T A A R
THE AUTOMATED AGENCY REPORT

www.taareport.com

May 2006
Volume 22 • Number 5

Inside TAAR

Steve Anderson — Editor

Five Critical Topics You Must Discuss With Your IT People Today

By Mike Foster

Insurance agency owners and company executives have a common communication problem with their Information Technology (IT) staffs. The results of this miscommunication can threaten business, clients, and employees.

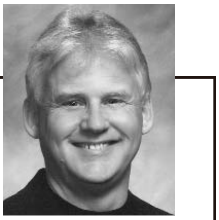
The problem begins when this question is posed to the IT staff: "Are our technology systems secure?" What the IT people hear is, "Do you want to keep your job?" As a result, they respond, "Yes!" So no matter what the *real* answer is, IT people generally assure executives that everything is fine. The simple truth is that most corporate networks are far from being sufficiently protected. It may be that the IT department is either unaware of the vulnerabilities or is planning to fix them "first thing in the morning."

You've probably heard some IT horror stories. You may even know of businesses that lost hundreds of thousands of dollars due to hacking or that were forced to shut their doors when their systems were destroyed. You already know that

continued on page 3

Even though most people are aware of the dangers, few companies are sufficiently protected from the numerous and growing threats to their technology.

Editorial



Alert Your Customers

As consumers demand more, the definition of what constitutes “good service” is ever-changing. It’s happening everywhere I go. Even grocery and drug stores now commonly have extended hours or are open 24 hours a day.

My youngest daughter, Stephanie (21 years old, junior in college), recently called home excited about a new service our bank now provides to account holders. It’s called Alerts, and she found out about it when she logged onto the bank’s Web site to look up information about her account. She can now monitor and manage accounts with free online banking alerts. By simply providing her e-mail address, she can now stay on top of her accounts through alerts sent by the bank. Alerts allow her to receive timely notifications about the activity in her accounts, including balance and transaction alerts. And, she can customize exactly what type of alerts she wants to receive based on her particular needs.

With this free banking service, Stephanie decides when and how to receive important information about her accounts. For example, she can avoid overdraft fees by choosing an alert that notifies her when the account balance drops below the threshold she set, or she can be alerted when a direct deposit has been posted to the account. In addition to e-mail, she can also receive alerts on her mobile phone as text messages.

Stephanie is excited about this service because she’s had a difficult time keeping track of the money in her checking account. I would argue that money management is a skill she still needs to learn. But the bank has taken away her “pain point” by providing a service that is customized to her needs. Even I admit that I have been known to overdraft occasionally — and would have welcomed an e-mail or text message alert when my account balance dropped below a specific limit.

How can the insurance industry take advantage of the alert concept? Most agents get questions continually about direct bill status. Insurance companies could establish a process to send alerts to an e-mail address or cell phone when a direct bill payment has been posted to the account. Or, how about sending a reminder message when a payment is overdue or when a policy is going to be canceled because of nonpayment?

The insurance industry has spent years and much time and money trying to streamline communication between insurance companies and their agents. But where is the client in this process? There is no question that we need to continue to work on improving communication efficiency between agents and their business partners. In the process, we can’t afford to forget our clients’ needs and desires. The reality is that the Stephanies of the world are not just coming; they are already here. What are you going to do to provide the kind of service they will want to call home about? ◆

THE AUTOMATED AGENCY REPORT

TAAR

MAY 2006
VOLUME 22 • NUMBER 5

Steve Anderson, EDITOR

Bruce Tippery, PUBLISHER

Andrea Serrette, ASSOCIATE EDITOR

CONTRIBUTING WRITERS

Patricia Alexander
NETTLES CONSULTING NETWORK, INC.
Jack Burke
SOUND MARKETING, INC.
Mike Foster
THE FOSTER INSTITUTE
A.J. Zaleski
UTICA MUTUAL INSURANCE GROUP

Jenny Kabakovich,
BUSINESS MANAGER & HIGH-TECC COORDINATOR
Char Campbell, PRODUCTION
Sissi Haner, COPY EDITOR
Afni Insurance Services, WEBMASTER

TAAR, The Automated Agency Report, (USPS 765-570, ISSN 0888-8205) is published monthly by The Automated Agency Report, Inc., 9711 Independence Way, Westminster, CO 80021. Periodicals Postage Paid at Broomfield, CO, and at additional mailing offices. Annual subscription rate is $199. POSTMASTER:
Send address changes to *TAAR,*
The Automated Agency Report,
POB 6218, Broomfield, CO 80021-6218.

KEEP IN TOUCH
Your comments, opinions, and input are encouraged. Letters and articles may be faxed or e-mailed to the editor at…

TEL: **303.404.0457**
FAX: **720.294.9797**
E-MAIL: **steve@taareport.com**
jenny@taareport.com
WEB: **www.taareport.com**

Five Critical Topics You Must Discuss With Your IT People Today, *continued from page 1*

viruses can shut networks down and disrupt business to the point of devastation. Hackers can get into your system, steal information, tarnish your organization's integrity with clients, and ruin your business.

Misery loves company

Even though most people are aware of the dangers, few companies are sufficiently protected from the numerous and growing threats to their technology. And the majority of threatened companies don't have a small breach in their security. They have a huge, gaping hole, and are waiting for disaster to strike.

According to the CSI/FBI 2005 computer crime and security survey, 43% of companies don't even report when they get hacked because they don't want the negative publicity, and 33% don't tell law enforcement because competitors might use the information to their advantage.

Negative publicity and competitive repercussions certainly exist, but your biggest concern is not how you'll deal with the results of such attacks; once you've fallen victim, there's very little you can do except notify the authorities and hope you and your team can salvage the business. It is much better to *prevent* the disaster *before* it happens.

Prevention starts with how you handle your IT staff. Many businesses make the mistake of handing over the keys to their company's security to IT people — who are sometimes outside vendors — without controlling and monitoring their work.

IT people are only human

Most IT employees believe that executives and owners need to see them in action, so they generally concentrate on fixing visible problems first. Though they mean well, IT people can become inundated with work generated by co-workers who need help deciphering computer error messages, fixing the local printer, finding a deleted file, or solving other problems. Meanwhile, the tape back-up system may not be functioning, but most of the time, that sort of "invisible" problem is not one that executives and employees notice for a day or two… unless disaster — in the form of a virus or hacker — strikes.

Most of the work done to beef up network security is not visible, which is why IT employees fear bosses won't notice what they're doing and will think they're slacking off. Technology people, like most of us, generally tend to have a high need for the approval of others. They may work hard all day to increase network security, but nobody

For more on security, including the chance to get a discount on a four-CD interview with Mike Foster, see this month's Connections column on page 7.

Since **anti-spyware** is only as effective as it is current, it is **crucial** to get **updates** daily.

notices; whereas if they solve the boss's problems with his Visio, they'll gain instant recognition and approval.

If every organization could secure their networks and remain secure, hackers could be put out of business. But the majority of corporate America remains blissfully ignorant of their security weaknesses and does not employ strategies to fortify their systems. This is compounded by the simple fact that most managers do not have the expertise necessary to manage the IT department. They don't know what questions to ask, what topics to discuss, or what exposures are potential threats to the business. They aren't trained in IT!

