CPCU SOCIETY INSURING YOUR SUCCESS

Cutting Edge

IT

Volume 10 Number 2 November 2003

Sys Out

by Patricia L. Saporito, CPCU

Patricia L. Saporito, CPCU, chairman of the IT Section, is a senior property-casualty insurance consultant for NCR Corporation where her responsibilities include business development, business strategy consulting, and strategic alliances in the property and casualty area.

Insurance is an industry run on data—in pricing, underwriting, claims, marketing, and finance. This issue's focus on data mining and analytic applications like fraud detection reinforce this. These are topics I work with clients on daily, in the decision support or analytic systems realm. They are part of a symbiotic relationship with operational systems like agency management, claims, and policy administration. The analytics provide the ammunition to develop and implement strategies to improve operational efficiencies and reduce operational expenses. They are increasingly becoming embedded in our operational underwriting, claims, and customer service systems for real-time decisioning. And they are changing the way we look at our customers, distribution, and service partners as we harness more data and develop more sophisticated ways of measuring their value to us.

I encourage both technical and business users alike to take the opportunity to learn more about data warehousing, business intelligence, and decision-support systems by visiting some of the following web sites:

www.datawarehousing.com

www.dmreview.com

www.dw-institute.com/
(The Data Warehousing Institute)

www.intelligententerprise.com ■

What's in this Issue?

Data Mining: A Call to Action

by Patricia L. Saporito, CPCU

Business intelligence solutions must deal with presenting the ever-increasing quantity of detailed data, and businesses must try to analyze and take action on this data. The result is that many business intelligence tools are becoming compromised in their effectiveness, primarily based on the size, complexity, and volume of data sets. This is a key issue that data mining is suited to address.

Data mining is a key part of the decision support environment. It thrives on detailed data, identifying relationships in the significant amounts of data available. Data mining should be integrated into the business process so that information can flow throughout the organization. With this flow of information, the insurance professional has more timely access to the data. Often, business users see emerging patterns while doing daily business analysis using business intelligence tools. The next step is data mining.

Because data warehousing and data mining play an important part in the business intelligence process, warehouse planners and data architects should be active participants in the mining effort and not passive onlookers. Raw data, alone, does not allow for timeliness in decision-making or for maximum return on investment from corporate information assets.

To maximize the effective use of such corporate assets, the data-mining effort should take place in the warehouse or warehouse environment so that mining results such as scores are fed back into the warehouse for further use and analysis by other users. Metadata, or data about the data, allows users to understand the source of the data, business rules, and calculations used.

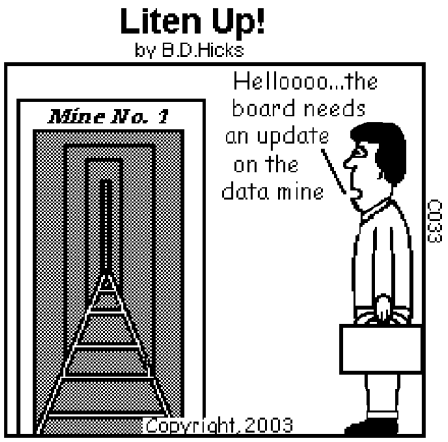
Mining is extremely critical in business intelligence but, unfortunately, some warehouse teams are unwilling or unable to support mining. And some business users are unwilling to relinquish control of departmental data mining. Warehousing teams should avoid being viewed as a passive repository that only serves up data to be mined by other teams or third-party vendors. Frequently such efforts result in additional data marts with costs and data issues. Data warehousing teams should focus on data quality, meta data, and business intelligence tools—allowing business users maximum flexibility in the tools but maintaining the data integrity.

Data-mining teams must perform extensive data transformation and cleansing to prepare their data, despite what's available within the data warehouse. Data mining requires special transformation of the data and may have unique data quality or quantity issues. In view of this challenge, many warehouse environments only serve up raw mining data. In order to make the process work most effectively, however, we need to look at data mining as an integral part of business intelligence in order to ensure that warehouse practitioners support the technology to address the most complex business requirements.

