technical® SUPPORT

Supporting Enterprise Networks and Operating Environments

JUNE 2014 VOLUME 6, NUMBER 6

Why College Students Should Also Run a Business

By Matt Stewart

From the Editor-in-Chief

Message from the President

Well, June has quickly crept up on us and excitement is in the air for all the new graduates. Congratulations to the Class of 2014! Now what do you do? First, join NaSPA. Do it now. It's free! Then visit the NaSPA web site and find that perfect job.

- Check out this month's center section of NaSPA's Technical Support Magazine for the highlighted jobs.
- Click the link at the end of the center section to see ALL the jobs – there are literally thousands of them and they are updated constantly through NaSPA's longtime partner, Job Target.
- Post your resume on our job site. It's viewed by thousands of readers each month!
- Read this month's featured article Why College Students Should Also Run a Business by Matt Stewart.
- Get noticed, publish your own article in a future edition of Technical Support.

We also have a slate of other great articles this month including *Getting Your Disaster Recovery Plan Funded with an Awesome Business Impact Analysis, Part 3 of 3*, (by yours truly and Sharon Wrobel), *"Doing the Math on IT Complexity Part 2 of 3"* by longtime NaSPA member Bill Elder and Roger Sessions. Concerned about the recent end of Windows XP support, or just viruses and vulnerability in general? You may want to have a look at *"Resuming Business Operations After a Virus Infection"* by Ajay Gupa. Need tips creating a team? Check out "*Seven Tips for Hiring "A Players"* by Richard Bryan.

As always there is lot to enjoy in this month's edition, and tons of great information. Tell your friends and employers about NaSPA and encourage them to join so that they too can enjoy these great resources and benefits. After all, it's free!

Best of luck graduates, see you in the workforce!
Leo A. Wrobel
Editor in Chief Technical Support Magazine
President, NaSPA, President@Naspa.com

technical SUPPORT
Supporting Enterprise Networks and Operating Environments

NaSPA

June 2014
Volume 6, Number 6

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

www.NaSPA.com

NaSPA Officers

President	Leo A. Wrobel
Secretary/Treasurer	Sharon M. Wrobel

NaSPA Board of Directors

Chairman	Scott Sherer
Directors	Leo A. Wrobel Sharon M. Wrobel
Board Advisor	Bill Elder

e-mail addressses available on www.NaSPA.com

Technical Support™ Magazine

Editor-in-Chief	Leo A. Wrobel president@NaSPA.com
Managing Editor	Sharon M. Wrobel sharon@b4ci.com
Associate Editor	Jim Justen jmjusten@gmail.com
Graphic Designer	Michelle Majerus-Uelmen graphics@techenterprises.net
Vice President of Staff Operations	Scott Sherer sherer@NaSPA.com
Membership Department	Nicole Cheever, 414-908-4945 Ext. 116, Manager NaSPA_membership@NaSPA.com
Advertising Sales	Jill Tucker, 414-908-4945 Ext. 111 j.tucker@NaSPA.com
CustomerCare Center	Bonnie Kuchinski, 414-908-4945 Ext. 450 customercare@NaSPA.com
List Rental	Jill Tucker, 414-908-4945 Ext. 111 j.tucker@NaSPA.com

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

Notice: You have received this magazine because you are a member of NaSPA, the Network and Systems Professionals Association, Inc., or you are a NaSPA subscriber. NaSPA believes this publication to be of value to you and your career. If you wish to opt-out and not receive this magazine in the future or would like to change your delivery address, please send an email with your request to Customer Care, customercare@NaSPA.com.

June 2014 Volume 6, Number 6

ARTICLES

Call for Authors

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*.

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.

The information and articles in this magazine have not been subjected to any formal testing by NaSPA, Inc. or Technical Enterprises, Inc. The implementation, use and/or selection of software, hardware, or procedures presented within this publication and the results obtained from such selection or implementation, is the responsibility of the reader.

Articles and information will be presented as technically correct as possible, to the best knowledge of the author and editors. If the reader intends to make use of any of the information presented in this publication, please verify and test any and all procedures selected. Technical inaccuracies may arise from printing errors, new developments in the industry and/or changes or enhancements to components, either hardware or software.

The opinions expressed by the authors who contribute to *NaSPA Technical Support* are their own and do not necessarily reflect the official policy of NaSPA, Inc. Articles may be submitted by members of NaSPA, Inc. The articles should be within the scope of host-based, distributed platforms, network communications and data base, and should be a subject of interest to the members and based on the author's experience. Please call or write for more information. Upon publication, all letters, stories and articles become the property of NaSPA, Inc. and may be distributed to, and used by, all of its members.

NaSPA, Inc. is a not-for-profit, independent corporation and is not owned in whole or in part by any manufacturer of software or hardware. All corporate computing professionals are welcome to join NaSPA, Inc. For information on joining NaSPA and for membership rates, see www.NaSPA.com.

Notice: You have received this email because you are a member of NaSPA http://www.NaSPA.com, the Network and Systems Professionals Association, Inc., or a subscriber to *Technical Support* magazine. NaSPA believes this publication to be of value to you and your career. If you wish to opt-out and not receive this magazine in the future or would like to change your delivery address, please send an email with your request to Customer Care, customercare@NaSPA.com.

All product names and visual representations published in this magazine are the trademarks/registered trademarks of their respective manufacturers.

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

Getting Your Disaster Recovery Plan Funded - with an *Awesome* Business Impact Analysis: Part 3 of 3, Tips to Turn Your Risk Analysis into Endorsement and FUNDING

By Leo A. Wrobel and Sharon M. Wrobel

Last month we discussed the first two things that management positively needs to know in order to support and fund your disaster recovery planning effort:

1. What can happen?
2. What is the Probability that it will happen?

This month we continue our discussion of techniques for securing approval and funding for your disaster recovery planning effort with the second two things management positively needs to know.

3. What does it COST when it happens?
4. What does it COST to make the problem go away?

In this regard we take up where we left off, with the **F**ailure **M**ode **E**ffects **A**nalysis (FMEA). After showing where the FMEA fits into your executive presentation, we conclude with a couple more examples that speak specifically to the last two questions above that management must have answered before they endorse and fund your plan. Our hope is to impart some compelling tools you can use to illustrate both of these issues, even to non- technical executives, which can and will get your plan funded.

Convincing management that you are the right person for the job can take a little bit of finesse.

Presentation is Everything

Ask yourself this question: Where do you get the best FOOD in the world? Answer: Your mother's house. Your mom has lots of experience, the food is good, and if you come from an Italian household like I do, it is also served in massive quantities. If I were to ask YOU to come and eat at Mom's house, you would probably be apprehensive. This is because you lack first hand experience that testifies that my mother is a great cook. In fact, you could truly be fearful of what you might get when you sit down to eat. Set in this context, where could we both agree to eat? Answer: The French restaurant. The food there BETTER be good, because dinner for two can cost $300 or more. More importantly, the PRESENTATION will be great, with just the perfect sauce and pizzazz. Not only will you not be apprehensive about eating at the French restaurant, you might even sit down and eat something that nobody in their right mind would normally eat. (For example, French chefs prepare escargot.) The presentation and sauces however would be SO good that you would probably give it a try.