What are some of the primary threats to your business's computer network? How can you motivate your IT department to help secure your system so the business and everyone in it thrives? It's like the "build a better mousetrap" game. Because hackers constantly make "better mice," the good guys need to diligently install better mousetraps. Although the dangers may seem overwhelming, knowledge really is power. Knowing what you need to discuss with your IT people is an essential first step toward security. Following are five key questions you need to ask your IT staff — right now.

Question #1:
Are we regularly installing updates to our desktop operating system?

In August 2005, computers at CNN, the *New York Times*, and ABC crashed when a worm infected them. By 5:00 p.m., the virus had taken a significant number of the computers down. Microsoft later reported that they had released an update for Windows 2000 operating systems four months earlier that would have prevented this. The patch on Microsoft's Web site said, "If you are using Windows 2000, you absolutely must have this tool installed; otherwise someone could crash your Windows 2000 system." But these massive news organizations apparently did not install that patch.

Microsoft will give your IT department Windows Server Update Services, a free tool to deploy updates to all the workstations in any way the IT expert sees fit. You can control how these patches get pushed out, whether your company has 30 employees or 30,000.

If you are concerned about your own workstation, you can personally check if your computer has the most current updates applied by going to Microsoft's Web site and using the Microsoft Update tool.

Microsoft reports three kinds of updates that may or may not be available for your computer system: high priority updates, software optional updates, and hardware optional updates. Make sure high priority updates get on your workstations immediately. These updates improve security by fixing areas that Microsoft knows a hacker could use to get into a system. Even if you find your system is current with high priority updates, check your system monthly in order to make sure your system is protected by the latest Microsoft patches. Everything needs to remain updated — operating systems, applications, and firmware.

Optional software updates are entirely up to you. They include things such as the Euro-conversion tool or the latest Windows Media Player. If you use these tools, you may want to get the update. Be aware, however, that optional hardware updates tend to crash systems. To avoid this, check with your IT department before installing any optional updates.

In regard to pop-ups, if you see one that claims to be from Microsoft announcing available updates, do not click on the pop-up because it may not be from Microsoft. Instead, go to *www.microsoft.com* and choose

"Microsoft Update" to see if updates are actually available. If they are, download them. If they're not, be very glad you didn't click on the pop-up, as that could have been spyware. Once your IT team begins using centralized patch management software, your systems will be updated automatically.

Question #2: What sort of anti-spyware protection do we have, and what else do we need?

Spyware is malicious software that can get into your computer and tell others everything you're doing within your computer, including the keystrokes you're making. If you have spyware on your system, and you go to your bank's Web site and enter your user name and password, all of those keystrokes that log you in at your bank have been logged and sent out to hackers.

To keep spyware out, first make sure your IT staff uses an effective centralized anti-spyware tool and diligently downloads anti-spyware updates. Since anti-spyware is only as effective as it is current, it is crucial to get updates daily.

Second, they must verify a successful scan of each of the systems at least weekly (preferably daily). Many IT departments never set up anti-virus or anti-spyware to scan systems every night, or even once a week, believing that the current anti-spyware will catch the program when the file initially comes in. In reality, there is a lag time between when a malicious program is designed and when the protection software gets updated to recognize the program as being malicious. So, the anti-spyware program may not realize that it's encountering a spyware program when the file first comes in, and the malicious program can get on your drive.

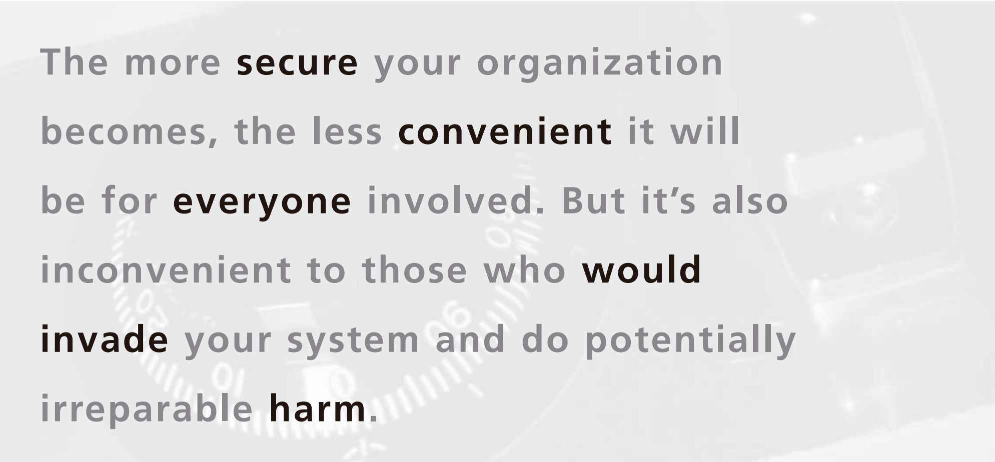
A lot of spyware is so tricky that the first thing it does is disable your anti-spyware. So, if you let the spyware in and it resides on your system, your anti-spyware still reports that "Everything's fine; there's no spyware here," when, in fact, all kinds of spyware live and breathe on your system.

Third, ensure that your IT people immunize your system, which involves using different programs that make it harder for spyware to stick when it tries to come in.

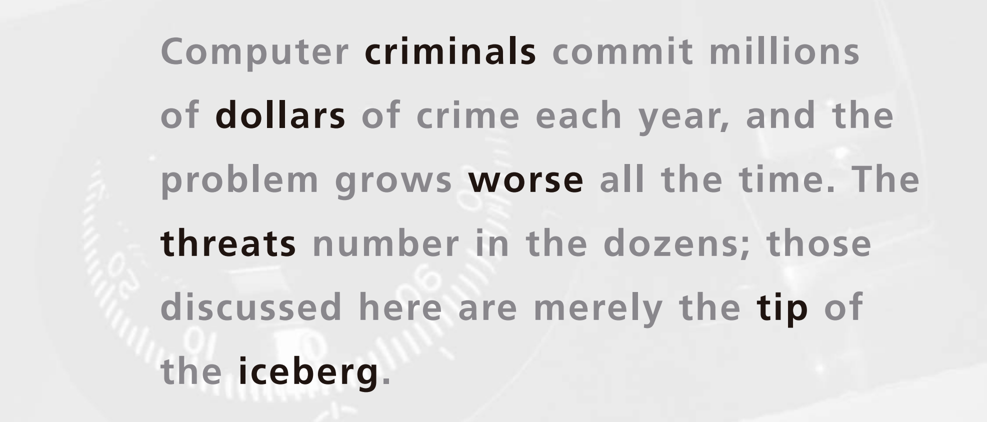
Question #3: Do we have an effective firewall strategy?

Many IT departments install anti-virus programs. The good news is that most anti-virus programs are exceptionally effective when they are configured properly. The bad news is that IT departments often don't include a personal firewall on each computer. A firewall is a program that runs on the system to keep hackers out. Every single computer needs a firewall — not just the network perimeter. If only your network perimeter is firewalled, it's like living in a gated community but not locking your front door. That's not a good practice for your residence or your network.