Warehouse environments should support several aspects of data mining. One of these aspects is data acquisition. Data warehouses are well suited to provide data acquisition, an effort that can account for about 40 percent of the overall mining effort. Another aspect is data cleansing and transformation. This task is very well suited for warehouse personnel and resources, and it accounts for about 10 percent of the overall mining effort. Data loading is another part of the data mining process. This requires the loading of mining model data. The data warehouse provides a good environment for this process, because of the flexibility from which to propagate data within the warehouse structures.

Production implementation of mining models is another aspect of data mining that provides flexibility. This allows data-mining designers to control precisely where and when the model is executed to best support the business issue being addressed. The last aspect of data mining that should be supported by warehouse environments is deployment of results. If the warehouse administrators control the implementation of mining models using SQL, then it becomes natural to structure the SQL around the model so that net results of the run feed directly into warehouse tables.

Many traditional warehouse teams do not have mining experts. That does not mean that they are not critical to an effective mining process. The warehouse team provides the necessary data so that the experts can spend the time mining the data. When approaching a data-mining project, all aspects of the data-mining process, including data acquisition and preparation, should be a part of the data-warehousing process. This will help to cut down on delays in the use of the mining results and will help assure that appropriate business decisions are being made based on all of the information that is available. ■



From the Editors

by Robert L. Siems, J.D., CPCU, (Mary Moore-Campagna, CPCU, CPIW, Lamont D. Boyd, CPCU, in absentia)

- **Robert L. Siems, J.D., CPCU,** is in private practice with the Law Offices of Robert L. Siems, P.A. He is founder and president of GF Practices, Inc., a consulting company specializing in litigation and risk management to the property and casualty industry as well as other businesses experiencing litigation exposures.
- **Mary Moore-Campagna, CPCU, CPIW,** is a senior consultant with (MC)2 Insurance Training & Consulting in Soda Springs, CA. Moore-Campagna is a member of the CPCU Society's Information Technology Section Committee and the Golden Gate Chapter.
- **Lamont D. Boyd, CPCU,** is director of business development, global financial services, for Fair, Isaac & Company. In this capacity, he is responsible for the identification of client and partnership opportunities that make use of Fair, Isaac's predictive technology and e-commerce products and services for the insurance industry. He previously managed insurance regulatory affairs on behalf of Fair, Isaac and its more than 300 insurance industry clients.

This second newsletter of 2003 focuses on three topics. A group effort has produced an informative article on data warehousing. We have then moved away from the technical side of our business to present a short summary of the Terrorism Risk Insurance Act of 2002. Cyberterrorism is a substantial concern to the property and casualty industry, which we will also address in future issues. An appreciation of this new federal legislation is an important foundation. Our final article looks at cybercrime and spam, respectively.

The article in your last issue on information technology to identify fraud is followed in this issue with a summary of the introduction by the Insurance Services Office (ISO) of ClaimDirector℠, a fraud-fighting resource Additionally, there is a summary of the recently released report from the Insurance Research Council on insurance fraud.

We hope many of you attended the Annual Meeting and Seminars in New Orleans, October 11-14, 2003. The opportunity for seeing old friends and meeting new ones is enjoyable and educational. The seminars sponsored by our section at the Annual Meeting in New Orleans were "Enterprise Risk Management," on Tuesday, October 14 at 10:30 a.m., and "Leveraging Third-Party Data," on Tuesday, October 14 at 1:30 p.m.

Congratulations to Larry E. Fagersten, CPCU, CLU. Larry is a 2003–2004 national governor of our CPCU Society. His nomination is well earned. He is a consummate professional with more than 30 years in our business. Presently a manager, p&c billing for the Indiana Farm Bureau, Larry has served the Central Indiana Chapter in various capacities including president. He has been a CPCU since 1984 and has an emphatic endorsement from your IT Section Committee. I can imagine no one more deserving. In keeping with the aphorism that if you want something done, ask a busy person to do it, Larry also has a distinguished record of service with the National Guard. He is presently a director of the National Guard Association of Indiana. One warning: Larry follows a soldier's physical fitness regimen so do not believe him when he asks you if you want to go on a little run. I have still not forgotten our jog in Seattle.

