



Joint meeting of the Communications and Membership Committees and UL Promotion Board



Former CSAA President Ron LaFontaine and Katherine LaFontaine celebrated their 39th wedding anniversary during the meeting. Congratulations!



Norman Cheesman (Fire Monitoring of Canada, Inc.) receives a membership plaque from CSAA President Ralph W. Sevinor and Membership Committee Chair Mel Mahler.

This year's social events lived up to CSAA's well-deserved reputation. Good weather and great company blessed those touring the FBI and the Mount Vernon estate, home of President George Washington. Both the Opening Reception and the Board of Director's Dinner were well attended and offered great networking opportunities.

See you in Monte Carlo!

See pages 12-13 for additional meeting pictures—these pictures and others are also available in the "Disaster Management" Web section at [www.csaaul.org](http://www.csaaul.org).

## MYM2000 Presentations


**Below are summaries of most of the presentations. The symbol  indicates that the overheads used in the presentation are available in the Disaster Management Web Section at [www.csaaul.org](http://www.csaaul.org).**

### **DISASTER FORECASTING**

**Claire B. Rubin**, Principal, *Claire B. Rubin & Associates*, used a timeline to show the major catastrophic events and governmental and policy responses in the past 35 years.


She mentioned UL Regulation 827, section 25 which requests that part of the plan identify natural and man-made disaster threats, national and local, that affect a central station. "What is past is prologue," she pointed out to illustrate the need to base forecasting of possible threats by looking at what has happened in the past. She also provided some informational resources to assist central station managers to anticipate disasters.

### **THE FEDERAL AND LOCAL GOVERNMENT RESPONSE TO DISASTER MANAGEMENT**

 **Col. Waldhauser**, *USMC* described the alarm systems' requirements established by the Department of Defense. He also invited the industry to participate in Force Protection Equipment Demonstrations (FPED), trade shows fully-

funded by the DoD to provide decision makers with a view of the available equipment.

**Michael Armstrong** invited the security monitoring industry to join the efforts of FEMA. "I think there are many yet unexplored opportunities where we can merge the disaster resistance agenda and your security agenda into a common agenda," said Armstrong. He used the example of glass design that minimizes damage in case of wind force, and at the same time improves security. He also emphasized the importance of exercising the industry's corporate citizenship by pointing out that "if you invest in your community, you will be able to get back in operation a lot sooner."

 **Chief Ed Plaugher**, *Arlington County, Virginia, Fire Department*, explained how a central station can do a better job to get ready for an incident, based on his experience in developing Arlington County's disaster plan, home of the Pentagon, National Airport and other governmental agencies.

"You got to stay in business...we have sold the entire United States on you being reliable as our built-in fire detection. You will not believe the number of protection

**MYM 2000 PRESENTATIONS, continues next page**

**MYM 2000 PRESENTATIONS, Continued from previous page** - The symbol ☞ indicates that the overheads are available at [www.csaaul.org](http://www.csaaul.org).

laws that we got rid off because of your protecting those buildings day in and day out," said Plaughner.

The first step in preparing your plan is the formation of a comprehensive team of safety planners and players. Next is an assessment of vulnerabilities, looking at all possible disasters, assessing their consequences and probabilities of occurrence. Internal plans already in existence must be reviewed: evacuation, fire protection, safety plans, insurance policies, etc. Internal and external resources for support and critical products must be identified.

The written disaster plan can be prepared once all these steps are completed. It must include an overall summary, an analysis of the emergency management elements, and an identification of the response procedures. It must also include support documents such as building plans, site maps, emergency call lists, resources needed (equipment, supplies, etc.) and a list of outside resources.

Once the disaster scenario is developed, the next step is to rehearse it to assess weaknesses in the plan, to test the abilities and build confidence in the plan.

☞ **Steve Souder**, Administrator, *Arlington, Virginia Public Safety Emergency Communications (911) Center* explored the role of public safety communicators during a disaster. He explained the similarities between PSAPs and central stations and the relationship between the two. He indicated that the same kind of events that affect central stations affect PSAPs. He suggested that central stations consider having their electrical power serviced, if not from two different power grids, at least from two different transformers. He described their alternate location plan and the fact that they can route the 911 and the non-emergency lines with the flip of one switch. He encouraged closer relationships between central stations and PSAPs since both can benefit from each other strengths.

