6-27-2000

Cybercrisis management: handling crises at the speed of light

Thomas Stanley Jason
Rowan University

CYBERCRISIS MANAGEMENT:

HANDLING CRISES AT

THE SPEED OF LIGHT

By
Thomas Stanley Jason
© 2000

A Thesis

Submitted in partial fulfillment of the requirements of the
Master of Arts Degree of the Graduate School
at Rowan University
June 2000

Approved by ____________________
Date Approved ______6-27-00______

ABSTRACT

Thomas S. Jason

Cybercrisis Management: Handling Crises at the Speed of Light

Thesis Advisor: Dr. Donald Bagin
Public Relations, 2000

This study's purpose was to compile information on how to handle different types of cybercrises and compile them into an easy to use guide for experienced public relations professionals. The data search included library and Internet searches for information on handling cybercrises. Additionally, an e-mail survey was sent out to on-line public relations personnel to determine their experience with cybercrises. From that survey, professionals who stated that they have handled cybercrises were interviewed via e-mail.

The study determined that 20 percent of those surveyed had faced a cybercrises. The study determined that the most important parts of cybercrisis management were Internet monitoring and the ability to act quickly. This is because cybercrises spread faster than any other type of crises faced by public relations professionals.

MINI ABSTRACT

Thomas S. Jason

Cybercrisis Management: Handling Crises at the Speed of Light

Thesis Advisor: Dr. Donald Bagin
Public Relations, 2000

This study's purpose was to compile information on how to handle different types of cybercrises and compile them into an easy to use guide for experienced public relations professionals. The data search included library and Internet searched for information on handling cybercrises. Additionally, an e-mail survey and interviews via e-mail determined how public relations practitioners in the field are handling cybercrises.

ACKNOWLEDGMENTS
AND DEDICATIONS

To my Mother, my Grandfather and Grandmother:

This thesis is dedicated to you. You were the greatest influences on my life. You taught me to value knowledge and hard work. Without you, nothing I have done would be possible. I love and thank you all.

To Ginger Buganski and Joseph Ogden:

Thank you both for being there for me. We've been through a lot since undergraduate and your friendship and competition inspired me to reach higher than I could have done on my own. A person couldn't ask for better friends.

To Dr. Donald Bagin:

Thank you for your advisement and aid in writing this work. Your dedication and patience have made this work greater than I could do on my own.

To Dr. Diane Penrod, Dr. Denis Mercier, Edward Moore and Larry Litwin:

You've been a big help during my university years. You've inspired, guided and counseled me. You've made my time at Rowan enjoyable and worthwhile. You've molded my mind and I thank you.

To Kyra De Blaker, Jackie Todd and Nancy Urban:

Thank you all for the friendship we've built during this program. You've been there when I've needed someone to talk to and kept me from going mad during this experience.

To Anthony Bersani and Rick Alcantara:

Thank you for your help with research. Without you I'd still be working on this thesis.

TABLE OF CONTENTS

Appendices

CHAPTER 1

Introduction:

The purpose of this study was to discover proven strategies and tactics for cybercrisis management planning and implementation.

With the growth of the Internet, the model of communication between an organization and its publics has changed. In the past, dissatisfied and irate publics were limited in what they could do. The Internet has changed this. Today's technology enables a dissatisfied or irate individual to reach a large number of people, creating the potential to seriously damage or hinder the operations of an entity.

This researcher focused on discovering proven methods for handling cybercrises and compiled them into a guide so that public relations professionals can handle them quickly and efficiently, preventing the damage from escalating.

Statement of Problem:

Information dissemination on the Internet has revolutionized the ways in which public relations practitioners reach their target audiences. The Internet can be a double-edged sword, as the same advances in technology allow damaging rumors, misinformation and disinformation to spread further, faster and with less liability than ever before.