It is very much the same way with Disaster Recovery consultants. No matter how good a cook YOU are, management has no frame of reference that proves you are a good cook. They are going to be apprehensive. And just like my eating at your Mom's, they are going to be skeptical of your abilities as a Disaster Recovery chef. But what could both you and your management agree on today? Answer: An expensive consultant. The expensive consultant is the corollary to the French chef in this example. Management knows that like the French restaurant, the consultant will be expensive. Also like the restaurant, management knows that the product will be GOOD. But is paying $400 an hour for a consultant really in your organization's best interest? Will a consultant know YOUR environment as well as you do? Will you even be able to claim ownership for the business resumption plan after the consultant produces it for you? Notwithstanding the financial impact of such a project, these are some of the questions you should be asking. It might be more advantageous to use some of the "tricks of the trade" that the expensive consultants use to communicate and sell their services. In short, here are some things that prove to management that YOU know how to cook. Let's look at a few ideas:

Management's Perception of Risk May Differ From Yours

If you ask ten people in a room, each with identical income, bills, homes, cars and number of dependents how much life insurance is enough to carry you will get ten different answers. Some people are risk adverse and want the maximum amount of protection they can afford. Others want the least they can get by with. The same holds true with decision-making executives. Since you probably will not know in advance what the persuasion of your audience is, concentrate on giving them accurate probability data that spells out precisely how exposed they are to a catastrophic event. With this in mind, how does one know the PROBABLITY that a given piece of equipment will fail? That's where you come in as a technologist. You probably have a pretty good idea of the risks but need some tips for communicating them to Management; in terms they can understand. After all, Management will need to know the probability of a failure in order to commit to funding your effort. They will also need to UNDERSTAND where you got your figures in order to back them up with cash. In this regard, I found a way to quantify the probability of a catastrophic failure in a piece of equipment or a system that I am especially fond of. It's called a FMEA (not to be confused with FEMA) which stands for Failure Mode Effects Analysis. I became familiar with this method in part from a conversation with a former Air Force General who was then the CIO of a $75 billion financial services organization. Essentially everything looking down at Iraq today was put into orbit by this guy's subordinates when he was still active duty. He summed it up this way:

> **"When we send up a military satellite, everything has to be perfect the first time. This is**

because no one has yet invented a 23,000 mile long screwdriver to fix it if it is not."

I got the feeling from his tone that this was the voice of experience. Being a veteran myself however (a Sergeant not a General) I could only imagine how many butts would be on the line if someone botched a $100 million satellite launch. Therefore in order to enhance its odds of getting it right the first time, the military uses FMEA to compute the probability something really pear-shaped might happen. It goes something like this:

1. Identify every mission critical component that could fail.
2. Compute or acquire from the manufacturer a MTBF (mean time between failure) for each identified mission critical component.
3. Combine the failure probabilities into a single mathematical factor that describes the probability of failure of a given system.
4. Use these figures to justify and prioritize expenditures to "harden" equipment rooms, networks or other facilities.

One can actually adapt this same military FMEA methodology and use it as contingency planners in corporations. We adopted the Internet, right? Like so many other aspects of recovery planning, here is another military invention we can dust off for commercial use.

Suppose you are tasked with performing a detailed analysis of your equipment room and associated networks. The objective of this analysis is to determine single points of failure, critical components that cause failures to multiple users and an overall assessment of past performance or incidents. In order to describe this information, your FMEA will be broken down into three steps:

1. The Problem Identification step. The rule of thumb is to ask, "What can possibly go wrong?" This includes both failure rates of the equipment itself as well as the external factors (heat, water, air, people, etc) which could affect it. Refer back to previous articles in this series for tips on how to complete this step.
2. The second step is to assign a Risk Priority Number or RPN value, also as we showed in part 2 of this series, to each of the issues you identified. Pick a number from 1 to 10. The higher the number, the greater the associated risk. (Except in the case of problem resolution, where the higher the number, the better your speed in fixing the problem, as you will see below)
3. The third and final component is to quantify the reaction process. This is the *"How fast can we fix the problem?"* step. (This step is shortened by modifying your company's Operating and Security Standards to moderate the risk and change the environment to make the selected systems more survivable) If you look back in part 2 of this series this is presented as S (severity) X F (frequency) X D (detection). The three of these factors are multiplied together form the Risk Priority Number or **RPN.**

Once you have the "ingredients" you need to cook in the form of the FMEA, then it is possible to borrow the "recipe" (presentation techniques) of an expensive French chef (consultant) to whip them into something delicious that management will swallow and enjoy. A few techniques for doing this follow.

QUANTIFYING PROBABILITY

1. Where Do You Get Probability Data?
   A. Personal Experience
   B. Experience of Your Organization
   C. Experience of Others
   D. Research
   E. Trade Groups

2. Insurance Companies / Actuarial Tables
3. NFPA
4. FEMA, National Weather Service, Other Agencies

Tools and Visuals that Communicate Disaster Recovery Concepts

Good consultants make extensive use of pictures and graphs to communicate abstract concepts, since executives have little time to do a lot of reading. Consider some of the following tools often used by high paid consultants use to communicate to management. For example, organize your data into an understandable matrix that can be quickly understood and absorbed by an executive. Please refer to the following example.

- Start by considering each of the specific items from the previous articles that are nasty things that could befall your organization. (Fire, flooding, disgruntled employee, lightning, power failure, etc) List each of these items (or the top 20 based on the results of your Failure Mode Effects Analysis or FMEA) in the first column.

Label this first column **“What Can Happen”** or **EVENT**. For the sake of discussion, let’s say the first **EVENT** is the possibility of “water in the equipment room.”