Thanks go to Lynn M. Davenport, CPCU, from all us! If you have not visited our Section's web site recently, please do so. She has constructed a model for the Society. The hard work of Lynn, the other members of the committee and the leadership of Pat L. Saporito, CPCU, and Lamont D. Boyd, CPCU, present and immediate past chairmen, have led to the IT Section's receipt of the gold Circle of Excellence. Thanks to Dave L. Mowrer, CPCU, CLU, ChFC, for his hard work in putting together our submission!

IT continues to play a principal part in current events. For example, the Internet's use as a resource for consumers seeking personal finance products and services increased dramatically according to a recent survey by the Dieringer Research Group, a Milwaukee-based marketing information and consulting company. They report that 58.7 million people used the Internet to learn about these products and services with 63 percent or 36.8 million following up offline by applying for personal finance products including insurance products, compared to 21.8 million applying for similar products last year. We will continue to use this newsletter as a vehicle to communicate with the section and to the rest of the CPCU membership on contemporary issues and better business efficiencies.

Planning is underway on topics for our third issue. Consideration is being given to the future of legacy systems, customer relationship management (CRM), XLM standards, and agent's and brokers' use of IT. This is your newsletter. To make it more valuable, please take a few minutes to be an advocate of the section through the newsletter and to improve the newsletter by e-mailing your ideas for future editions to Lamont Boyd (lamontboyd@fairissac.com) and/or to me (bobsiems@lawrls.com or bobsiems@gfpractices.com). ■

IT Committee Spotlight—
Larry W. Lagedrost, CPCU, AMIM, CTM

Larry has 34 years in the information technology industry, with the last 28 in the technology division of the property and casualty section at the Great American Insurance Group and its parent, the American Financial Group, in the home office in Cincinnati, Ohio.

Larry earned his CPCU in 1982 and Associate in Marine Insurance Management (AMIM) in 1996. For the past three years, he has held the position of I/T relationship manager, which is an advocate of I/T to two of GAIC's Specialty Divisions—the Ocean Marine Division and the Specialty Human Services Division (which markets commercial insurance to non-profit organizations). He earned his B.A. in math from Thomas More College. Larry is active in his company's Toastmasters chapter.

He has spent much of his career in project management, developing insurance policy administration computer systems, billing systems, Y2K remediation, and Internet development.

His personal interests include home remodeling. In the past, Larry was a scuba instructor and captain of his local water rescue/recovery team, an EMT ambulance attendant, and a volunteer fireman. ■

Summary of Terrorism Insurance Act (TRIA) of 2002

Information technology will be a critical tool in the war against terrorism and cyber terrorism. Recent federal legislation insinuated the federal government into the reinsurance industry. A short summary of TRIA is helpful to all of us.

President Bush signed the Terrorism Risk Insurance Act into law on November 26, 2002. The immediate, practical effect was to expose insurers to billions of dollars of terrorism risk that they had excluded in the months after September 11. The Act immediately nullified any terrorism exclusions that were in place. Congress addressed this problem with provisions giving insurers 90 days to let their policyholders know that they were eligible for terrorism coverage and quote them a price. The policyholder then had 30 days to accept or reject the offer. Until the notices were provided by the insurers and the 30 days for the insured to respond had passed, insurers were providing terrorism coverage for free. The administrative burden was substantial. Now the industry is faced with the challenge of pricing terrorism risk.

TRIA is in place for three years. The federal government will come to the aid of the insurance industry if terrorism losses exceed $5 billion from a single event. After this threshold is reached, insurance companies must retain a certain portion of the losses under what is referred to as a deductible.

The deductible rises every year the Act is in force. For 2003, the deductible is 7 percent of the companies' direct earned premiums. The deductible rises to 10 percent in 2004 and 15 percent in 2005. The government pays 90 percent of the losses above the deductible and the industry pays 10 percent.

The government plan recoups its payouts from insurers if the industry's loss is below $10 billion in the first year, $12.5 billion in the second year, and $15 billion in the third year. According to one source, the retentions are not small. Individual companies could end up with losses of $1 billion and pay 10 percent on top of that up to $100 million.