☞ **Chief Ron Siarnicki**, *Prince George's County, Maryland, Fire Department*, described the local government response during a disaster. He explained the responsibilities and the operation of the Emergency Management System, the state-wide Emergency Medical Systems, law enforcement, public works and other services, such as the State Departments of Transportation, Agriculture, etc. He emphasized the importance of identifying a "spokesperson" that will be able to communicate with outsiders, and of planning temporary shelter, food and water, and other resources.

## **DEVELOPING A DISASTER PLAN**

☞ **Jay Heiser**, Senior Security Consultant, *Lucent Technologies*, discussed disaster recovery from the point of view of central station communications. He proposed that the re-

covery of networks and information is more critical than the recovery of the facility. "You can have a backup facility, but if you do not have the information, you are in trouble." The challenge of central stations is that there are limited external redundancy possibilities and that everything revolves around the switch. Some of the solutions are to use FX lines, wireless connections, diverse routing, and SONET (Synchronous Optical Network). One of the main goals is to restore dial tone. The central station should require that it be placed in the list of who gets service restored first. Heiser described the process of how service is restored. He recommended establishing a relationship with the state Public Utility Commission (PUCO) where the central station operates. He believes that using the Internet for central station monitoring is not a good idea at the present time—there is no redundancy; no guarantees of service; and at the moment, no way to authenticate that the incoming signal belongs to whom it says. In addition, it is too exposed to viruses.

☞ **Jay Autrey**, Director of Customer Relations, *Brinks Home Security, Inc.*, spoke about the employee side of disaster planning and recovery. He said that understanding the impact of disasters on your employees is critical. You can test all the other disaster procedures, but the "people" procedure will be hard to test. He emphasized the importance of considering your employees' needs; and of understanding that they will have different levels of commitment to the organization. It is important that you involve your employees in the planning, as well as in the testing of your disaster recovery plan. He analyzed the procedures established by Brink's for hurricanes and bomb threats and recommended having a consistent plan, monthly tests, and frequent updates. He finished with "always plan for the human aspect."

☞ **Charles Hunter**, Director, IS Technology, *Brinks Home Security, Inc.*, discussed the elements of a good disaster plan. He pointed out that the reaction of one can determine the reactions of the group—"so be sure you are the first one to react." He emphasized the importance of having off-site provisioning. Once established at that secondary site, you need to prioritize the recovery—first the central station, then billing (cash flow), customer service, payroll, and the Internet. He reminded attendees that disasters strike at inopportune times—usually at night or on the weekend. He emphasized the importance of tape backups, having all the software versions available, and keeping copies of the plan off-site.

☞ **Kim Schellenberg's**, Central Station Manager, *AAA Alarm Systems, Ltd.*, presentation explained the steps taken by AAA Alarm Systems during the development of its disaster plan a year ago. She described three critical lists needed to manage and recover from a disaster. In addition, she described the building blocks of a Business Resumption Plan (BRP), identifying the information that needs to be collected.

**MYM 2000 PRESENTATIONS, continues next page**

**MYM 2000 PRESENTATIONS, Continued from previous page** - The symbol ☞ indicates the overheads are available at [www.csaaul.org](http://www.csaaul.org).

☞ **Tina Richardson-Jones**, President, *Figaro Consulting*, talked about the seven steps of a disaster plan and what goes on in each of the steps. She also discussed applicable regulations (i.e. NFPA, UL 827). She provided a list of resources with additional information about disaster management, as well as a short outline of the disaster plan used by Ackerman Security.

☞ **Pete Tallman**, Alarm System Group Leader, *Underwriters Laboratories Engineering Services*, described the fundamental ingredients of a disaster plan. As in the case of other speakers, he emphasized the need to collect call lists with emergency employees' names, equipment vendor contacts, municipal agencies and utility contacts. He also described the form and format that should be followed when developing the plan.