> *The Internet has exacerbated the need for crisis planning. Thanks to the information age and the many-to-many communications model,*

> *crises can emerge from nowhere and turn into all-consuming emergencies with unprecedented speed.*[1]

The nature of the Internet has changed the traditional ways dissatisfied customers or individuals handle their problems. In the past, the individual had great difficulty getting his or her voice heard. The Internet now allows individuals to broadcast their messages with the same reach and scope of a multi-million dollar corporation.

> *While a small company may find the egalitarian nature of an Internet presence advantageous, the down side is that negative public voices have as much authority as anyone else's. Any person with criticisms or negative statements to make about your company, not-for-profit organization, or client has as much visibility as you have. On the Internet, such critics can bypass the media and distribute their manifestos, no matter how outrageous, to Internet users worldwide.*[2]

In only a few short years, crises on the Internet, dubbed "Cybercrises," have cost organizations and individuals countless dollars and hours of lost productivity. A single posting to an Usenet group caused Intel to lose over $425 million.[3] A rogue Web site forced Ford Motor Company to issue a recall that cost the company close to $300 million.[4] An activist group used "cyber pressure" to force Pepsi Co. to sell their Burma operations.[2] While not usually as costly as these, cybercrises can add up. What some

[1] Holtz, Shel, Public Relations on the Net (New York, New York: AMACOM, 1998), p. 198.

[2] Sherwin, Gregory R; Avila Emily N, Connecting Online: Creating a Successful Image on the Internet (Central Point, Oregon: The Oasis Press, 1997), p. 54.

[3] Uzumri, Mustafa V; Snyder, Charles A, " Information Technology and Accelerated Science: The Case of the Pentium Flaw"
California Management Review, Vol. 38 No. 2 Winter 1996 p. 44-63, 20 pp.

[4] Coombs, Timothy W., "The Internet as Potential Equalizer: New Leverage for Confronting Social Irresponsibility"
Public Relations Review, Vol. 24, No. 3, p.289-303.

view as minor irritants when taken as a whole affect company image. And eventually they have an impact on the bottom line.

Hackers are a growing concern in the world of cybercrisis management. Traditionally content with cracking codes, passwords and databases, hackers are now beginning to intrude on the communication process between an organization and its publics.

> *Although a relatively small group, online hackers maintain a great presence on the Internet and therefore pose a great obstacle for public relations professionals because they are disenfranchised consumers who have a deep understanding of the medium.*[5]

Disgruntled hackers are using their skills to pose as representatives of companies to post false or misleading information to damage the reputation of an organization. Some are even going so far as to hijack the web site of their target and use it to further their cause. While organizations and people in the public eye are the main targets, private citizens may find their homepages "sitejacked." An example of this is when a hacker sitejacked the homepage of Turkish citizen Mahir Cagri, turning it into an object of amusement, turning his life upside down.[6]

In a presentation to the National School Public Relations Association, Rowan University professor Edward H. Moore, APR stated:

> *Technology is freeing our traditional supporters and critics to set their own agendas. The future will belong to those of us confident enough*

[5] Basso, Joseph, "How Public Relations Professionals are Managing the Potential for Sabotage, Rumors, and Misinformation Disseminated Via the Internet by Computer Hackers"
IEEE Transactions on Professional Communication, Vol. 40, No. 1 March 1997 p. 28-33

[6] Weise, Elizabeth (1999) Web hijack turns Turk into sensation. USA Today. Found on: www.usatoday.com/life/lds050.htm

> *in our thoughts and convictions to do business in this engaged environment.*[7]

With the advent of the new technologies of the Internet, a study of cybercrisis management is needed. Traditional crisis management is failing to keep pace with today's technology. To combat this, new and proven methods are needed to handle these incidents. This study set out to meet the goal of discovering and compiling these methods for the use of public relations professionals.

[7] Moore, Edward H, National School Public Relations Association 46th Annual Seminar, Baltimore, Maryland. July 20, 1999

Definition of Terms:

Cybercrisis – a crisis of image starting on or growing through the Internet.

Discussion Forum- generic term that encompasses newsgroups, listservs and message boards.

E-mail- an electronic two-way form of communication, an electronic memo.

