificate of Membership • Members only web access • All member discounts and services • One e-mail account • NaSPA luggage tag • *Rate per year: $20 U.S., $26 International*
❑ **Group**	• *Technical Support*™ magazine • Member ID Card & Certificate of Membership • Members only web access • All member discounts and services • NaSPA luggage tag • One e-mail account per member • *Rate per year (for up to five members):* *$150 U.S., $150 International*
❑ **Life**	• *Technical Support*™ magazine • Member ID Card & Certificate of Membership • Members only web access • All member discounts and services • Two e-mail accounts • NaSPA luggage tag • Choice of one NaSPA appreciation gift* • An individual Web site account with 20mb of space • *Rate: $995 U.S., $1,010 International*
❑ **Corporate**	• *Technical Support*™ magazine • Five memberships • Member ID Card & Certificate of Membership • Members only web access • All member discounts and services • NaSPA luggage tag • Unlimited Job Postings for one year • Choice of one NaSPA appreciation gift* • *Rate per year: $1,850 U.S., $1,850 International*

***Gifts are available at the time of paid membership renewal only.**

Virtualization & Network Solutions

Fortify Security

Minimize Downtime

Boost Energy Efficiency

SAVE 15%

- Support and sustain business growth with a next-generation virtual data center
- Create a rock-solid recovery plan for any size organization
- The ultimate guide to the VCP exam
- Protect your systems from the disastrous loss of data
- Slash business costs and streamline your data center with state-of-the-art virtualization methods
- Cut costs while improving functionality
- A step-by-step guide for implementing server virtualization
- Maintain content integrity and network assurance

CRC Press
Taylor & Francis Group
AN AUERBACH BOOK

From the premier publisher for IT professionals

Use **Promo Code 405EA** when ordering and **SAVE 15%!** Expires 7/31/09

www.CRCPRESS.com

CONTENTS

JUNE 2010 VOLUME 2, NUMBER 2 1

VERBAL and Written
Communication Skills
for Technology Professionals 1