- Label the second column “**PROBABILITY**.” What is the probability that a leak in the equipment room will occur? As we have stated in previous articles, you can’t just dream up a percentage figure and stay credible, but there are sources where you could get one. For example, the NFPA (National Fire Prevention Association) might have an idea, or consider asking an insurance company, they have actuarial tables for disasters. The important thing is don’t make one up – get one from someone that knows.
- The third should be labeled **“Cost When it Happens.”** This is a figure you will want to get from that Vice President of Sales or another person that the executive holds in confidence. A sales VP is good however because this person may have an incentive plan based on sales that decides his or her commission. I can bet they would be able to venture a plausible estimate of lost sales.
- Add another column that contains a figure for how many days (1/2 day, three days, seven days) such a disaster would disrupt operations. As you can already see, management will take the “Cost” figure in the previous column and multiply it by the “time in days” figure. This is by design. Rather than concentrating on the technology, management is concentrating on the money. This is how it should be, and how it will be if you do a good job at substantiating the figures.
- The next column “Cost of New Capability” is where you are asking for the money you need. Note however how management can now make a decision without concentrating on the technology. It is remotely probable in fact that management will not even KNOW what the piece of equipment is that you are asking for. If you are asking for fire extinguishers for the equipment room for example that is one thing. If you are asking for route diversity on a dual fed counter rotating fiber optic ring from the telco, they are not intuitively going to know what that is – except by referring back to the “what can happen” column. In that case it would say “Telephone cable cut.” Most executives know what those are.
- Finally, since you will be asking for a lot of money in the form of many different things, add a **“Priority”** column. This helps everyone understand that the lack of a fire prevention system in the equipment room is a higher priority than, for example, the failure of a small work group.

Now that you have gone through this example, albeit a very modest example, ask yourself how the proposal to your executives would have gone if you only started with the column that asked for money - and skipped the other essential columns! Yet this is exactly what technologists do year after year, not because they don’t know what they need but because they don’t know how to communicate that need effectively to management, in terms management can understand.

PRESENTING THE PROBABILITY OF A DISASTER TO MANAGEMENT

1. Figures must be substantiated
2. Figures must be relevant to your organization
3. Best to express in % probability
4. Figures must communicate easily. (Use color, charts, graphs, if possible)
5. Consider conducting a Failure Mode Effects Analysis (FMEA)

EVENT	PROBABILITY	COST OF OUTAGE PER DAY	TIME IN DAYS	COST OF NEW CAPABILITY	FINANCIAL BENEFIT/ PRIORITY
				TOTAL	$

CHARACTERISTICS OF A GOOD PRESENTATION

1. Brief, 3-4 slides, Use Good VISUAL Media
2. Well-researched
3. Validated with persons the executive holds in confidence.
4. Must cover the "Four Things" an executive needs to know in terms the executive understands.

- What Can Happen?
- What is the Probability it will happen?
- What does it COST when it Happens?
- How Much to Make the Problem Go Away?

SUBSTANTIATE CONCLUSIONS WITH PEOPLE MANAGEMENT HOLDS IN CONFIDENCE

1. Corporate Controller/CFO
2. General Counsel
3. Vice President Sales
4. Vice President Marketing
5. Vice President Production
6. Subsidiary/ Corporate Officers
7. Vice President MIS/Technical Services
8. Others

Summary

Needless to say, even after three articles there is still a LOT more to a successful executive presentation. If you would like more information, perhaps you might want to order my book, *Business Resumption Planning Second Edition*, © 2008 Taylor Publishing Inc.

Hopefully, these examples will jog a few ideas loose on how to present a compelling funding request to executive management. Note that almost without exception, the slides and communications mediums used speak to *business issues* and not *technical issues*. Business terminology is the topic in which the executives will be conversant, not technology issues and a good consultant always writes for his audience.

By establishing "hard" and substantiated probabilities, backed by individuals that management holds in confidence, it *may not even be necessary* that management understand precisely what the technical capability of the equipment you propose is! It is more important that they clearly understand the business risk your proposed solution is alleviating so that they can make informed decisions. The comfort level you establish with them in this regard translates directly into approval of purchases, project funding and general support.

If you follow the rules in this article series we are confident you will convince your management that you too can be a master chef, and that they can safely swallow anything you cook up in the way of disaster recovery. Best of luck in your pursuits!

Leo A. Wrobel has over 30 years of experience with a host of firms engaged in banking, manufacturing, telecom services and government. An active author and technical futurist, he has published ten books and over 400 trade articles on a wide variety of technical subjects. Leo served ten years as an elected Mayor and City Councilman (but says he is "better now"). A sought-after speaker, he has lectured throughout the United States and overseas and has appeared on several television news programs. Leo is presently CEO of Dallas-based TelLAWCom Labs Inc, and b4Ci. Inc. See www.b4Ci.com call (214) 888-1300 or email leo@b4ci.com.

Sharon M. (Ford) Wrobel is a Director at NaSPA and Managing Editor for Technical Support Magazine. She can be reached at sharon@b4ci.com

Give Your Information Technology Career That "Extra Edge."

Get Published with NaSPA

The **N**etwork **a**nd **S**ystems **P**rofessionals **A**ssociation (NaSPA) has provided award winning publications like *Technical Support Magazine* to Information Technology (IT) professionals worldwide since 1986. Our publications begin and end with people like YOU. NaSPA has published the work of hundreds of IT professionals for the benefit of thousands of members and IT practitioners. Do you have what it takes to be a NaSPA contributor? We invite you to find out today.

Call for Original Articles and Technical Papers

NaSPA invites you to submit a 1000-1500 word article or research paper for one of our publications. The topic is open as long as it is germane to IT, however mainframe, data center, and other high end operations and systems programming subjects will be given preference.

You must be a NaSPA Member in good standing. *Gold Membership is FREE.* Platinum Members enjoy higher publication priority for only $39.00 yr. All members receive:

- ***Technical Support* Magazine Subscription**
- **Employer Advertising Discounts**
- **Expansive On-Line Technical Library**
- **Job Placement and Hiring Site**
- **Discounts on NASTEC and IDCE Shows**
- **Discounts on Auerbach and Cisco Press Publications**
- **Home and Car Insurance Discounts**
- **More**

Restrictions apply and all articles become property of NaSPA. For more info and author agreement Email president@naspa.com. First time authors welcome. Remember, whether you are already in the IT profession or are still in school, articles look GREAT on a resume! Corporate submissions acceptable if they are not overt sales pitches. **What are you waiting for? Get your name out there today in one of NaSPA's great publications!**

NaSPA®

Doing the Math on IT Complexity: Part II of III

By Roger Sessions and Bill Elder

Making the simple complicated is commonplace;
making the complicated simple, awesomely simple,
that's creativity.
~ Charles Mingus

Welcome to part two of our series on exploring IT complexity. In part one, we explored the prevalence of complexity in the IT field. Most will agree that complexity has become a widespread problem that needs a solution. Gartner recently came out with their Top Ten Strategic Technical Trends Through 2015. Gartner states that one of the Top Ten Trends is IT Complexity. IT Complexity, Gartner says, is a major inhibitor "of an enterprise to get the most out of IT money spent." Pointing to Glass's Law (sourced to Roger Sessions of ObjectWatch), which states that "for every 25 percent increase in functionality of a system, there is a 100 percent increase in the complexity of that system." Gartner predicts that there will be an emphasis on the ability of an enterprise to get the most out of I.T. money spent.

How can we solve the IT complexity problem? In this interview with Roger Sessions, we explore some of the major approaches used to day to address complexity.

NaSPA: Roger, who is responsible for addressing IT complexity? Is it the IT architect? Business architect? Somebody else?