Your network perimeter firewall may do a great job of protecting you from attacks from the Internet, but you could very easily have an employee unintentionally bring in a virus on a CD, USB memory stick, or laptop they've had outside the company. When they carry this media into the building and connect to a perimeter-only secure network, they may inadvertently load a virus, which then has complete reign in the internal network without restrictions. Individual



The more **secure** your organization becomes, the less **convenient** it will be for **everyone** involved. But it's also inconvenient to those who **would invade** your system and do potentially irreparable **harm**.



Computer **criminals** commit millions of **dollars** of crime each year, and the problem grows **worse** all the time. The **threats** number in the dozens; those discussed here are merely the **tip** of the **iceberg**.

firewalls on each workstation can keep that virus from spreading further. We've paid so much attention to the viruses coming in from the Internet that many of us have forgotten that we can pick up nasty viruses carried into the building by an unsuspecting employee.

Plus, with mobile technology, count the number of employees who utilize laptops at home and on the road and then return to the office and dock that laptop into your network system. In some cases, their children may have been using that laptop the night before. Always err on the side of prudence.

Question #4: What's our password policy and procedure?

Too many businesses maintain a "sticky note" policy: as you walk through the office, sticky notes cover desktops and computer screen edges with password information. Or, there's a sheet with passwords written on it stored in an individual's desk drawer. Worse yet, someone within the company has compiled a list of everyone's passwords so he/she can get into each workstation in cases of absence. These systems are totally vulnerable to any client, prospect, vendor, sales person, repair person, or cleaning crew who enters the establishment. It's like leaving the spare key to your house on top of the mat, rather than underneath it — and neither is a good idea.

How frequently do you require passwords to be changed (everyone's passwords for every account)? Have your IT people recommended password programs to automate the process? Today's insurance agency deals with numerous programs from numerous companies. As a result, agencies can feel overwhelmed when it comes to password control and security. However, the alternatives would be far more overwhelming. Security is not the easiest path, but it is the essential path.

Other potential password problems relate to former employees. How many people have left your employment with knowledge of their passwords and possibly the passwords belonging to co-workers? What is your password policy upon employment termination? A disgruntled former employee can quickly do serious damage to your business with access to your system, or even a nasty e-mail to your client and prospect e-mail directory.

As with the prior questions, unless you discuss this with your IT staff, they may not put passwords on the top of their priority list.

Question #5: How's our physical security?

If hackers — employees or someone pretending to be a contractor — are able to gain physical access to your servers, they can get everything they need to wreck total havoc in 10 minutes or less. They can copy password information onto a USB thumbdrive, carry it home, and use that data to discover every password on your system. Your servers must be in a secure room, locked up tight as a drum. Access must be restricted to people with an absolute need to enter; it's a great idea to have an entrance tracking system that monitors who entered and when.

This may seem like overkill to many agency owners because they trust their staff and don't see a danger in giving everyone access to the server room. That type of open door policy is like leaving the office door unlocked when you leave at night. Access can be gained by anyone, and there really are times when no one is watching the door. Since

continued on page 9

by Jack Burke

The Elephant in Our Living Room

Many families have an elephant in their living room that everyone refuses to acknowledge. For some, it might be a family member's addiction or mental illness; for others, it could be financial distress or other dysfunction. The simple fact is that these "elephants" are easier to deny than address.

In the insurance industry, the proverbial elephant is IT Security. Whatever you choose to call it — Information Technology Security, Internet Security, Data Security, Electronic Security, Digital Security — the problem is that our data is not secure, particularly at the agency level.

Granted, I normally write about relationships and marketing. But IT security goes to the very foundation of both relationships and the insurance industry. Both are based on trust. Without trust, our insurance industry becomes an extinct dinosaur. Without trust, any relationship is doomed to failure.

We trust our companies to keep our data secure in their electronic vaults. Our companies trust us to keep their data secure — and our E&O carriers expect no less. Our clients trust that our systems are secure enough to safeguard their valued information. Our employees trust that we are also protecting their data within our systems. And finally, our corporate structure trusts that our systems will protect our own corporate data.

The reality is that such trust is misplaced. The information contained in the average agency's system is not secure. Our clients, companies, and employees — even the very existence of our agencies — are at risk. Although most agencies will initially deny that they have left the door to the vault open, they have. It was not a conscious act; it has simply been a sin or omission and denial.

Agency owners trust that their IT people have secured the enterprise. Yet most agency owners do not know enough about security to manage, or even question, the actions of their IT staff or outside vendor. Most IT people are aware of the existing vulnerability, but they have been given a misguided vision of their jobs. They believe that the greatest urgency is often reconnecting someone's printer to a computer, or helping someone who forgot their password. Maintaining security is not necessarily their highest priority.

Time for a reality check

Still doubt me? Have you walked around the office lately? Ever notice any sticky notes with passwords stuck to the computer or desktop? Getting a lot of spam? Have any of your computers (or your system) been disrupted with a virus? Can former employees still access your system with knowledge of their former passwords (or the passwords of their former peers)? What sort of protection do

...the problem is that our data is not secure, particularly at the agency level.

you have against spyware — not anti-virus, but spyware? How does your IT person handle updates? Are you current on every update and patch — or aren't you sure? How frequently do you change passwords? Is there a master password list that people know about? How many people have access to the room where your servers are located? What does your policy and procedures manual say about IT security?

Those are just a few security questions that come to mind. A recent interview with the security expert who authored *TAAR*'s lead article this month raised many more. In fact, my meeting with Mike Foster definitely heightened my awareness on this topic. For instance, the September issue of *Consumer Reports* indicated that:

- 1 out of 2 computer users are experiencing heavy spam loads.
- 1 in 4 experienced major and costly virus problems.
- 1 in 6 experienced major and costly spyware problems.
- 1 in 200 has lost money from an account due to hacking.

Foster also told me about security breaches he had found at major banks and financial institutions, as well as major corporations. In one case, a CEO's new computer became infected because he allowed his son to use it while he was visiting at the office. The problem is pervasive, yet the insurance industry seems to be addressing only a minor segment, if that. Plus, the insurance industry's continued evolution toward mobile technology is creating even greater risks: laptops that are brought home for work in the evening; remote access to the system by producers and account executives; system access that is given to valued clients. The list goes on and on.

I'm not suggesting that agency owners and managers need to become experts on IT security. I *am* suggesting that they need to learn enough to effectively manage IT activities, or at least know what questions to ask their IT people. As managers, we need to know how to hold others accountable — and that requires some self-education.

The interview I mentioned earlier with Mike Foster was one of the most memorable interviews I have ever had the pleasure to conduct. He had a unique ability to put a lot of technical information into a language that I could understand. What was originally supposed to be a 30-minute conversation turned into a three-and-a-half hour marathon. Because I believe the content is so vital to the insurance industry, I approached Foster about turning this into an audio resource for insurance executives, and he agreed.

The resulting four-CD album is entitled *Securing Your Enterprise: 12 Steps to IT Security for the Insurance Industry*. The CDs are jam-packed with critical information that every executive, manager, and agency owner should hear. It is the initial step in educating yourself on the problem and the solution. From there, I would also recommend attending the HIGH-TECC conference every year and possibly schedule someone to actually perform a security audit on your operations.

