



Approach	About	Services	Clients	News & Articles	
----------	-------	----------	---------	-----------------	--

[<< BACK TO AF](#)



OUTLOOK 2002

Security Issues Come to the Fore

by Alan Pell Crawford

The terrorist attacks of last September have forced corporate cultures to change dramatically, from a business-as-usual approach to one in which security issues have come to the forefront.

"Awareness of security issues is everything," according to Elena Gamble, founder of Elena Gamble & Co., an Oklahoma City-based PR firm with several former FBI agents on staff.

PR professionals must respond to the new world in which their clients live and work. Organizations must become more sophisticated about safety and security issues and get up to speed quickly on how to communicate intelligently about them. "I don't think of this as a new opportunity for PR firms," says Gamble. "I see it as a new responsibility to our clients and to the public they serve."

This responsibility involved more than advising clients on how to protect themselves against risk, which is a tall order in itself. It also entails counseling clients on how to communicate effectively about what they are doing to protect their businesses, employees and customers.

In the months to come, concern for security in all its forms -- the security of employees and customers in their physical surroundings and the security of information and information technology -- will need to be incorporated into communications plans. If PR professionals are to offer valuable counsel to clients and fellow employees, they will need to become more knowledgeable

about such issues than the clients themselves are. "PR firms should understand how vulnerable their clients are and what a critical role they play in safeguarding information," says Joseph Cooper, CEO of Digital Defense, San Antonio-based security consultants. "Security is now a huge part of consumer confidence, and PR firms play an important part in instilling and maintaining that confidence."

"Even after Sept. 11, few clients understand how critical security is," says Cynthia Randall, vice president/group account director for AtomicPR, a San Francisco-based firm that represents Digital Defense. According to Randall, many clients do not understand their vulnerabilities or the business and financial implications of a security breach on their premises or with their computers.

"Because companies are embarrassed when their systems are hacked in a way that there's a physical incident in the workplace, they try to conceal it. But a cover-up, even if successful, contributes to the false sense of security that until recently, a lot of companies and their customers took for granted," says Randall.

Richard B. Isaacs, senior vice president, The LUBRINCO Group, which provides international investigative and protective services, says PR firms become involved only after the fact to handle damage containment. "To be really valuable, they need to get involved earlier, educate their clients about security risks, anticipate emergencies and help develop procedures to prevent them and to deal with them should they occur," he says.

Crisis communications plans aren't enough, Isaacs insists. "A lot of companies have plans that the CEO has never seen and no one can find," he says. "Plans have been tested in a real-time simulation or updated as conditions change."

Prevention Planning

Preventing a security breach is much less expensive than dealing with one that has occurred. "It takes \$7 to recoup \$1 in losses from stolen products, and the same kind of pattern holds no matter what kind of security problem you're talking about," Isaacs says.

To offer adequate counsel, PR practitioners need a better understanding of the risks their clients run.

PR firms should also be more aware of the necessity of guarding sensitive client information. "You have to be wary of corporate spies and of competitors," Isaacs warns.

Corporations sustain \$300 billion in information-related losses every year part of which is stolen by corporate spies. Isaacs, whose firm is frequently hired to assess how carefully a client is safeguarding sensitive information, says PR people may unwittingly give away such information. "Unfortunately, PR people are the source of much of their clients' most sensitive corporate intelligence. They give it away in their press releases and at trade shows. We can almost always get any information we're looking for from the market through people who are working the booth. Sometimes they give it to people posing as students writing term papers," Isaacs reports.

PR firms are sometimes privy to information that, by law, cannot be released to the public. "Whenever they're working for clients in highly regulated situations they have to educate themselves about what information can and cannot be released," Cooper says. "They should reassure clients that they understand the sensitivities -- and criminal implications -- involved."

A full-fledged approach, such experts say, involves, at least, the following aspects:

Education

Learn everything you can about the security risks your clients face, so you can educate them. Familiarize yourself with the increasingly sophisticated technology of security, which will be an important part of many clients' strategies. Stress to clients the importance of preventing crises and of incorporating security precautions into their operations and security-related messages in their communications. "You might even encourage clients to retool their corporate philosophy or mission statement to include a safety and security message," says Joanna Brody of Los Angeles-based Schnack & Brody Communications, Inc.

Secure Your Own Systems

PR firms advising clients about security have to make sure they themselves handle information responsibly, in oral presentations, at trade shows and on their computers. Cooper tells of a case in which hackers got into a PR firm's computers and downloaded the draft of a client's press release. They then posted it on the Internet, "which had a tremendously detrimental impact on the client," he says. Securing your own systems may require bringing in security consultants to assess vulnerabilities.

Review Your Crisis Communications Plans

Make sure your clients understand the importance of sending strong messages

to and through their employees. Also remind them that strong messages, backed up by consistent behavior, lack credibility. Security procedures, like having to show corporate ID cards, need to be followed by everyone, including senior management.

Everyone Is A Communicator

Incorporate appropriate security messages into key messages, and then make sure they have been shared throughout the client's work force. Front-line employees, like members of the sales force, bank tellers and customer-service representatives, should be able to respond to security-related questions from customers. Workers who deal directly with the public should also be provided with a source to which they can refer more complicated security-related questions. "If a client has a security officer," Brody says, "media train him or her. Ideally, you want the CEO to speak, but since that's not always possible, make sure the security officer is prepared to deal with the public and the media."

A Richmond, Va.-based writer, Alan Pell Crawford has worked for both M&M Public Relations and Emergence Brand Labs, where he was vice president/director of branding intelligence.