Sessions: Of course, everybody shares some responsibility for driving simplicity. The executives need to recognize the business value of simplicity. The IT architect needs to understand the close relationship between simplicity and architectural qualities such as reliability, testability, adaptability, and security. The implementer needs to take pride in delivering code that is clear and elegant. But IT simplicity ultimately must be driven by those who have a good understanding of both the business and IT. This group is usually described as Enterprise Architects.

NaSPA: What approaches have traditionally been used by Enterprise Architects to simplicity in IT?

Sessions: This first approach was the Zachman Framework^{tm}. In 1987, John Zachman introduced the idea of a framework that focused on ensuring that what IT delivered was what the business wanted. He felt the best way to do this was to ask six basic questions of five major stakeholders. The questions were What, How, When, Who, Where, and Why. The stakeholders were the Executives who defined the business goals, the Business Managers who defined the business concepts, the Architects who defined the system logic, the Engineers who defined the system implementation, and the Technicians, who defined the system delivery.

His idea was that an Architect, say Anne, needed to be able to articulate what, how, when, who, where, and why as would an Executive, say Elizabeth. But Anne's *what* is going to be quite different than Elizabeth's *what*. Nevertheless, Anne's *what* should be related to Elizabeth's *what* in three ways. First, Anne's *what* should be traceable back to Elizabeth's *what*. Second, every aspect of Elizabeth's *what* should be represented in Anne's *what*. Third, Anne should not have anything in her *what* that is not a projection of one of some aspect of Elizabeth's *what*. Think of this as Anne's *what* is Elizabeth's *what*, all of Elizabeth's *what*, and nothing but Elizabeth's *what*.

I often describe Zachman as a *perspective-centric approach* to enterprise architecture, because of its focus on vertically lining up different perspectives.

The second approach was TOGAF^{tm}. TOGAF stands for The Open Group Architectural Framework. TOGAF is most easily recognized by its daisy-like description of the enterprise architecture process in which *architectural vision* drives *business architecture* which drives *information system architecture*, which drives *technology architecture* and so on and so forth (the petals of the daisy), with the whole cycle feeding off of the common well of *requirements* (the center of the daisy).

TOGAF is doing its best to address the lack of a common understanding of what enterprise architecture means and how one does it. The underlying approach is to produce the best possible documentation of what the best minds believe is the best way to deliver the best enterprise architecture. The theory is that if the cognoscenti are able to agree on best process, the riff-raff will meekly follow. So the TOGAF specifications are debated at meetings around the world attended by hundreds of enterprise architects from well-known (and well-funded) companies. The resulting specifications define in excruciating detail the goals that guide enterprise architects, the process used by enterprise architects, and the artifacts delivered by enterprise architects.

I often describe TOGAF as a *process-centric approach* to enterprise architecture, because of its focus on getting the process right.

The third approach is FEA, or the Federal Enterprise Architecture. FEA focused on the issue of language standardization. As the Gershwin brothers put it, if you say po-tay-to and I say po-tah-to, let's call the whole thing off. So FEA standardized the language of describing the enterprise with the goal of making it easier both to find opportunities to reuse existing systems and to collaborate on similar systems. The United States Federal Government spent billions of dollars trying to get FEA right and eventually abandoned it after seeing no value delivered, a sadly familiar refrain.

I often describe FEA as a *standardization-centric approach* to enterprise architecture, because of its focus on developing a common descriptive language for enterprise architecture.

NaSPA: So how successful have these three approaches been with respect to simplifying IT?

Sessions: Not very. There is a strong inverse correlation between the size of an IT project and the chances that it will be successfully delivered. In other words, the bigger they are, the harder they fall. And it seems to make no difference which, if any, of these approaches one adopts.

NaSPA: What is the problem?

Sessions: There are two problems. The first is a lack of any clear understanding about what it means to simplify an IT system. None of these approaches have a model for what drives complexity, a metric for measuring complexity, or a process to validate whether or not simplification has been achieved. As Sun Tzu said more than 2,000 years ago, "Know your enemy." When it comes to IT systems, complexity is the enemy. You can't vanquish an enemy you don't understand.

NaSPA: You said there are two problems. What is the other?

Sessions: The other problem is mathematical. These three approaches are all essentially linear. This means that the complexity of the problem they can solve is linearly related to the amount of effort they put into solving the problem. Two TOGAF architects can generate twice

as many artifacts as can one TOGAF architect and four TOGAF architects can generate twice again as many. Unfortunately complexity is not a linear problem, it is an exponential problem. So a two million dollar IT system is not twice as complex as a one million dollar IT system, it is eight times as complex. And a four million dollar IT system is eight times more complex than that two million dollar IT system and sixty-four times more complex than the one million dollar IT system, and so on. It is a fundamental law of mathematics that linear solutions can only solve exponential problems when the exponential problems are kept small. As soon as they grow very much, the exponential increase in the problem outpaces the linear ability of the solution.

This is why it makes no difference which of these approaches is used if the IT system is under one million dollars. At the small size, any of these solutions work. And it is also why it makes no difference which of these approaches is used if the IT system is over ten million dollars. At that larger size, none of these solutions work. Someplace between one and ten million dollars, the exponential increase in the complexity of the IT system obliterates the linear ability of these approaches to keep up. There is nothing any of these approaches can do about this. They are all fundamentally linear and complexity is fundamentally exponential. They are doomed before they leave the starting gate. Or at least, doomed by the time they get ten million dollars out of the gate.

Next month: Attacking IT Complexity.

Roger Sessions is the CTO of ObjectWatch. He has written seven books including *Simple Architectures for Complex Enterprises* and many articles. He is a past founding member of the Board of Directors of the International Association of Software Architects, Editor-in-Chief of Perspectives of the International Association of Software Architects, and a Microsoft™ recognized MVP in Enterprise Architecture. He has given talks in more than 30 countries, 70 cities and 100 conferences on the topic of Enterprise Architecture.

Bill Elder is a consultant who is employed by Knight Point Systems (www.knightpoint.com), a federal IT contracting firm based in Reston, VA. Bill is a certified software tester and a past member of NaSPA's Board of Directors. He is originally from Pennsylvania where got his Public Policy degree from Penn State University. Bill now lives in the Northern Virginia suburbs of Washington, DC.