Arrangements have been made to offer this album to *TAAR* subscribers at a special discount. Rather than paying the normal $199, *TAAR* subscribers can purchase the album from Sound Marketing for $149 — a $50 savings. It will probably save you thousands of dollars in potential loss and will also provide tools to increase productivity in your

Ordering Information

To order ***Securing Your Enterprise: 12 Steps to IT Security for the Insurance Industry***, please go to:
www.soundmarketing.com/securitytaar.htm

The Elephant in Our Living Room, *continued from page 8*

IT department. In fact, there are so many benefits to be found in the words and expertise of Mike Foster that I will guarantee your satisfaction with the information — or your money back. That, by the way, is a first! Our company has always guaranteed production quality, but we have never before guaranteed content quality on any project.

For additional information, or to place an order, simply go to: *www.sound marketing.com/securitytaar.htm*. ◆

Jack Burke is the president of Sound Marketing, Inc., editor of *ProgramBusinessNews*, publisher of Audio Insurance Outlook, and author of *Creating Customer Connections, Relationship Aspect Marketing*, and his newest book — *Get What You Want*. He can be contacted at *jack@soundmarketing.com* or 800.451.8273

Five Critical Topics You Must Discuss With Your IT People Today, *continued from page 6*

insurance is a business of managing risks and exposures, why should you treat your business any differently than you treat your clients? The companies that insure *your* business expect more of you, and you could find yourself in a difficult position explaining why you "left the door open."

Security lies outside the comfort zone

Ours is a convenience culture, but when it comes to computer security, convenience and security are often mutually exclusive. The more secure your organization becomes, the less convenient it will be for everyone involved. But it's also inconvenient to those who would invade your system and do potentially irreparable harm. A little inconvenience for your IT people and the rest of your employees is a very small price to pay to keep the business secure and running smoothly.

Computer criminals commit millions of dollars of crime each year, and the problem grows worse all the time. The threats number in the dozens; those discussed here are merely the tip of the iceberg. But if you educate yourself about the dangers and communicate openly with your IT staff, beginning with an honest discussion of these five questions, you can work together to keep your organization safe, secure, and successful.

There are many more areas of security that need to be managed. Every business could benefit from a technology security audit, but there just aren't enough experts to go around, and many firms might not be able to afford a good audit. In partnership with *TAAR* "Connections" columnist Jack Burke, we have produced a four-CD audio album to help insurance agencies, companies, wholesalers, and brokers begin to get a handle on the management of their IT Security. The audio is recorded in "plain English," so executives can understand the 12 steps they need to take in order to effectively support the IT team in making the network more secure.

For more information on *Securing Your Enterprise: 12 Steps to IT Security for the Insurance Industry* and a special price for *TAAR* subscribers, visit *www.soundmarketing.com/securitytaar.htm*. ◆

Mike Foster is a consultant who serves as a skilled interpreter between management and IT departments, providing important and insightful results for both. As president and founder of The Foster Institute, he provides solutions to high-tech issues to make businesses safer, more efficient, and more successful. For more than 25 years, Foster has helped to demystify computers, networking, and data protection, guiding even beginners to become e-savvy and more confident. He makes IT easy to understand and apply with solid information and good humor. He can be reached at *mike@fosterinstitute.com*, 800.657.7107 and *www.fosterinstitute.com*

How•To by Steve Anderson

Creating Dynamic Documents — Part 2

Editor's Note: *Agency staff spends more time creating form letters and proposals than almost any other task. In this series of articles, TAAR explores advanced options available in Word that can help reduce the time and the number of keystrokes needed to complete these tasks.*

Word tables

If you have been using tables for any length of time, you've probably noticed the similarities between a Word table[1] and an Excel spreadsheet. Tables provide an excellent way to organize information in a document, and they should be used extensively. One of the more powerful features of Word tables is that, like Excel spreadsheets, you can set them up to perform calculations on numbers contained in a table cell.

Simple Word formulas

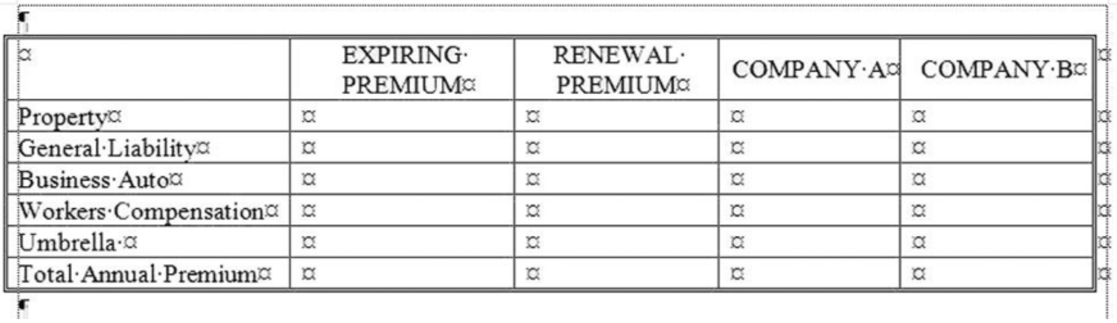
If you've used Excel, you're already familiar with formulas, which allow you to perform calculations based on information in your spreadsheet. A Word table provides you with similar capability, but nowhere near the extent provided by Excel. In Excel, for example, you can create complex formulas that reference information from multiple spreadsheets and manipulate output to appear how you want it. Word can't do this — and that's because it is fundamentally a word processor. That said, Word does provide some capability to perform calculations based on information in a table.

Suppose, for example, you have a renewal premium comparison table (see Figure A) that is a part of your renewal proposal. You can format this table in the template to automatically total the premium fields.

As you would expect, the bottom line in the table holds the total annual premium for each column. Why dig out the calculator, punch in the numbers, and type totals into the cells when Word can do the work for you? To make Word do the work, position your cursor in the Total Annual Premium cell for the Expiring Premium column of the table and choose Table, Formula. You will get a window similar to the one shown in Figure B.

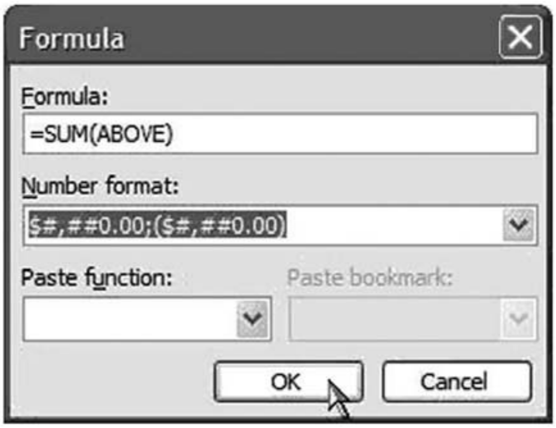
When you open the window, the Formula box will read =SUM(ABOVE) as long as you positioned your cursor in the bottom row of the table. If you placed your cursor in one of the cells in the right-hand total column, the

[1] To learn more about table basics, including how to create tables, format them, and add and remove columns and rows, use the Help function in Word.