According to one source, future terrorist attacks in the United States are likely to be smaller but could cost the industry between $1 billion and $3 billion. Although the bill limits companies' exposure to terrorism risk, the retentions are high. The industry is being asked to take on more risk. There is confusion about the bill's implications.

Many feel that even what some describe as a flawed terrorism backstop in place is better than having nothing at all. It may not prevent heavy losses but it could stop companies from collapsing completely in the event of a terrorist act. An upper boundary for losses is created, and TRIA increases confidence that a terrorist attack will not bankrupt our industry.

The Act is not about protecting the insurance industry. It is about protecting policyholders, and it is designed as a backstop. IT professionals will need to be aware of its provisions and how they will affect their work. If any of the IT section members have been involved in projects related to TRIA, a report to bobsiems@lawrls.com would help follow up on TRIA in future editions. ■

Cybercrime

During 2003, the government has reported that the FBI and other agencies are tackling cybercrime by touting many of their most important Internet investigations. Their effort is dubbed "Operation E-con." Over the past five months, federal investigations have identified many criminal acts. These have ranged from a purported Russian marriage service, in which 400 victims lost about $3,000 each in a scheme that promised them a Russian woman to marry, to online banking fraud.

According to Attorney General John Ashcroft, "Operation E-con" is "a decisive, nationally coordinated effort to root out and take action against some of the leading online, economic crime." These cases have involved not only the FBI and Secret Service, but also the IRS, Custom Service, Federal Trade Commission, Postal Inspection Service, and state and local police agencies. It has been estimated that there were 89,000 victims and the estimated collective losses were $176 million across more than 90 investigations. Since last year, complaints of cybercrimes have increased 300 percent.

Dan Larkin, the FBI's senior representative to the Internet Fraud and Complaint Center says that the FBI is committed to tackling cybercrime. He stressed the importance to the American public because they are the victims. Robert Mueller, FBI director, has stressed that among his most urgent priorities, cybercrime is high on his list. Cybercrimes are difficult to solve because digital evidence is easy to erase or falsify. Often, cybercrimes involve overseas connections, which are hard to trace or can be falsified or erased. According to Ashcroft, "The Internet enables criminals to cloak themselves in anonymity."

Mueller has said that there will be a strong cyberdivision at FBI headquarters under Assistant FBI Director Jana Monroe. The FBI has created 60 specialized cybersquads around the country and they are working on putting investigators in other countries.

If any of the IT section members have been involved in projects related to cybercrime, a report to bobsiems@lawrls.com would help follow up in future editions. ■

Large Agent and Broker Technology Summit

The technology needs of agents and brokers, a possible subject for our next newsletter, has been the focus of a special meeting immediately preceding the Independent Insurance Agents and Brokers Association's convention of September 21–24 in Las Vegas, NV. The large Agent and Broker Technology Summit was put together by the Agents and Brokers Roundtable and included CEOs (chief executive officers) and CTOs (chief technology officers) from major carriers and executives for agency management system vendors.

Robert Rusbuldt, the IIABAA CEO, states: "Our members who comprise IIABA's Agent & Brokers Roundtable wanted to put a special focus on technology issues this year because efficient processes are so critical to the future profitability of their firms. This Summit brought decision-makers into the same room from both the large agency side and the company side to heighten our mutual understanding of the technology and workflow issues affecting them and to recommend improvements that will make both parties more efficient."

The topics discussed included an overview by insurers of their technologies to interface with agents and brokers, agents' and brokers' feedback, and vendors' perspectives and recommendations. Specific topics that were included were downloads and AL3 ACCORD standards, real-time interfacing, and client relations management.

For more information, visit www.independentagent.com. ■

ISO Introduces ClaimDirector℠

Earlier this summer, the Insurance Services Office, Inc. (ISO) introduced ClaimDirector℠. In the last issue of the *Cutting Edge*, the heavy cost of insurance fraud and the role of information technology being used to fight it were addressed. ISO's product is another example of the important place for information technology in the fight against fraud. ClaimDirector is a claim-scoring system. Claim attributes and industry-wide claims histories are analyzed to produce a claims-handling score. The scores are used to administrate how loss handling is assigned and how claim referrals are made to a special investigations unit (SIU). Each claim receives a numerical score, ranging between 0 and 999. The higher the score, the more fraud indicators have been identified. For more information, visit www.iso.com.