A Few Job Postings on NASPA's website

Master Software Engineer (AI)
Capital One
Glen Allen, Virginia, United States

Horizontal Voice Operations Manager (TC)
Capital One
Glen Allen, Virginia, United States

Business Systems Analyst Master (IO)
Capital One
Glen Allen, Virginia, United States

Senior Financial Advisor III 59th Street and 3rd Avenue New York City
Capital One
New York, New York, United States

Horizontal Operations Support Specialist (TC)
Capital One
Plano, Texas, United States

Testing Specialist Master (AI)
Capital One
Richmond, Virginia, United States

Staff Nurse-Patient Aligned Care Team (PACT)
Veterans Affairs, Veterans Health Administration
West Palm Beach, Florida, United States

Senior Financial Advisor III New York NY (Grand Central)
Capital One
New York, New York, United States

Executive Director
Doctors of the World, USA
New York, New York, United States

Mechanical (Simulation & Control) Engineer
Advanced Technology Innovation Corp.
Wrentham, Massachusetts, United States

Principal Associate Supplier Management
Capital One
Richmond, Virginia, United States

Aerospace Engineer
Advanced Technology Innovation Corp.
Massachusetts, United States
IT Development Program The Ohio State University
Capital One
Richmond, Virginia, United States

Lead Software Engineer (AI)
Capital One
Glen Allen, Virginia, United States

Database Administrator (AI)
Capital One
Richmond, Virginia, United States

IT Development Program Georgia Tech
Capital One
Richmond, Virginia, United States

Senior Financial Advisor III Montgomery County MD
Capital One
CHEVY CHASE, Maryland, United States

Senior Calibration Technician l-San Francisco, CA-Analytical Services Team
PCI
San Francisco, California

CLER Field Representative - Remote
Furst Group on behalf of ACGME
Chicago, Illinois, United States

Employment Technician (1755_35052157)
Metropolitan Washington Airports Authority
Washington, Dist. Columbia, United States

Leasing Consultant
IPA Management - Arizona, LLC
Phoenix, Arizona, United States

Web Developer (Information Technology Analyst II)
Placer County
Auburn, California, United States

Deputy Vice President for (1755_35046042)
Metropolitan Washington Airports Authority
Washington, Dist. Columbia, United States

Financial Systems Business Analyst (1755_35046047)
Metropolitan Washington Airports Authority
Washington, Dist. Columbia, United States

Senior Financial Advisor III South Jersey New Jersey
Capital One
NORTH BRUNSWICK, New Jersey, United States

Accounts Receivables/Billing Assistance
Dual Manor
Cincinnati, United States

Dosimetrist (1180_21582)
Wheaton Franciscan Healthcare
Milwaukee, Wisconsin, United States

Master Java Software Engineer (AI)
Capital One
Glen Allen, Virginia, United States

Senior Software Engineer (AI)
Capital One
Glen Allen, Virginia, United States

Java Technical Lead (AI)
Capital One
Glen Allen, Virginia, United States

Employee Development Specialist (1755_35040962)
Metropolitan Washington Airports Authority
Washington, Dist. Columbia, United States

Airport Access Control System (1755_35040957)
Metropolitan Washington Airports Authority
Washington, Dist. Columbia, United States

Senior Regional Planner
San Joaquin Council of Governments
Stockton, California, United States

Rail Project Design Engineer (1755_35038272)
Metropolitan Washington Airports Authority
Washington, Dist. Columbia, United States

Deputy Mgr. Procurement & (1755_35038262)
Metropolitan Washington Airports Authority
Washington, Dist. Columbia, United States

Public Health Division Director
Department of Health
Santa Fe, New Mexico, United States

Power Section Assistant Manager I (Line Superintendent)
City of Tacoma
Tacoma, Washington, United States

Executive Director
Evansville Museum of Arts, History & Science
Evansville, Indiana, United States

Business Systems Analyst Master (IO)
Capital One
Glen Allen, Virginia, United States

Click here for more.

Why College Students Should Also Run a Business

By Matt Stewart, Entrepreneur Specializing in Internships Shares 5 Benefits

These days, it seems as though Americans are spending more for college while getting less value in return – a trend research validates, says entrepreneur Matt Stewart.

"The average cost for an in-state public college is $22,261, and a moderate budget for a private college averaged $43,289 for the 2012–2013 academic year; for elite schools, we're talking about three times the cost of your local state school," says Stewart, a spokesperson for College Works Painting, (www.collegeworks.com), which provides practical and life-changing business experience for college students who have shown potential for success. Interns operate their own house-painting business with hands-on guidance from mentors.

Making matters worse, adults in their 30s have 21 percent less net worth than 30-somethings 30 years ago, according to a new Urban Institute report.

"More students are being saddled with long-term debt while getting less value for their education," Stewart says. "Because of the difficulty recent college grads are having finding jobs in today's tough economy; today's students may have even less worth in their 30s than 30-somethings today."

To add value to their professional career, Stewart encourages students to seek outside-the-box avenues for increasing their career stock while in college. Running a business is a great way to do that; he explains why.

- Employers love ambition. A college degree is the minimum qualification employers are seeking. What hiring managers are looking for is that something extra when reviewing a stack of qualified resumes. At the heart of the economy is innovation; it's the difference between simply existing in a market, and thriving in one. Employers know they need people with creativity and gumption for innovation.

- Real-world management of time and money. College is a time when young adults learn to live autonomously. It's the rare student, however, who learns to manage his or her own affairs and the most precious resources in the business world – time and money. Managing employees, driving sales, developing specific skills for a real market and building strong customer relationships are best learned with hands-on experience.

- Learn where they need help. What do you do well and where do you need help? The best way to know with any certainty is through experience. Running a business while attending college allows students to circle back to their education and focus on their trouble areas by adjusting their curriculum in future semester.

- Develop meaningful bonds. One of the most meaningful aspects of the college experience is the relationships students develop with each other, which often have professional consequences after college. Enlisting the help of fellow students for a common business purpose tends to have a powerful bonding effect.

- Immediate ROI – finding phenomenal success. Most students who run a business during college will not prove to be the next Steve Jobs, Mark Zuckerburg or David Geffen, which is precisely why students should not drop out of college like those pioneers did. However, a student doesn't have to be the next Zuckerburg to experience amazing success as an entrepreneur. College Hunks Moving Junk is just one recent example that began in an entrepreneurial student mind.

Matt Stewart co-founded National Services Group, which operates College Works Painting, SMJJ Investments and Empire Community Construction. Under the executive team's leadership, NSG has grown from a small Southern California business into a national leader in two industries and has been recognized as an entrepreneurial leader by Ernst & Young, the Orange County Business Journal, Inc., Entrepreneur and hundreds of other periodicals. Stewart has received a several awards, including the Excellence in Entrepreneurship Award from the Orange County Business Journal; was named "40 under 40;" and he has twice been a finalist for the Ernst & Young Entrepreneur of The Year Award.

Supplement Facts

Serving Size: All You Can Eat
Servings Per Container: 1

Amount Per Serving	% Daily Value
Energy	100%
Experience	100%
Enthusiasm	100%
Initiative	100%
Technical Savvy	100%
Reliability	100%

* Percent NaSPA-Established Daily Values based on organizations that want to succeed and prosper!

Are YOU Hiring? Find one of the most useful EMPLOYMENT SITES in the industry, proudly sponsored by one of the most trusted names in information technology.