Flamemail- an email sent to incite or anger an individual person or organization.

Internet- a global network of interconnected computer networks.

Listserv- an e-mail mailing list

Message Board- a non-Usenet newsgroup hosted by a Web site.

Netiquette- standards for behavior established for the Internet.

Newsgroup- a virtual community facilitated by the Usenet system.

Usenet- the system of asynchronous discussion groups on the Internet.

Posting- a single message added to a discussion group

World Wide Web- the universe of resources on the Internet using the HTTP protocol.

Web Site- a collection of Web pages that combine to form a complete entity.

Cookies- packets of information stored on a user's computer that can be collected and analyzed by special code in a Web site.

Rogue Web Site- a web site created with the intent to harm or damage an entity's reputation.

Hacking- the illegal act of breaking security measures via a computer for malicious or other purposes.

Hacker- one who practices Hacking

Sitejacking- the act of hacking a Web site or its address to take control of it.

Cyberpressure- is using the power of the Internet to force a person or organization to do something they wouldn't normally do.

Assumptions and Limitation:

This study assumes that public relations practitioners have a basic understanding and working knowledge of the World Wide Web. The study also assumes that the organization the PR practitioner represents maintains some form of presence on the Web. Another assumption is that the growth of the Internet will see the growth and spread of cybercrises.

The last assumption is that the employer of the PR practitioner views cybercrises in a negative light and wishes them to be handled in an efficient manner.

Limitations include finding experts in a field still in its infancy who are willing to share their knowledge and experience. A dearth of reference material exists since the topic is only a few years old.

The final limitation is that the technology that the web uses evolves faster than any previous technology. While the majority of information gathered by this study will be relevant for a long time, specifics may change due to the advent of new technology.

Significance of the Study

The Internet is the greatest communication tool developed by man. A truly global community, it brings people together in ways that would never be possible in the past. These interactions of cultures challenge professional communicators like never before. Techniques used in the past to handle traditional image crises may not be relevant with the advent of the cybercrisis.

The intent of this researcher was to discover proven methods of cybercrisis management and compile them into a single reference source for public relations professionals. Professionals will be able to refer to this study to aid them in planning for and dealing with cybercrises.

CHAPTER 2
Literature Review

This researcher discovered literature relating to cybercrisis management through a variety of sources including web sites, on-line databases, search engines and on-line retailers.

Books on the subject were discovered through Amazon.com's books in print search engine. The key words used for this search were "cybercrisis," "cybercrisis management," "public relations," "Internet," "crisis public relations" and "online relations."

Pertinent on-line databases were searched through the Rowan University Library Homepage. These databases included Lexis-Nexis, WebSpirs and the Virtual Academic Library Environment of New Jersey (VALE). The key words used for this search were "cybercrisis," "cybercrisis management," "public relations," "Internet," "crisis public relations," "online," and "hacking."

Web sites maintained by public relations practitioners and agencies were searched for information relating to cybercrisis management. The researcher found these sites through Internet search-engines, as well as previous literature review.

A large number of articles about the topic were discovered. The majority only served to outline the problems, without discussing how to handle the problems. The majority of articles that were helpful in determining how to handle cybercrises were discovered on agency web sites.

This chapter will attempt to review the secondary research related to cybercrisis management. This section will list and define the known types of cybercrises and offer experts' suggestions on how to handle them.

Classifications of Cybercrises

This researcher was unable to turn up any complete listing of the types of cybercrises that exist. Instead this researcher will list and define the most common types of cybercrises as they are discussed in material relating to cybercrises management.

The closest to a comprehensive list this researcher found was the article "What to Do When a Crisis Hits—and How You Can Prevent It" in the journal "Interactive Public Relations." This article lists several types of cybercrises and gives the following advice on how to handle them:

- *False representation of your company.*

There have been a number of cases where stock shorters have put out false and misleading press releases, ' Middleberg says. Here 's how they work: They take one of your existing press releases—with your corporate logo and other formal identifiers—from your Web site, and then they modify the text as they wish.