New Publication on Insurance Fraud

The Insurance Research Council has issued a new report, *Insurance Fraud: A Public View*. The Council addresses public awareness, tolerances for various forms of insurance fraud, and possible actions by individuals, insurers, and law enforcement to prevent fraud. For more information, go to www.ircweb.org. ■

Spam: Can the Cure Be Worse Than the Disease?

by William C. Wilson, Jr., CPCU, ARM, AIM, AAM

William C. Wilson, Jr., CPCU, ARM, AIM, AAM, is director of the Virtual University of the Independent Insurance Agents & Brokers of America (IIABA). He has served as a trainer and speaker for various organizations, including the Independent Insurance Agents of America (IIABA national conventions and state convention programs and seminars); the CPCU Society Annual Meeting and Seminars, National Leadership Institute and chapter programs; the National Association of Insurance Women (NAIW); the Southern Agents Conference; and the Risk & Insurance Managers Society (RIMS).

Wilson is currently seeking a publisher for his first trade book—the first in his Speakers & Writers NoteBook™ Series—entitled *"Quote"Notes™ . . . The Ultimate Quotational Reference System and Authoring Tool for Professional Speakers and Writers*, a work that has received the endorsement of Zig Ziglar, Brian Tracy, Terry Paulsen, and other prominent authorities.

Individuals, organizations and their ISPs are increasingly implementing e-mail filters, with the goal being the reduction in, if not the elimination of, spam. It could be that their efforts are largely wasted and, more important, that the cure can be worse than the disease . . . and perilous to their businesses. Here's why. . .

In the past, I've written about subscribers of our Virtual University newsletter that have had problems receiving it due to e-mail filters. Like most organizations, IIABA receives tons of spam, so we recently implemented an e-mail filtering system. Unfortunately, one of the side effects is that now we can't receive the newsletter!

Upon checking with our IT department, I learned that our service provider uses an e-mail filter that had a chain mail setting to bounce any e-mails that suggested they be forwarded to others. Needless to say, most any legitimate newsletter that would like to have readers would mention something about passing along the newsletter to others.

To make a long story short, we've gotten that setting revised to permit the newsletter to make it through our system . . . at least until I send out an issue with another term or phrase that triggers the spam blocker. Our IT head assures me that the e-mail filter is blocking a huge amount of spam, and I believe him (though I sometimes wonder how those 15 Viagra™ e-mails get through to me when I check my e-mail every morning).

However, it's clear that our current filter settings can, and do, block some legitimate e-mail. When this happens, a message to that effect goes back to the sender. Hopefully, the senders won't accidentally or mistakenly delete it, not knowing that their e-mail never made it through. Also, what if the e-mail is an urgent message from a VIP or one of the government officials that we often deal with? And, for your agency or company, what if a critical e-mail from a client or underwriter is blocked? Obviously, this could cause problems for you . . . and your E&O carrier. So, what can you do about it?

Don't use e-mail filters. One thing you could do is not employ any e-mail filters, either on the e-mail server side or individual PCs. Expect to be bombarded with spam. So, while you wade through the spam every day, much of which could be offensive to your employees (and one wonders how long it would take before an employee filed a sexual harassment suit for failure to filter pornographic e-mail), you'll have the assurance that you won't miss any legitimate e-mails. . . unless you overlook them while on a spam search-and-destroy mission. You might not be able to get around server-side filters if you use an outside e-mail service provider who cannot change filter settings for individual clients.

Use more effective e-mail filters. There are several major spam-filtering systems being used by ISPs, including Brightmail, Mailshield by Lyris, Realtime Blackhole List by Mail Abuse Prevention System (MAPS), and ScanMail eManager by Trend Micro. AOL and Yahoo! use proprietary systems.