Since 1986, NaSPA (the Network and Systems Professionals Association) has been the premier not-for-profit advocate to Information Technology (I.T.) and Network professionals worldwide. Thousands have coursed through NaSPA training programs, subscribed to its award winning publications, attended its conferences and trade shows, and enjoyed the many benefits of membership. Platinum members, access our expansive SOFTWARE LIBRARY including recent contributions and those hard to find "legacy" applications!

If you are looking for the perfect employment candidate, it's all in one place you can *truly trust.* Explore the many benefits NaSPA offers to its members, for FREE. At the same time re-energize your organization with proven nutrition from our vast membership pool. Don't do anything until you talk to us! Dollar for dollar we are the best value in the industry for finding that next candidate. Visit our EMPLOYMENT SITE and see for yourself, or email Jill Tucker at j.tucker@naspa.com.

NaSPA®
NETWORK AND SYSTEMS PROFESSIONALS ASSOCIATION

www.naspa.com

7044 S. 13th St.
Oak Creek, Wisconsin 53154
(414) 908-4945 x 111

Resuming Business Operations After a Virus Infection

By Ajay Gupta

This article is provided courtesy of NaSPA Supporter Pearson Publishing (Informit). Did you know NaSPA Members get 30% off Pearson / Cisco Press? See More Here!

Even when following cybersecurity best practices, your business very likely will become infected by malware at some point. During the recovery process, someone will have to decide when it's safe to get systems back online. Ajay Gupta, a coauthor of Hack I.T.: Security Through Penetration Testing, describes the issues and steps involved in putting your business back into production after a virus infection.

When dealing with viruses (or any variety of malware), the adage "Prevention is the best medicine" rings true. Still, infections are almost inevitable, and even a minor instance can be debilitating. Organizations that rely on 24/7 availability of their IT resources need a documented incident-response (IR) plan that coordinates their resources to fight infections and restore services with minimal downtime, while simultaneously ensuring data integrity.

An overall incident-response plan requires public relations and internal communications departments to relay information at the appropriate times to employees, business partners, customers, and the public. This article focuses on the benchmarks that let you know when the infecting virus or Trojan is neutralized, and systems can be restored to production safely.

Immediate Response

As some point in the course of operating a network on the Internet, your organization's infrastructure very likely will become infected. As soon as an infection is identified, the incident-response team must swing into action, quarantining affected systems or files, and then remediating any problems caused by the infection. The following sections discuss these processes.

Identification

Your IT department may learn of the infection through an alert from a security monitoring tool, such as a desktop firewall or antivirus software. The product will indicate that it has encountered a file, email message, connection, connection attempt, or other activity that is suspicious and bears closer scrutiny.

Identification of the infection also may come from Help Desk calls complaining of unexpected behavior on desktop or laptop PCs. It usually takes more than one call before people realize what's happening; unfortunately, this lag time gives the infection time to propagate through the network, compromise hosts, steal or corrupt data, and build its footprint.

NOTE

The ability to track and correlate security alerts and Help Desk calls in real time can be priceless, if such measures speed detection of incidents and launching of incident-response activities.

Without an incident-response plan in place, confusion often erupts over what exactly is happening and what must be done when an organization's security measures have been penetrated by a virus. Organizations with an IR plan, on the other hand, can marshal resources and manpower more quickly to fight the infection. An IR plan tells everyone which steps need to be taken and in what order. It's important that such plans document when systems can be reconnected and business operations resumed.

Quarantine

After the infection has been verified, the next step is to quarantine all infected hosts, limiting the ability of the attacker to spread, transmit data outbound, or receive instructions from command-and-control servers managing a potential bot network. Depending on how far and wide the infection has spread, the quarantine may need to include hosts, subnets, or entire domains. It's possible that restricting the flow of the virus may require disconnecting the entire network from the Internet, at least temporarily. The infected organization must avoid two risks:

- The attacker may alter, destroy, or transmit the organization's data off-network.
- The infected network may serve as a jumping-off point for the infection to affect other networks.

Simultaneously, the staff must log all witnessed behavior and symptoms of the infection. Post this info on the walls of the incident command room to ensure that all known information is shared among staff investigating and fighting the infection. Given the speed of virus propagation and the fact that viruses can lie dormant for varying periods of time, the data-gathering process must continue while you're quarantining hosts and disinfecting machines.

NOTE

Quarantine can also involve blocking outbound connections at the firewall and/or gateway router. In fact, one of the initial clues to an infection may be a high number of outbound FTP requests to an unknown IP address. As FTP connections can be restarted if indeed legitimate, blocking such outbound connections can be done even before verifying that they're the result of a compromised system. A virus may well adjust, attempting to establish an FTP connection to yet another IP address—an indication that the source host is infected and should be quarantined. Such unexpected outbound connections provide some information about the virus as well—it's one link in the chain between the infected machine, its command-and-control server, and ultimately the virus/Trojan creator.

With the infection successfully quarantined, it's time to remediate.

Remediation

Remediation is the process of cleaning the infected hosts or mitigating all witnessed behavior and symptoms of the infection. A host is deemed "clean" if any of the following statements are true:

A means of deleting the infecting virus, Trojan, or other malware is known, and reinfection has been prevented (for example, if you're using a virus-removal tool or production virus signature from an antivirus/security vendor).

- The host can be compared to a clean image, and data integrity is maintained.
- The host can be rebuilt from a clean image.

These options may not always be available in the midst of an infection, especially in the case of zero-day attacks or infections from "unpopular" viruses against which signatures are not actively being developed.

Your IT team may want to stay offline until every infected host has been thoroughly cleaned or rebuilt—even if this process takes a week or longer. However, in many organizations such a loss of computing resources may simply be intolerable. On the other hand, businesses certainly shouldn't operate with an active virus on the network. You need a "middle ground" that allows for resuming operations while disinfection activities are underway. The following section describes such a system.

Mitigation and Countermeasures

With mitigation, security countermeasures are in place to block or deny each witnessed action and behavior of the infection—this is where the running list of the infection's activity is taken into consideration. For example, let's assume that the following is a listing of witnessed actions and behaviors of the infection:

- Changes to normal operations:
  - ◊ Windows Explorer breaks
  - ◊ Unexpected reboots
  - ◊ Regular and frequent reboots
  - ◊ Machines shut down upon initial infection
  - ◊ Changes to log settings
- System configuration changes:
  - ◊ Windows Registry settings edited
  - ◊ New user accounts created
- Software installed on host:
  - ◊ Keystroke logger
  - ◊ Spyware
- Files created on infected hosts:
  - ◊ "Password" text file seen on infected hosts
  - ◊ Filenames corresponding to the name of the virus
- Unusual communication attempts:
  - ◊ Attempted FTP connections from infected machines to multiple unrecognized addresses

- ◊ SMB connections to and between IPC$ shares originated by infected hosts to potentially clean hosts (potential means of virus propagation)

Some of this behavior can be observed by IT personnel, gleaned from user reports to the Help Desk, researched online, or reported by AV vendors or industry and government security alerts. Other evidence requires research into the virus itself. If files are being written to infected hosts, for example, it's helpful to track the path in the directory structure where the files are written, as well as the naming convention used for the directories and files, so this information can be used to search other hosts for signs of the same infection.