### RECOVERING FROM A DISASTER

---

**Craig Leiser**, President, *Kismet Group*, talked about his experiences with disaster management while he was employed at National Guardian. He described how they handled snow storms, hurricanes, and even the arrest of a central station operator. The major disaster that he experienced was when a disgruntled former telephone employee cut a 24-foot T-1 line in 3-foot segments. Due to good planning, the central station was able to communicate with their customers through public phones, cell phones and phones at a remote customer service location to let them know service was down. In addition, the station had spare cable which allowed the telephone company to repair their connection within 12 hours—it took 23 days for the rest of the telephone subscribers in that area to recover.

**Chester Donati**, President, *DMC Security Services, Inc.*, also described some of his disasters experiences and the lessons learned. His first incident occurred before his central station was UL-Listed and only had a runner and an operator. The operator passed out and the runner did not follow the procedure of checking in every 15 minutes. Other incidents included a thunderstorm that knocked down the electricity and also the backup generator—having a UPS system saved the day; a small electrical fire; computer crashes; and the lack of a spare power supply for the phone system. Through all these incidents, Donati indicated that he learned the value of spare equipment and of clear, written procedures so the employees know what to do in case of emergency.

☞ **Bob Rankin**, Vice President, *Protection One*, described what happened when Protection One's Hagerstown, Maryland facility was struck by lightning and lost all telephone and voice data lines. He showed the steps taken to recover and bring the station back into operation minute by minute. The total damage was estimated at \$186,000. The disaster plan and procedures were

evaluated and improved, based on the lessons learned. Despite the popular belief that lightning doesn't strike twice in the same place, the same facility was struck again one year and one day later. The estimated cost of recovering was \$155 this second time (not a typo!).

### THE LEGAL RAMIFICATIONS OF DISASTERS

---

Not convinced of the importance of disaster recovery plans yet? See what **Jeff Gorelick** and **David Chanin** had to say on the subject.

“While your [limitation of liability clause in your] contract should give extraordinary protection in circumstances where an individual incident occurs, if you have gone out to the community and said that you are going to provide service to a certain standard, and when a disaster hits you have not met that standard, you have probably breached the unfair business practice law in your state and the contract is going to be useless in protecting you from the consequences,” said **Jeff Gorelick**, Partner, *Carroll, Burdick & McDonough, LLP*. And further, “if you were to be hit by a class action lawsuit by a large group of your customers who were affected because you failed to document an effective disaster plan, the contravention of UL standards to which you [claimed to] adhere would put your company severely at risk.”

**David Chanin**, Partner, *Tannenbaum & Chanin, LLP*, started his presentation by discussing the enforceability of contractual limitations of liability, giving as an example the case of One Meridian Plaza, probably the largest high-rise disaster in the US involving monitoring. He talked about the importance of being obsessive about developing a quality disaster plan; having valid, signed contracts; maintaining records and ensuring that the history of an account is retrievable even years after the software and the hardware is no longer in use.

“In a disaster, it is extremely important to have counsel familiar with the alarm industry,” added Chanin. Investigators may not be familiar with the industry, what questions to ask and what information to gather; the information gathered may or may not be privileged—“it's extremely important, particularly in major disasters, to preserve attorney/client privilege of all communications.”

In conclusion, Chanin emphasized the importance of the preservation of records; gathering the records promptly after the disaster; having a plan and having the employees instructed on the plan; and having experienced counsel brought in during the early stages to preserve the evidence and the attorney/client privilege as to discussions and to assist in conducting the investigation.

### OTHER THREATS TO OUR INDUSTRY

---

**Todd Schwenk**, Founder & CEO, *Eye On Alarm*, requested the support of the industry for the California Alarm Association's battle against the City of Livermore's restric-

**MYM 2000 PRESENTATIONS, continues on page 17**

**MYM 2000 PRESENTATIONS, Continued from page 10 -**  
The symbol ☞ indicates that the overheads are available at [www.csaaul.org](http://www.csaaul.org).

tions on monitoring. Livermore declared that all commercial buildings with sprinkler devices had to be monitored by their “authorized provider” or by UL-Listed central stations located within the boundaries of the City.

While the current law does not include burglary signals yet, the existing contract between the City and their exclusive provider specifies that the alarm receivers in operation need to be capable of accepting intrusion signals.

Mr. Schwenk opined that “to allow this precedent to ignite could spark a widespread application of monitoring laws from coast-to-coast that would eventually prevent all of our companies from offering monitoring services.”