In tests conducted in March 2001 by eTesting Labs, Inc., Brightmail was found to be the vastly superior server-side system at that time. During its test, Brightmail successfully blocked 94 percent of spam, while 100 percent of

legitimate e-mail was allowed through the system. Next were Yahoo! and AOL, which blocked 64 percent and 28 percent of spam, respectively, followed by Trend's ScanMail eManager at 18 percent, MAPS at 12 percent, and Mailshield at 3 percent of spam blocked. Most of these systems other than Brightmail allowed more than 95 percent of legitimate e-mail through the system. For a full copy of eTesting Labs' report, visit its web site at www.etestinglabs.com.

Note: While full results are not in, eTesting Labs just recently repeated this study and, while Brightmail continued to be vastly superior to other products or services, it now only screens out 73 percent of spam (compared to 94 percent a year and a half ago), followed by AOL and Yahoo! at 40 percent and 36 percent, respectively. It would seem that we are losing the war on spam. One estimate is that 40 to 50 percent of all e-mail is spam, and that number could reach 60 percent by the end of 2003. Needless to say, this puts a significant burden on e-mail systems, driving up the cost for everyone.

Note: It was interesting to see that the Blackhole MAPS system was quite ineffective in blocking spam. We have a couple of major organizations with dozens of newsletter subscribers who are unable to receive the VU newsletter because our newsletter service provider is on MAPS' Blackhole list as a "spam haven." With a success rate of only 12 percent in blocking spam, we wonder how much other legitimate e-mail is being blocked by its system.

As existing filtering systems attempt to become more sophisticated, professional spammers appear to be staying a step ahead. As these filters employ increasingly more complex recognition algorithms, spammers can experiment with different phraseology to defeat them. It's similar to viruses, bacteria, and other microbes that genetically mutate to become more resistant to vaccines. So far, the spammers are winning. But one possibility for the future is a personalized system being promoted by web guru Paul Graham (www.paulgraham.com).

This system employs something called Bayesian filters that can be "trained" to recognize spam. Initial testing indicates that these types of systems are more than 99.5 percent effective in blocking spam, while permitting 100 percent of legitimate e-mail to come through. One such product now available for $20 is SpamSieve (www.c-command.com/spamsieve/), though even more effective products are in development.

Not only will more effective filtering systems result in less spam in your inbox, but such systems could go a long way toward ending the spam industry. It currently costs professional spammers only about $200 to send a million e-mails. Although response rates are perhaps 15 per million at best (compared to 3,000 per million for catalog mailings), if you're sending out 80 million e-mails every two weeks, as one professional spammer does, it's easy to see that spamming can be very lucrative.

According to the November 2002 issue of *PC World* magazine, "Louisiana spam sultan, Ronnie Scelson," sends 80 million e-mail messages twice a month for a client who sells insurance. At least 700 people respond and 400 of those are converted to paying customers. Scelson receives $12 per response (i.e., $16,800 a month, or $201,600 annually, for this one client). If the client nets just $50 per new customer, that's $480,000 a year! And all of this from a monthly response rate of only one person per 400,000 e-mails, or a 0.00025 percent response rate!

In another report on e-mail marketing from DoubleClick, Inc. about spammers, the success rate was much greater. For every 1,000 e-mail messages sent, three purchases were generated, with an average order size of $101.55. A response rate of 0.3 percent may sound low (i.e., 99.7 percent of recipients ignored the spam), but we're talking about solicitations sent to millions of people. If the spammer above sends "only" 10 million e-mails (a low number for professional spammers), that would generate sales of more than a million dollars per mailing! One major spammer claims that he generates $250,000 of revenue per month!

So how can an effective e-mail filtering system put these people out of business? Simple . . . by reducing the response rate to a negligible level. If the spams can't get through, then there's no one to respond and no money to be made.

So far, it appears that client filters (those on individual PCs) are increasingly much more effective at blocking spam (but not legitimate e-mails) than server-side filters. For example, one of our VU newsletter subscribers recently installed MailFrontier's Matador (www.mailfrontier.com).