¤	EXPIRING· PREMIUM¤	RENEWAL· PREMIUM¤	COMPANY·A¤	COMPANY·B¤
Property¤	¤	¤	¤	¤
General·Liability¤	¤	¤	¤	¤
Business·Auto¤	¤	¤	¤	¤
Workers·Compensation¤	¤	¤	¤	¤
Umbrella·¤	¤	¤	¤	¤
Total·Annual·Premium¤	¤	¤	¤	¤

Figure A: Sample renewal premium comparison table.



Formula: =SUM(ABOVE)

Number format: $#,##0.00;($#,##0.00)

Figure B: The formula window is simple but has quite a bit of functionality.

Formula box will instead read =SUM(LEFT). Word is smart enough to look at your data to figure out which formulas make the most sense. Text in a table cell may confuse Word, so if you have text, enter the formula by selecting the function you want to use in the Paste box. If you do not have data in your table, you may have to enter everything manually.

Immediately below the Formula box is a Number format box. As you might expect, the options in this box allow you to indicate how you want to format the result. In the example shown in Figure B, the output would format with a leading dollar sign. However, you don't actually have to indicate anything in the Number format box. Word also helps you with this. If, for example, one of the numbers in your table column already has a dollar sign on it, Word will assume that the formula result should also be a monetary figure and will tack the dollar sign onto the result for you.

Other functions are also available using Word's Formula window (see Figure C).

The Count function counts the number of cells, while the Max function locates the largest value. When using the Average or Count functions, be aware of this caveat. Suppose you want to use the Average or Count function and your table has a heading. In older versions of Word, the formula includes the heading cell, and treats it as a zero. Therefore, the Average calculated value has one additional count and isn't accurate. Word 2003 is a little smarter, but not much. Word 2003 looks at the data and tries to determine where your heading row is located so it can exclude it from the results. But this only works if you're using different kinds of information. If your data is text instead of numbers, Word can't make any kind of determination and gives you an incorrect result.

More complex Word formulas

The solution to the above problem is to use more complex Word formulas. For example, if you want to perform a granular calculation, such as multiplying two of the numbers in your table, or including just specific cells in a calculation, you can do this by referencing specific table cells in a formula.

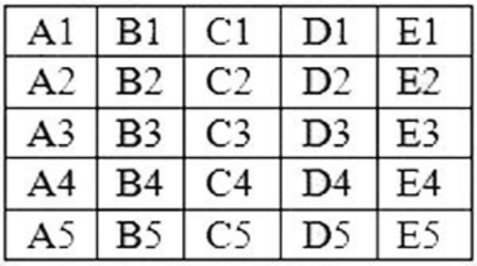
If you have worked with Excel, you understand how it names cells. The column letter and the row number are concatenated to form a cell reference such as A4 or B6. Excel even provides you with a nice grid to help you keep track of where you are. Word uses the same cell naming scheme (see Figure D on page 12), but does not provide you with the nice grid, so you have to do a little counting and reciting of the alphabet.

Using these cell references (instead of a word like ABOVE and LEFT) allows you to avoid the problems discussed above and allows you to perform direct calculations on values in your table.

This table shows both the formula and the result. The shaded cells indicate which cells

SUM(ABOVE)
AVERAGE(ABOVE)
COUNT(ABOVE)
MAX(ABOVE)

Figure C: Sample Word formulas.



A1	B1	C1	D1	E1
A2	B2	C2	D2	E2
A3	B3	C3	D3	E3
A4	B4	C4	D4	E4
A5	B5	C5	D5	E5

Figure D: Columns are designated by letters and rows by numbers.

are involved in the formula for a particular column.

In Figure E, you can see a number of different ways to create a formula, using cell references to identify the exact cell you want to work with. You also can see some direct calculations, such as C2*C3 (the * character is used to denote multiplication) and D2-D3. You can reference cells anywhere within a table, but not to another table in the document.

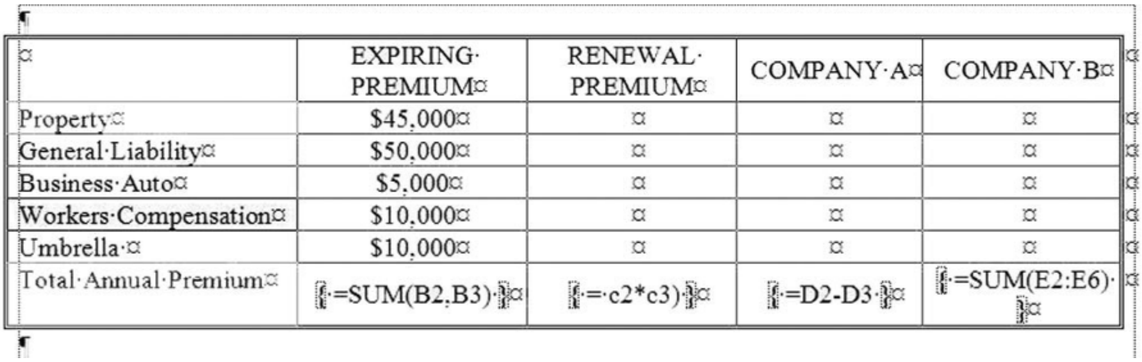
Figure E also shows two different ways to address cell ranges in a formula. In column B (Expiring Premium), you can see the formula =SUM(B2,B3), which, when read literally, reads "Add up cells B2 and B3." Now look at column E (Company B). This formula reads =SUM(E2:E6). When read literally, this formula says, "Add up cells E2 through E6, inclusive." The only difference is a comma versus a colon. A comma allows you to provide a list of individual cells you want added together, whereas a colon allows you to specify a range of cells.

Note also that the second total column showing the formulas has curly braces. Those cells actually contain the formula. You can see the formula because I set the Toggle Field Codes option on. When you select a cell containing a formula and a result and turn the Toggle Field Codes on, Word shows you the formula instead of the result. This can be really handy. To do this yourself, select a cell with a formula, right-click it, and, from the resulting shortcut menu, choose Toggle Field Codes. Or, you can use ALT-F9.

Recalculating formulas

If you make a change to your table's data Word does not automatically recalculate the result. This is one big difference between Word and Excel. Excel recalculates your entire spreadsheet every time you make a change. Word does not. You need to tell Word to redo its calculations. To recalculate your formulas, select your entire table and press the F9 key on the keyboard. To make sure your calculations are always up to date, it's a good idea to select the entire document just before printing and press the F9 key.

Word tables can be very useful when used as mini-spreadsheets, but they will never replace the power and flexibility of Excel, which is designed to crunch numbers. For many, Word tables are more than sufficient. If you need more, but also need the power of Word's document-creation capabilities, a future article in this series will detail how you can combine the best of both products into a single document. ◆



¤	EXPIRING·PREMIUM¤	RENEWAL·PREMIUM¤	COMPANY·A¤	COMPANY·B¤
Property¤	$45,000¤	¤	¤	¤
General·Liability¤	$50,000¤	¤	¤	¤
Business·Auto¤	$5,000¤	¤	¤	¤
Workers·Compensation¤	$10,000¤	¤	¤	¤
Umbrella·¤	$10,000¤	¤	¤	¤
Total·Annual·Premium¤	{·=SUM(B2,B3)·}¤	{·=·c2*c3)·}¤	{·=D2-D3·}¤	{·=SUM(E2:E6)·}¤

Figure E: Word provides several ways to create formulas.

by Patricia Alexander

Planning for Change in Your Agency

Insurance agents and brokers have waited decades for the types of agency management systems that are available today. As a warrior who has managed insurance technology in agencies for the past 30 years, I have seen these systems improve dramatically. However, today's systems are so loaded with technology that they can be overwhelming.