Once we know what the virus does, we can design, test, deploy, and verify security measures to block these symptoms. For example, the following measures can address the symptoms from the preceding list:

- Configure and run antivirus software with the latest signatures and rules to block the creation, writing, and execution of all suspected bad files.
- Run scripts in loops to delete all virus-related files and kill its processes and services.
- Prevent repopulation of infected files after deletion.
- Restore Windows Registry settings to correct/ default settings.
- Verify normal operations:
  - ◊ Windows Explorer operating normally
  - ◊ No unrecognized rebooting
- Delete unauthorized accounts
- Prevent further outbound FTP connection attempts to known "bad" IP addresses
- Change system and domain administrator passwords

Testing and Adjusting Countermeasures

To ensure that countermeasures are working, network connectivity and services can be restored in a deliberate, phased approach, with testing taking place at each stage to ensure that the infection is held in check. For example, we might allow a server to operate disconnected from the network for a period of time, such as three hours or half of a working day, and monitor its behavior. If we see normal behavior (for instance, no unexpected FTP requests), we can take the further step of restoring internal connections, such as connecting a mitigated LAN or host to the server—again, monitoring operations for evidence of virus activity. All business rules should remain implemented and functioning properly.

Throughout this time, we look for signs telling us that the virus is active, or is being blocked. We also work with users to ensure data integrity.

NOTE

Which services do you bring back first? As a general rule, services should be restored in order of their importance to the organization from a business continuity perspective. While you're testing countermeasures, servers and services hosting the least-sensitive data can be tested first, followed by services and services hosting more sensitive data, and so on.

A business-impact assessment will identify the services that are most critical to the organization, as well as the IT resources that support them, ranking the sensitivity of the data processed by each service.

During these tests, if new or additional hazardous behaviors are witnessed, additional countermeasures must be developed, tested, and implemented before fully restoring services. For example, if infected files reappear in the original directory and/or the Windows\ directory on one or more hosts after they have been deleted, that fact suggests that the virus isn't fully contained and the services are not ready to be restored.

There are many ways in which such re-creation of once-deleted files may happen:

- The virus/Trojan source code remains resident on the host even after deletion of the discovered infected files, such as under alternate filenames or within a zipped file, and are rewritten after deletion.
- The files may be written during system startup, prior to the execution of antivirus software.
- Files may be reintroduced to the system through an infected USB data key.
- The virus may be able to write files to the server while acting as an account with greater privileges than those of the antivirus application (or the agent deleting the files).

These situations can be addressed in part by adjusting and adding the following countermeasures:

- Continuous deletion of all infected files through an automated script.
- Implementing antivirus rules that block execution of all infection-related executables.

- Restoring the Windows Registry settings to their correct/default values and checking the settings to ensure that they don't revert to their prior settings.
- Temporarily disabling USB ports on hosts.
    ◊ Changing the password for all system, domain, admin, and privileged user accounts. This practice relies on the virus being unable to recapture these passwords. As long as virus execution is blocked, the virus shouldn't be able to recapture the passwords.

If no new or additional behavior is witnessed, testing of the countermeasures can be expanded to additional hosts and services. If the countermeasures continue to hold against the infection, management can make the tough decision to bring all systems back online.

Virus Removal

Restoring services doesn't complete the incident-response effort. The task of removing the virus remains, and it must be completed by one of the three processes identified in the "Remediation" section. From a strict security perspective, it's preferable to restore services only when you're fully confident that the infection is cleared out. However, security is often only one of the considerations that CIOs must juggle—productivity and profit concerns play important roles as well.

This compromise—reconnecting services and resuming operations once the known behavior of the infection is neutralized, but before the virus is truly cleaned out—carries risk. Organizations must be willing to accept this risk to get back online prior to fully cleaning the network.

One additional note: The decision to bring services back online—or even how you fight infections—may not be yours alone. Organizations that have connections with business partners over public or private networks may need to make these decisions in concert with their partners. At the very least, security countermeasures used to mitigate an infection must be shared with all partners prior to reconnecting networks and services, and those partners should be prepared to implement similar measures.

On the Internet, we really are all in this together.

Ajay holds an M.B.A. from Georgetown University's McDonough School of Business; and both an M.S. and B.S. (cum Laude) in Electrical Engineering from the University of Maryland, College Park. He is a member of Tau Beta Pi (the national engineering honor society), Beta Gamma Sigma (the international honor society in business management), and Phi Kappa Phi (the national honor society).

Seven Tips for Hiring “A Players”

By Richard Bryan

Your business doesn’t run itself. The quality of your organization depends on the quality of your team—a motivated, energized staff is the key to companywide success. You want *A Players*, those colleagues who contribute disproportionately to the advancement and profitability of the organization.

In the same way that the Pareto Principle states that 80% of results come from 20% of your employees (based on research by the Italian economist Vilfredo Pareto in the early 1900s), your *A Players* have a measurable impact on your bottom line.

The Pareto Principle is often used in a sales environment, but it applies equally to a variety of different industries. If you can build a team of *A Players* around you, then your job as a business leader or owner becomes much easier, as you do not have to deal with endless crises and can work more intentionally on developing the future strategy for your organization.

So how do you find *A Players* for your team?

The funny thing about *A Players* is that you can find them in the strangest of places. A few years ago, James was running a car dealership that was lacking in quality salespeople. He received a call from his wife while she was out shopping for strollers, and asked him to meet her at the store.

“I want you to meet Louise. She has a great attitude and I think you’ll like her.”

Ten minutes later he was walking into the shop to meet Louise. She was a class act and spent the next half an hour asking them lots of qualifying questions about their lifestyle. Once she had all the information she needed from them, she launched into a brilliant sales demonstration of various products. She was impressive.

They ended up spending over $1,000 in the shop that day and were absolutely thrilled with their interactions with Louise. James was particularly impressed by her enthusiasm, her energy and her ability to listen intently to their needs, and then repeating this information back when closing the sale. Too many sales people believe that selling is about talking, but in reality it is actually about the ability to listen to your customers so that you can truly understand their needs.

A few days later James went back to her store and offered her a job. He was not sure that selling cars had been on her career plan, but to her credit she took a risk and joined the team the following month.

Initially, Louise struggled a bit because she had no product knowledge, no customer base and was the only female on a sales team of 30 people. However, after continual support from James and the upper-level staff and a combination of hard work and positive attitude she began to flourish. By the end of the year she was the top sales person at the dealership.