Solution: Insert a special code in your online news releases, and disclose the code only to trusted reporters so they can distinguish your bulletins from spurious ones.

- *Hacks that paralyze your Web site.*

Recall the incident in October when the New York Times Web Site was shut down for more than nine hours—two days after the publication of the Starr Report, a standard-setting traffic driver. For newspaper sites like the

Times, a hack risks credibility. What if the hackers had changed content? Of course, commerce sites risk revenue and consumer confidence, as well.

- *Trademark infringements that enhance violators' own credibility.*

'We have seen cases of people using our advertising in places that we haven't approved,' says Intel spokesman Chuck Mulloy. 'If it's a questionable site, they may be able to gain some credibility by putting our brand up there. We take those sorts of unauthorized uses very seriously.'

- *Employee Publication of unauthorized information.*

If an employee—even with the best of intentions—visits an online chat room and says, 'I understand there's a big contract about to be signed,' Wallace explains, it essentially forces management's hand. Since it is functionally a selective disclosure, 'you then have to issue a release to either deny what's being said in the chat room or confirm it.'

An ounce of prevention: Internet use policies

Your Company should have a published Internet use policy that makes it clear to your employees exactly how they can use the Internet.

No matter what form an online PR crisis takes, be aware that what takes place on the Internet is not divorced from the rest of the world. 'Your online communications should be a strategic component of your entire communications plan,' Middleberg says. 'If there are misleading perceptions or inaccuracies taking place online, you have to deal with it in all media—not just one. You can't deal with the online media in isolation.[8]

[8] "What to do when a crisis hits—and how you can prevent it"

Rogue Web Sites

Another type of cybercrisis is the "Rogue Web Site." In the book "Public Relations On The Net: Winning Strategies To Inform And Influence The Media, The Investment Community, The Government, The Public And More!" the author, Shel Holtz, states that:

> *In the broadest sense, "rogue" Web sites (a term coined by New York public relations agency head Don Middleberg) are unofficial sites that address a company, a product, or other entity that is owned by another group. Rogue sites break down essentially into two categories: those that merely appropriate intellectual property (such as sites established by fans of a television show or movie), and those that attack something. Both categories of rogue sites have generated concern among companies that make major investments in establishing brand images, only to see them affected by a site that an individual with an agenda can build in an afternoon.*[9]

Some famous examples of Rogue Web sites are www.flamingfords.com and www.untied.com.

Fan Sites:

Holtz gives the following advice for dealing with Fan Sites:

Interactive Public Relations, http://www.ragan.com/html/main.cgi?sub=180&bum=0&maga=&reach=8558&base=story&ma=IPR

[9] Holtz, Shel, Public Relations on the Net (New York, New York: AMACOM, 1998), p.183-184

If your organization owns the trademark or copyright for an entity that is likely to encourage the creation of fan sites, avoid a "scorched-earth" policy that treats all sites the same. Instead, evaluate each site. Do nothing if the site does not:

- *Use copyrighted materials.*
- *Misrepresent the entity.*
- *Potentially damage the company's ability to earn profit from the entity.*

Except for the use of copyrighted materials, the situations listed above do not necessarily represent any violations of trademark or copyright law. Except for instances of copyright violation, assess the site to determine the degree to which it could damage your company's investment. Only if it meets threshold criteria you establish should you proceed to take other action. Resist the temptation to send letters immediately threatening legal action. Ultimately, those threats can do your brand more harm than good. Try the following steps instead:

1. *If a certain type of site seems to be gaining momentum, try to co-opt the effort and make it part of the company's official approach to branding the entity. Fan fiction, for example has been a part of Star Trek fandom for over thirty years. Since it would be impossible to stop the practice, the owner of the trademark can turn the fan fiction to its advantage, publishing the best efforts, holding contests, and promoting the careers of promising talent. In*

this way, the company does not lose its hold on its brand but rather brings the rogue efforts into the official fold.