Before moving forward with new technology, it's important to ask these questions: How does this new technology affect the processes and workflows currently established in our office? What happens to an already backlogged workload when systems change or we implement a new system?

The importance of planning

Most agencies don't ask these questions. In other words, they don't plan for change. The result? Chaos, which often causes failed technology implementation.

Agencies spend a great deal of time planning in many areas. They plan their marketing strategy, their budget, their five-year plan for growth, etc. However, there is often no real plan for upgrading or implementing new systems. Agency principals may have some ideas in their heads or a few notes they jotted down during industry meetings. There might have even been a few discussions with agency managers and staff about impending changes. But no plans were ever made or put into place.

While the agency management system is your biggest technology investment, there are many other systems that are equally important and require the same level of planning. Consider, for example, the importance of the following systems to the operation of your agency: telephone, copiers/printers, network or desktop faxes, e-mail, imaging, Web pages and even paper files. A change in the equipment or software that runs any of these items can cause ripples throughout the agency.

Every agency (no matter its size) should have written workflows that document how everything is handled in the agency. This includes, but is not limited to: issuance of certificates of insurance, ordering, receiving and processing endorsements, renewal timeline, checking policies, and marketing new and renewal business. When something changes in your agency management system (or any of the other systems), you must look at how that will impact your current workflows. Of course, the challenge is learning how to implement the changes that come at you constantly and still keep workflows intact. In order to succeed, you must have a plan — and you must use it 100% of the time.

In the past, I have advocated that you should never change your workflows to match the system. However, some of today's systems do cause workflows to change, and mostly for the better. Also, adding phone systems that record files that can be attached to the agency management system (and other such technological changes) can cause a change in workflows as well. New interfaces that allow you to send information from your agency management system to multiple carriers should change your workflows.

Another thing to keep in mind when it

comes to workflows is that what may seem like a simple "patch" for your agency management system can cause a great deal of interruption if you don't understand the change and test it before implementation. Often, a patch that fixes a new or existing problem or a new function can cause something else not to work. You must determine how patches will impact how the system is used once it is installed. The new twist in this plan is that some systems operate in the Internet Application Service Provider (ASP) environment. When a patch or hot-fix is loaded, it's instant to all users. The agency must review and test the release from the vendor immediately upon receipt so that it knows the impact as soon as possible.

Planning for change

If you are going to make a change to your agency management system, consider setting up a test copy of your system, if possible. This will allow you to load any changes to the test system first. Then the change can be reviewed, along with the documentation from the vendor, before implementing on the live system.

- ***Patches*** — These occur frequently and often have little effect on your established workflows. However, they can cause something major to go wrong elsewhere in the system. Before loading patches, download and read documentation from the vendor. Check with other agencies using your system to see if anyone has installed the patch and ask about their experience. You should test your workflows in the test system to determine if the process still works as planned or if changes need to be made. Once you have determined that everything is functioning correctly, the patch can be loaded to the live system.
- ***Functionality changes*** — Many vendors are addressing the requests of their user groups by continuing to improve the agency management system. These changes include integration with e-mail and faxing software or a change to the functionality in the current process, better navigation, access to the system via the Internet, etc. These changes are usually great enhancements to the system and your workflow. However, the only way these changes can benefit your agency is through planning, training, and proper implementation. Many times, people tell me that the new functionalities don't work. At the same time, other employees in the same agency say the new changes are great. The negative comments are usually from individuals who experienced a failure of the new functionality once, did not attend the training, or needed more training and did not speak up. Other times, the agency doesn't even provide formal training. As a result, only the "techies" understand the new functionality, while everyone else flounders.
- ***Database or software changes*** — As technology moves forward, software vendors make shifts to better behind-the-scene products. Sometimes the change is unnoticeable to the majority of the agency's users. In other instances, the entire look and use of the software changes. When this happens, your agency can experience a significant setback if proper planning, training, and implementation are not completed prior to the software upgrade. These types of system changes often require a total review of your workflow and substantial changes.

It is very important that all system changes be implemented on a test system or tested immediately on implementation in an ASP as soon as the update is

continued on page 16

by A.J. Zaleski

Insurance Deregulation

Insurance is now a rapidly changing global business — particularly when it comes to commercial insurance. However, regulation of commercial insurance markets in the U.S. has not kept pace with the changing nature of the insurance industry or the needs of buyers. Regulation works best when it remedies significant market failures and *truly* protects insurance buyers. Many states have lost sight of this principle with respect to commercial insurance, and in some cases, have been too slow at the state legislative level in rewriting laws that were put into place 50, 60, or even 100 years ago.

Concerns about the variance between regulation and markets prompted state insurance commissioners and the industry to develop a framework of recommended reforms for commercial insurance regulation. A principal component of this initiative was to deregulate insurance transactions of large businesses with operations in multiple states. The change was also supposed to enable a flexible and progressive approach to easing the regulation of all commercial insurance prices and products. The concept was to decrease the intensity of regulation as the size and sophistication of the buyer increased. The National Association of Insurance Commissioners (NAIC) showed its support of this platform with its adoption of a guiding brief in 1998, which was a major change in regulatory philosophy that would substantially increase market efficiency. The hope was that states would enact and implement the recommended reforms. As expected, some states made adjustments, but others did not.

Effects on the Errors and Omissions market

ISO and other similar entities have provided a consistent form and policy structure for many insurance lines and products over the years so agents don't have to review and understand scores of policy forms from multiple carriers. Even so, agents are still required to have an intimate understanding of coverages, terms, and policy forms. With deregulation evolving, it is inherent that agents review all products and policies prior to selling them. It is incumbent upon regulatory bodies to maintain a quality educational standard in their respective CE programs to reinforce this. Additionally, insurers (and states they do business in) should apply the social criteria of simplicity to the policy creation process. If insurers are going to create their own forms as a result of deregulation, they should be held to the standard of ensuring that they are relatively simple to interpret and that they afford proper coverage.

Conclusion

The easing of regulatory restrictions should extend as far as possible in terms of all markets, buyers, insurers, and intermediaries. No segment should be regulated more heavily than is absolutely necessary and appropriate to protect buyers in that market. Unfortunately, at the state and federal levels, decision makers do not have the necessary expertise to understand the true need for reform. Prior approval requirements for rates and policy forms should be rescinded and competitive regulatory systems instituted for

continued on page 16

Planning for Change in Your Agency, *continued from page 14*

implemented. The current agency workflows will need to be reviewed step-by-step and revised to work properly with the new functionality. Training sessions need to be established to test the revised workflows and new system functionality. Each session needs to be specific to each group of users. Producers will need different training than CSRs. Each session needs to address how staff uses the system and how it changes agency workflows. A good practice for ASP users is to review the data prior to live date. Share the data with the staff via e-mail. In the e-mail, include specific information on any new functionality that they should not be using until further notice from management.