When you are seeking *A Players* for your organization, don’t just look for skills and experience but start by looking for someone with a great attitude.

Here are seven tips to help you find your own *A Players*:

1) One page plan - Have a simple one page plan that you can share with future employees. This plan highlights what you have achieved as an organization during the past year and also what your Vision is for the next 3 to 5 years. “A Players” are motivated as much by being part of an organization that has clear goals and aspirations as they are by salary and benefits. They want to be part of an organization that has a purpose.

2) Think outside the box - Don’t just look in the same old places for new employees. Think about looking outside of your industry for people with the right attitude and a track record of success. You can always train skills and product knowledge.

3) Telephone screening interview - Consider having a 15 to 20 minute telephone interview with potential candidates. This can save both parties a lot of time and expense before a more formal interview is arranged.

4) Personality profiles - Use DISC or another similar personality profiling tool to make sure that you have a good fit for the role you are seeking to fill. Different fields require their own unique brand of skills, such as high-influencing personalities or levels of compliance.

5) Watch the body language - Always have another person interview with you and if possible get them to ask the questions, so that you can concentrate on listening to the answers given and also observe the body language to make sure that it is congruent with what is being said.

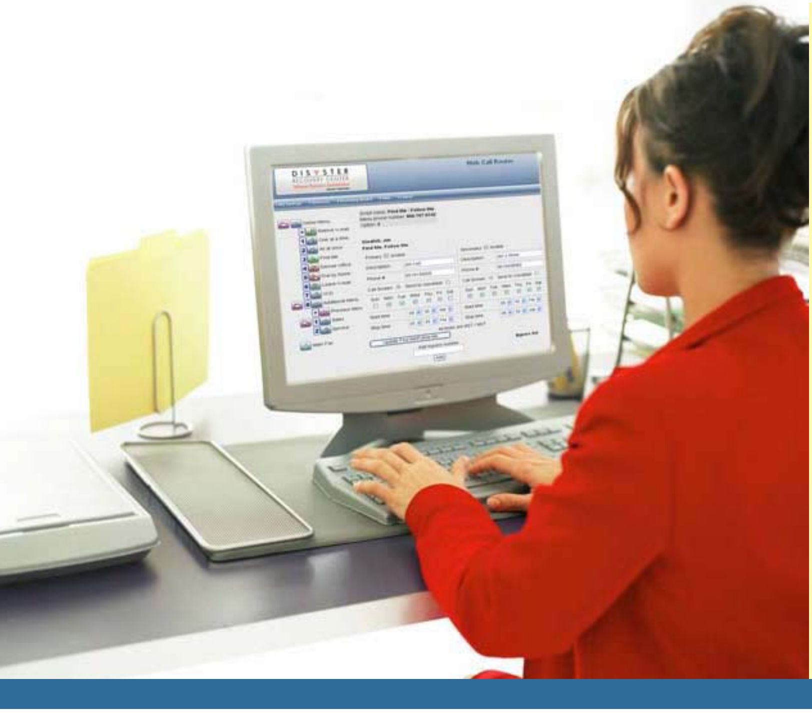
6) References - Always insist on speaking to a former boss for a reference. Sometimes it is not what is said about the candidate but the way in which it is said over the phone that can alert you to potential problems but also provide clues to the positive aspects of the candidate. Written references are usually very brief and not very helpful.

7) Staff referral program - Have a program in place that rewards existing members of staff if they recommend someone for a position you are trying to fill. For example, you could offer a cash bonus to your employees if their recommended candidate is taken on, and another bonus if the candidate is still with you and performing well 6 months later. This has the added benefit of ensuring that the new member of staff has a mentor looking out for them during their initial 6 months!

Try some of these tips and see what works best for you. If you can surround yourself with a team of *A Players* who have great attitudes, are motivated by achievement and are strong in areas where you are weak, then your role as a leader or business owner becomes far easier. You can concentrate on setting the future strategy for your organization while your team achieves amazing results.

Richard J. Bryan is an international speaker, executive coach and author of the forthcoming book, *Being Frank: Real Life Lessons to Grow Your Business and Yourself*. Through his experiences as the 4th Generation CEO in a family-owned business, Richard gained a wealth of knowledge and developed into a true leader. By applying his creative strategies, Richard helps businesses hire the right people, forge dynamic teams and increase their profits. For more information, please visit www.richardjbryan.com.

Introducing the World's Fastest, Most Flexible, and Easy to Use Disaster Recovery System



- Rapidly Recover From Natural Disasters, Network Outages and Other Complex System Failures
- Stay in CONTROL - No Matter WHAT HAPPENS
- No Equipment to Buy, No Capital Expenses
- Available Now From Your Local Phone Company, or CALL US Directly for Immediate Set-Up

"Houston, we have a problem."

- Astronaut Jim Lovell, Apollo 13, April 13, 1970

Does this phrase sound familiar? It should, and not just because you saw the movie. Any disaster begins almost exactly the same way. You don't know what happened. You don't know how bad it is. You don't know what has been affected. You don't know what to tell the media. What you DO know is that until you have some hard information, you are recovering blind. How would YOU communicate with your responders after a disaster?

We have all seen the movies where the General picks up the "Red Phone" and is in instant control of a situation. Today, commercial organizations and government demand "military-grade" command and control. They find it with us.

Welcome to FailSafe Communications

FailSafe offers a telephone company-grade service for recovery of critical communications. Our Command and Control services allow for almost instant *situation analysis* by executives and responders. This allows your recovery plan to change quickly, and allows executives to make informed decisions based on each unique event. Just as important, FailSafe recovers inbound calls transparently, without changing phone numbers. Remember, when customers stop calling in, the cash register stops. Either way, the key to successful recovery is COMMUNICATIONS. With FailSafe you cover all the bases and are *always in control.*

In a hurry? Download our Complete Brochure HERE.

In 1986 our principals made disaster recovery history when we were the first in America to locate a disaster recovery center inside a telephone office. Today we offer a phone company-grade disaster recovery service "in the cloud." We serve police, fire departments, 911 centers, universities, banks, credit unions and others in conjunction with their local phone company. If your service provider is a member of our network, our service can be conveniently charged on your your phone bill. If not, no problem. We can sign you up directly and activate you in days.

Hear it yourself. Dial 1 (866) 501-8430 now for recorded information from our actual system. Better yet, why not sign up for our free online demo held EVERY WEDNESDAY. Discover how to keep your business running, and yourself in control, when it matters most.

ARE YOU A SERVICE PROVIDER?

Now Hiring Sales Agents and Channel Marketers including Independent Telephone Companies, CLECs, VARs, Network Integrators and VoIP providers. Learn More HERE.

Fast, Reliable, Affordable , and Available Now In Your Area

FailSafe
Communications Inc.
"For Your Information.. We've Got Connections!" TM

(866) 501-8430
Info@failsafecommunications.com