The California Alarm Association filed a Federal Anti-Trust lawsuit against the City of Livermore for prohibiting free-trade and interstate commerce.

*Editor's note: see page 7 on the result of this lawsuit.*

## INDUSTRY ANALYSIS

**Susan Whitehurst**, publisher of *SDM Magazine*, opened her presentation, “The *SDM 100*: Playing Under New Rules”, by recalling a quote cited by Col. Thomas Waldhauser that summarizes her vision of what is happening in the security industry, “New circumstances require new approaches to the entire scope of how we go about our business.”

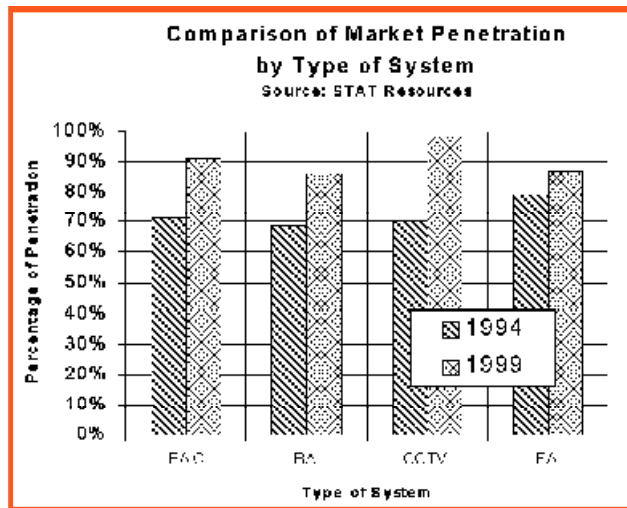
She then contrasted what worked in the “old” economy and what works now. She indicated that “old rules don’t apply—old rules give way” and further, “rules (are) made to be broken.” She proposed that companies must have a global, regional outlook to succeed in the new economy. Other solutions include paying top dollars for quality and managing attrition.

She characterized the new industry as one in which integrated systems are on the rise and one which reaches out to new customers and new markets. New cooperation among stakeholders and new technology hold promise in the area of false alarms. Whitehurst then previewed the results of the latest *SDM 100* survey.

**Albert Janjigian**, former Executive Vice President, *STAT Resources*, reported on the results of the replication of a 1994 market research study of 1,500 security directors of the largest 1,000 corporations in the US.

The survey indicated that the security function is highly decentralized at the local level and that security directors no longer have full purchase authority—chief technical, financial and operating officers do.

He compared the 1999 market penetration of Electronic Access Control (EAC) systems, Burglar Alarm (BA) systems, Fire Alarm systems (FA) and CCTV systems with that in 1994 (see chart above). Of these systems, CCTV and



EAC systems have the highest annual growth rate—14-15% and 12-14% respectively.

Janjigian also identified vertical markets of opportunity: burglar alarms in the communications/utilities market; fire alarms in both the retail/wholesale market and in the communications/utilities market; electronic access control in the retail/wholesale market; and CCTV in the communications/utilities market.

He indicated that computer protection was identified by 85% of the survey respondents as the issue of highest concern, followed by access control (78%), integration of security systems (78%), and the theft of intellectual property (75%). Three new issues were also identified: workplace violence (66%), asset tracking (58%) and employee protection (58%).

On the issue of integration, Janjigian suggested that “you need to make sure you are talking the same language as the people you are selling to.” The survey showed that there is a vast disparity of ideas as to what is an integrated security system, from components that coexist to fully interoperable systems. He added that “for most, the idea of an integrated system is calling one person to get problems fixed.” And “if you are not in all of these different services, you are at a disadvantage when competing against someone who is.”

He concluded by saying that what customers want is to move information around—they don’t want to enter the information more than once—and suggested that the industry become information-centered, rather than hardware-oriented, or other disciplines will start encroaching on our industry.

*The updates on UL and FMRC requirements given by **Pete Tallman**, Alarm System Group Leader, UL Engineering Services, and **Robert Elliott**, Senior Engineer Manager, FMRC will appear in the next issue of the CSAA Dispatch. Both presentations are available at the “Disaster Management Web section” at [www.csaaul.org](http://www.csaaul.org), as well as additional information, articles and links on disaster management.*