Call to action

Change is constant. Your agency should assign personnel who continually oversee systems, interactions with carriers, and new technologies.

Determine what management personnel will review and test changes. Who is going to define and write revised workflows? Who will be in charge of presenting the training sessions? Questions always arise during training sessions, so someone who can give management input or make a decision should always be in attendance so training can move forward.

Remember — properly defined workflows are roadmaps for staff to get through their daily work. Always consider how changes to current systems and new systems will work for you. Change your workflows to fit the new system as it makes sense. Above all, plan, plan… and plan. ◆

Patricia Alexander, CIC, is a consultant, coach and mentor. Her many years of experience in retail agency and MGA settings gives her a broad range of knowledge in agency operations. She is dedicated to educating her clients on using technology to enhance and build their businesses and profitability. She can be reached at 817.605.1663 or *pma@pmaassociates.com*

Insurance Deregulation, *continued from page 15*

all commercial insurance lines, regardless of the type of product and the size of the buyer. If individual consumers fare well under such systems for auto and home insurance, certainly businesses can do the same for the types of insurance they purchase. Currently, 20 states still require prior approval of commercial lines rates, and the vast majority requires prior approval of commercial policy forms. Requiring the filing of policy forms for standard products purchased by small businesses and compulsory coverages (e.g., workers' compensation) is a matter for regulatory judgment. Regulators can judge whether they can use alternative means to ensure that forms comply with state laws. For other products, effective monitoring of the policy forms used by insurers should be sufficient to prompt regulatory action when necessary. While commercial lines deregulation represents a positive and modern development, its implementation to date falls far short of what is needed to promote market efficiency and benefit to the insurance provider or consumer. ◆

A.J. Zaleski is National Underwriting Manager, Insurance Agents Errors & Omissions, at Utica Mutual Insurance Group. He can be reached at 866-860-1914 x6970 or *tony.zaleski@uticanational.com*

Vendor Contacts

AMS Services, Inc.
800.444.4813 • Windsor, CT
www.ams-services.com

Applied Systems, Inc.
800.999.5368 • University Park, IL
www.appliedsystems.com

Ebix, Inc.
800.433.5744 • Atlanta, GA
www.ebix.com

DORIS Insurance Systems
800.282.3394 • Alpharetta, GA
www.dorissystems.com

InStar Corporation
800.736.1425 • Kennewick, WA
www.instarcorp.com

irs-aims
800.876.1466 • Universal City, TX
www.irsaims.com

Keal Technology
800.268.5325 • Concord, ON
www.keal.com

MI-Assistant
800.755.2329 • Eleva, WI
www.mi-assistant.com

Strategic Insurance Software, Inc.
800.747.7005 • Gahanna, OH
www.sisware.com

Terrace Consulting, Inc.
(888) 269-6200 • Oakland, CA
www.terrace.com

VRC Insurance Systems, Inc.
818.707.4295 • Westlake Village, CA
www.vrcis.com

XDimensional Technologies, Inc.
800.789.2567 • Brea, CA
www.xdti.com

Association Contacts

Independent Insurance Agents & Brokers of America (IIABA)
800.221.7917 • Alexandria, VA
www.independentagent.com

Professional Insurance Agents (PIA)
800.742.6900 • Alexandria, VA
www.pianet.com

ACORD
800.444.3341 • Pearl River, NY
www.acord.org

IVANS, Inc.
800.288.4826 • Greenwich, CT
www.ivans.com

CSIO – The Centre for Study of Insurance Operations
416.360.1773 • Toronto, ON
www.csio.com

User Group Contacts

AMS Users' Group (AMS)
Susanne Buyck, Executive Director
TEL 972.929.8803 • FAX 972.915.2863
www.amsug.org

Applied Systems Client Network (Applied Systems)
Linn Wheeling, CEO
TEL 407.869.0404 • FAX 407.869.0418
www.ascnet.org

Ebix Users Association (EUA) (Ebix, Inc.)
TEL 805.557.1111 • FAX 805.557.1133
www.eua.org

ANeU (Affiliated Network of Ebix Users)
Kitty Ambers, Executive Director
TEL 804.674.4899 • FAX 804.276.1300
www.ebixusergroup.com

DORIS User Group (DORIS)
Linda D. Bisceglie, President
TEL 585.591.1590 • FAX 585.591.1637
www.dorissystems.com

National InStar Users Group (InStar)
Stephanie Hulcher, Executive Director
William Mitchell, President
TEL 253.549.0004
www.instarusers.org

MI Management System Resource Group (MI-Assistant)
Bill Sterry, Resource Group Director
TEL 715.287.4262
www.mi-assistant.com

National Association of S.I.S. Partner Agents, Inc. (NASPA)
Ron Binning, President
TEL 262.473.3930 • FAX 262.473.3289
www.partneragents.com

AIMS Users Group, Inc. (irs-aims)
Mark Willingham, President
TEL 915.365.2516 • FAX 915.365.3667
www.irsaims.com

Nexsure User Group (NUG)
Karen Bitzer, President
TEL 972.744.2720
kibitzer@rhshins.com

VIP-VRC's Insurance Partners (VRC)
Bob Pachner, President
TEL 212.338.2526 • FAX 212.682.3299
www.vrcis.com

Terrace Users Group (TUG)
Stephen Sentz, President
TEL 410.339.5245 • FAX 410.583.5459
www.terrace.com

The TAAR Network...

consists of insurance and business professionals with a wide range of talent and expertise. The following individuals are available for consulting, training, and speaking:

Steve Anderson
steve@taareport.com
- technology audits
- rent-a-CIO
- imaging technology

Nettles Consulting Network
lnettles@nettlesconsulting.com
- workflow consulting
- automation implementation
- managing change

Mark Parrish
mparrish@ajasent.com
- automation selection
- LANs and peripherals
- internal systems, operations

Michael J. Weinberg
mweinberg@gatewayins.com
- marketing and sales
- agency management
- incentive-based compensation

Tim Woods
twoods@afniinc.com
- custom Internet development
- application software development
- Internet business consulting

For more information about the TAAR Network or referral to specific members, contact...

The Automated Agency Report, Inc.
PO Box 6218
Broomfield, CO 80021-6218
TEL 303.404.0457
FAX 720.294.9797
jenny@taareport.com

HIGH-TECC 2006
Maximizing Success

TAAR's Steve Anderson invites you to attend HIGH-TECC 2006 to focus on

Maximizing Success...

at one of the industry's most unique events for agency and company insurance professionals.

HIGH-TECC 2006 — July 16-19 — Vail, Colorado

How will you grow your agency? What must you research today so you are ready to implement next year? What does your agency need to look like in the future so you are a survivor? What technology is available that will help you achieve your goals? How are you going to satisfy changing prospect and client expectations? How will you keep up?

Using technology as a strategic advantage is more important today than at any time in the past. HIGH-TECC 2006 will help you understand the latest technology trends and how you can make them work for you as you move your organization forward. You will learn practical ideas that will help you take full advantage of the technology you already have as well as learn what is coming so you can plan accordingly.