When Matador suspects spam, or otherwise receives an e-mail from an unknown source, rather than block the e-mail, it automatically responds to the sender that the e-mail has been placed on hold. To permit your e-mail to be delivered, you must click on a link that will enable your e-mail address to be added to the "Allowed" list maintained by the software. Since professional spammers use automated systems, there is no one to respond to this message, so their e-mails are permanently blocked while legitimate e-mails (like the VU newsletter in this case) continue to go through.

Lobby for legislative relief. A number of states have implemented spam laws (www.spamlaws.com). However, since the Internet knows no state boundaries, enforcement could be expected to be relatively ineffective against out-of-state spammers. What is probably needed are federal laws dealing with unsolicited commercial and pornographic e-mail sent via automated systems. It's interesting that a newsstand can't display a *Playboy* magazine where minors can see it, but spammers can send children the foulest and most degrading e-mails imaginable with impunity.

The biggest difficulty with attempting to legislate the problem is the First Amendment. It's very difficult to make it illegal for someone to express an opinion or provide information (if you can call it that), but there are prohibitions already on unsolicited faxes. What could easily be done legislatively is to require that spam e-mails have: (1) a certain prefix in

Continued on page 8

Spam: Can the Cure Be Worse Than the Disease?

Continued from page 8

the subject line or body of the e-mail so that filters can easily separate them from other e-mails, (2) headers (which tell you where the spam came from) that aren't forged, and (3) a provision to opt out much like direct marketers have with snail mailings.

If you believe that spam is becoming an increasing burden on your business and/or an intrusion on your privacy, then contact your Congressional representatives (www.congress.org). For more information on state and federal spam laws and proposed legislation, visit www.spamlaws.com.

Does your agency or company have a newsletter? If you send an e-mail newsletter to your clients, it could be blocked by their e-mail filters or those of their ISPs. If you'd like to check your newsletters before they're e-mailed, there is a great free service from www.SiteSell.net where you can e-mail your newsletter and receive an automated response rating its likelihood (as measured by Spam Assassin) to be blocked as spam.

Finally, if you're so fed up with spam that you just want to vent your frustrations, then point your browser to the "Torture a Spammer Game" http://torturegame3.emailsherpa.com/ and have some fun. ■

Cutting Edge
is published four times a year by and for the members of the Information Technology Section of the CPCU Society.

***Cutting Edge* Co-Editor**
Lamont D. Boyd, CPCU
Fair, Isaac & Company
PMB 214 Suite 45
4727 E. Bell Road
Phoenix, AZ 85032-9380
Phone (602) 485-9858
Fax (602) 485-9874
E-mail: lamontboyd@fairisaac.com

***Cutting Edge* Co-Editor**
Mary C. Moore-Campagna, CPCU, CPIW
(MC)2 Insurance Training & Consulting Services
PO Box 609
Soda Springs, CA 95728-0609
Phone (530) 426-0646
Fax (530) 426-9503
E-mail: mary@mc2itcs.com

***Cutting Edge* Co-Editor**
Robert L. Siems, J.D., CPCU
Law Offices of Robert L. Siems and GF Practices, Inc.
3683 Clipper Mill Road
Baltimore, MD 21211-1900
Phone (410) 366-3796
Fax (410) 366-4613
E-mail: bobsiems@gfpractices.com

Information Technology Section Chairman
Patricia L. Saporito, CPCU
NCR Corporation
6B, 250 Gorge Road
Cliffside Park, NJ 07010
Phone (201) 941-2330
Fax (201) 941-2994
E-mail: patricia.saporito@ncr.com

Sections Manager
John Kelly, CPCU, AIT
CPCU Society

Managing Editor
Michele A. Leps, AIT
CPCU Society

Production Editor
Joan Satchell
CPCU Society

Design
Susan Chesis
CPCU Society

CPCU Society
PO Box 3009
Malvern, PA 19355-0709
(800) 932-2728
www.cpcusociety.org

CPCU SOCIETY INSURING YOUR SUCCESS

Cutting Edge

IT

Volume 10 Number 2 November 2003

CPCU Society
720 Providence Road
Malvern, PA 19355-0709
www.cpcusociety.org

PRSRT STD
U.S. POSTAGE
PAID
BARTON & COONEY