2. *Develop an official site from which fans can extract authorized images for use on fan-oriented sites. Use the official site to list acceptable uses of trademarks and copyrights and to explain why the company pursues efforts against unacceptable uses. Provide access to company authorities for questions. These fans are your best customers; they provide public relations that you cannot buy. Rather than alienate them, work with them so their efforts satisfy their desires to promote their favorite entity while also meeting your need to protect the way your brand is presented to the public.*
3. *Use e-mail to contact individuals who built sites to lead them to the official site and to explain what your organization objects to about their efforts. Make it clear that you do not wish to inhibit the free expression of ideas but that you wish to ensure that the brand remains as appealing for others as it did for the fans who built Web sites dedicated to it. Give your phone number or e-mail address (or that of the appropriate company representative) so the fans can discuss specific issues with the organization.*
4. *If these steps do not lead fans to revise their sites, send e-mail that expresses regret that these individuals are putting the company in the position of having to take less agreeable action.*

5. *Resort to legal action only if the site threatens the brand and the owner of the site is completely intractable.*[10]

Attack Sites

"Attack sites" are different from "fan sites" in that their purpose is to purposely damage the reputation of an organization or its product. Shel Holtz states the following about "attack sites."

> *Attack sites present companies with a different type of dilemma. The whole point of such sites is to turn the general public against a company or its brand based on an individual's disenchantment. Such sites are much quicker to gain notoriety than fan sites. They can be built by disgruntled customers (such as the Flaming Ford site mentioned earlier) or by former employees.*
>
> *Many companies approach rogue attack sites by engaging attorneys. This can be effective in removing the site, since few of the "little guys" who establish sites can afford the fees associated with fending off a legal attack funded by a corporate entity. However, companies need to be aware that often it is only the money that produces the desired results: The force of the law itself is questionable. Companies cannot win a case in court simply because somebody has made derogatory comments about them; the First Amendment guarantee of free speech protects such comments. Instead, the law requires a company to prove it has suffered damages specifically as a result of an attack Web site, considering that companies are still struggling to figure out how to measure the effectiveness of their own Web sites!*

[10] Holtz, Shel, Public Relations on the Net (New York, New York: AMACOM, 1998), p.185-186

Further, sending lawyers after purveyors of attack Web sites can serve to add fuel to the fire. Somebody who already has enough strength of conviction to take his anger to the World Wide Web would not hesitate to respond to a legal challenge. For instance, when the Internet service provider that hosts the "Distorted Barbie" site forwarded a threatening letter from Mattel to the site owner, the owner added a new page to the site rather than remove it. The page begins:

"Two days ago I received an e-mail from my Internet Provider requesting that I remove this Web page from the Internet. They explained that a lawyer from Mattel had claimed that The Distorted Barbie violates Mattel's copyright on Barbie."

The page includes a graphic reproduction of the actual letter from Mattel, an excerpt from a Los Angeles Times article about Mattel's efforts to protect Barbie, excerpts from other materials that support the author's position, and the following statement:

"I do not mean to imply that there are any easy answers here. As an artist, I appreciate and respect copyright laws. What I am suggesting is that an image, when it becomes ubiquitous within a culture, ceases to be simply property. It enters into and becomes part of an ongoing cultural conversation. And the Web is a medium that calls attention to-and gives concrete form to-this conversation."

As people read the editorial opinion of the page's author, they may decide to support his point of view and develop their own sites. The effort to remove his page through legal strong-arm tactics will have backfired, even if the company *ultimately wins its effort in court to have the site taken down. Another site that attacks Mattel's approach to protecting the Barbie property features quotes from Mattel executives who admit that Barbie has been marketed as a person and not a doll. How damaging would it be to the company's efforts to protect its' trademark if a court determines that Barbie has, indeed entered the realm of popular culture, open to any artistic or editorial interpretation that anybody can dream up? Finally how much more damage is done to a company's reputation when it is branded, among a segment of the product-buying population, as an opponent of free speech?* [11]

How To Deal With Attack Sites

Holtz offers the following advice on dealing with Attack sites:

The best approach is to send an e-mail to the site author. The following templates can serve as models for constructing your e-mail to the author of an attack site borne of a bad experience with your company.