HIGH-TECC is not just for the IT staff or "techies;" it is also designed for owners and managers who want to acquire a better understanding of what technology is available to help them solve their most pressing business problems.

HIGH-TECC brings together a wide cross-section of people in the industry — agency owners and managers, producers, company reps, vendors, technology specialists, industry consultants, and user group and association leaders. In fact, that's one reason why so many people keep coming back. Each session is specifically designed to promote active interaction with everyone participating and exchanging ideas face-to-face.

Nowhere else in the insurance industry will you find the unique experience that HIGH-TECC offers — a focused, relaxed atmosphere that facilitates face-to-face interaction with agents, company executives, and other industry leaders to provide real world solutions to today's industry challenges.

At HIGH-TECC we work hard to address the specific issues and concerns of all participants. Our goal is to help agencies gather the information they need to make wise strategic technology plans. We also help you make the best use of appropriate technology, enabling you to become more effective in providing your customers with quality service experiences.

"I have gone to several vendor conferences, but they are all obviously biased. This was a setting where I was able to hear honest opinions from other agencies, vendors, and companies. It was great to talk with people who have the same issues as we do and discuss possible solutions for the future."
Shane Davis, Sky Insurance,
Maumee, OH

Early Registration Savings

FOUR EASY WAYS TO REGISTER ➢

Phone
303.404.0457

Mail
PO Box 6218
Broomfield, CO 80021-6218

FAX
720.294.9797

Online
www.taareport.com

Name ________________________ TEL ________________________

Company ________________________ FAX ________________________

Address ________________________ E-Mail ________________________

City/State/ZIP ____

Will you be bringing your spouse/significant other and/or family members?
(Additional meal and activity tickets will be available at registration) ________________________

Registration Fee: includes conference-sponsored meals (Sunday reception & Tuesday dinner, all breakfasts and lunches), breaks, and materials.

□ **Before May 26** 1st Registration **$649** Add'l Registration **$595**
□ **After May 26** 1st Registration **$749** Add'l Registration **$695**

Note: Registration fees do not include hotel accommodations. Hotel space is limited. HIGH-TECC registrations may be canceled until midnight, June 30, 2006. A $100 service fee will be assessed. After July 1, 2006 there are no registration fee refunds.

Send to:

The Automated Agency Report, Inc.
PO Box 6218 • Broomfield, CO 80021-6218
TEL **303.404.0457** • FAX **720.294.9797** • **www.taareport.com**

Remember, you can register online using our secure Web site by going to ***www.taareport.com***

Payment Method: □ Check/MO □ Bill me □ Credit Card

□ MasterCard □ VISA □ AMERICAN EXPRESS Expiration Date ____________

|_|_|_|_| |_|_|_|_| |_|_|_|_| |_|_|_|_|
Card Number

____
Print Cardholder Name

____
Signature

TAAR506

by Steve Anderson

Wait Staffs Go High-Tech

If the wait staff at restaurants appear just as wired as U.S. Secret Service agents, it's because technology is becoming a bigger part of restaurants. For example, point-of-sale (POS) handhelds — minicomputers that transmit restaurant orders directly to the kitchen — eliminate dashing about from table to kitchen. These minicomputers can also take credit card payments right at the table, eliminating fears of identity theft, since the credit card is never out of sight. Future POS handhelds will be more efficient and will include handwriting and voice-recognition devices. High-tech advances are also available to the restaurant customer. More and more people are turning to the Internet to make dinner reservations, while eWinebook helps diners navigate a restaurant's wines and includes recommended food pairings.

E&S Submissions Streamlined

AMS Rackley recently launched SUBMITWrite, a tool for the MGA marketplace that streamlines the submission process for applications and quote data from retail agents to the MGA. It enables retail agencies to electronically submit quote information and supporting ACORD applications via the MGA's own branded Web site. The submitted information is available to the underwriter for import directly into Rackley's POLICYRater system. SUBMITWrite also has the functionality to ask supplemental questions as a part of the submission process. General Liability and Commercial Auto are currently available, with Commercial Property to be released this year.

Communicate Pay and Benefit Packages

AMS Benefits has released two new features to its suite of applications that will allow brokers to help employers attract and retain workers. Benefits Benchmarking is a tool that allows employers to compare their benefit packages to those offered by other employers. Total Compensation Statements gives employers a way to communicate the total value of the pay and benefits programs to workers. Both enhancements are available to existing and new AMS Benefits customers immediately.

Benefits Benchmarking provides access to critical, timely, and relevant benefits information, including average employee size, average amount spent on healthcare, or the total amount spent on employee benefits. With this application, brokers can benchmark against their own customer base or against a larger pool to determine how their clients compare to national averages.

The Total Compensation Statements solution delivers personalized, up-to-date information to employees either online or as a printed statement. With one click, employees see a comprehensive snapshot of their cash compensation, including base salary, commissions, bonuses and overtime, as well as their employees' benefits, including health care and retirement benefits, paid-time off, vacation time, and tax savings programs. Additionally, employers have the ability to include information on estimated tax savings from various programs such as 401(k) plans and flexible spending accounts, as well as real-time balances on retirement and investment plans. The Total Compensation Statements tool can be added to any of BenefitsCenter's three portals — one for brokers, employers, or employees.

Federal Data Protection in the Works

A new bill is making its way through Congress that would establish national standards on data security. The bipartisan bill, the Financial Data Protection Act, would require that state regulators enforce uniform federal standards, as related to the insurance marketplace. It was introduced last October by Rep. Steven LaTourette (R-Ohio). It would help to safeguard sensitive consumer information, combat identity theft, and establish a national standard to notify customers of improper access to personal data. This is an important issue that is not likely to disappear. Currently, there are 23 states with some type of security breach notification laws on the books.

Tech Tips

by Steve Anderson

An Outlook on Categories

"Categories" is a feature of Outlook that you've probably seen but never used. Any Outlook item (a message, contact, appointment, note, or task) can be assigned to one or more categories. Once you've classified items by categories, you can group or search them with ease.

For example, you can use tasks to manage what you need to do during the day. First, assign each task to a category that describes where you need to be to finish the task. Place phone calls in a "Phone Calls" category; put tasks that require an Internet connection in an "At computer/Online" category. Then, sort your tasks based on where you are at any given time.

To create a new category, click on the Edit menu and choose Categories. You'll see a long list of predefined items. Simply delete the ones you don't want. To make new categories, type in the name at the top and select "Add to List." Your category will now appear with a checkbox in the list. Next, you can attach items to that category. Every Outlook item has a category field at the bottom of the date entry screen. Just type the category name or click on the button and select the appropriate checkbox on the list displayed. (It's wise to use the list in order to ensure you don't misspell the category name.)

Using the Rules Wizard, you can automatically assign incoming e-mail to a category. You do this by creating a rule that looks for e-mails coming from a sender you specify (e.g. a person, company, underwriter, etc.) and then puts those e-mails into the category you select. The same applies to outgoing messages; the Rules Wizard can assign a category to certain messages in your Sent Items folder.

Give Categories a try. They can help organize your life — and your e-mail. ◆

THE Automated Agency REPORT, inc.
PO Box 6218
Broomfield, CO 80021