Template: E-Mail to Attack Site Author When the Site Focuses on a Case of Perceived Mistreatment

Dear Name:

I was recently directed to the World Wide Web site you have built and was quite distressed to learn of your grievance with our company. The circumstances you cite contradict the core values of our organization and the approach we insist our representatives take with customers.

[11] Holtz, Shel, Public Relations on the Net (New York, New York: AMACOM, 1998), p.186-188

I hope you will give me the opportunity to rectify the situation. Please call me at phone number so I can get the details of your situation and take action to make sure we appropriately and adequately address your concerns and rectify any misunderstandings for which we may have been responsible.

Company Name certainly respects your right to use the World Wide Web – and any other legal means – to express your feelings. However, we feel it would benefit both of us if we can achieve our ultimate goal of satisfied customers.

I am looking forward to hearing from you.

Template: E-Mail to Attack Site Author When the Author is Not Satisfied With a Company Decision

Dear Name:

I was recently directed to the World Wide Web site you have built and was quite distressed to see that you have chosen to take your dispute with our organization public. I have researched the case your site addresses and believe we can speak with each other directly. Please call me at phone number so we can discuss the situation. If the information you present in the course of our discussion warrants it, I will see to it that your case is reviewed.

> *Our goal always is to serve the interests of our customers and to adhere to the guidelines and rules by which our business is governed. I believe a candid conversation between us can resolve any differences we may have.*
>
> *I am sincerely looking forward to hearing from you.*[12]

General Advice On Dealing With Rogue Web Sites

Holtz gives the following tips for dealing with Rogue Web sites:

1. *Assess the potential damage of the site as a means of measuring your response.*
2. *Contact the author of the site to determine the core reasons he (sic) is attacking your organization.*
3. *Offer to find a way to resolve the differences.*
4. *Make sure your company Web site offers your point of view on any issues of substance addressed on the rogue site.*
5. *Provide material the site author can use that more accurately reflects your company's position or activities.*
6. *Use legal muscle only after all other avenues have been exhausted (That way, you can always say that the organization tried to reason with the site author before resorting to more draconian means.) Make absolutely sure that the site violates a law that can be upheld in court. Do not use the threat of a lawsuit as a means of getting somebody to back down who is*

> *not violating the law but cannot afford to fight against the resources your organization brings to bear.*[13]

Calling in the Lawyers

The content on some rogue Web sites borders on libel. While it may be tempting to go after the publishers of libelous material, lawsuits can sometimes cost more than they are worth. Don Middleberg offers the following advice.

> *Cases where libel may be involved present more problems. Lawyers will want to take action, but this may not be the best way to handle the situation. Because there have been few precedents and rulings concerning libel and the Internet, it is unlikely that your company will win such a suit. In addition, the case will likely be expensive and may very well draw unwanted media attention to the crisis.*
>
> *The nature of the Internet allows people to publish any information they want, virtually without consequence, no matter how offensive, inaccurate, or vulgar. In light of this, a careful public relations plan should be considered before taking legal action.*
>
> *For the McLibel case, McDonald's made a mistake in taking the case to court. In court, sensitive information about McDonald's business practices became available to the public for the first time. Ultimately, it*

[12] Holtz, Shel, Public Relations on the Net (New York, New York: AMACOM, 1998), p.188-189
[13] Holtz, Shel, Public Relations on the Net (New York, New York: AMACOM, 1998), p.192

> *was because of the availability of this information that the McSpotlight site was developed, thus worsening the situation for McDonald's*[14]

Others agree that often attacking a Web site can be worse than letting it lie.

> *Tackling an offending Web site with legal action can be tricky, agrees Tim Wallace, executive vice president at Makovsky & Co., a PR agency in New York which manages online crisis management. 'Sometimes these sites can become damaging not because of the actual site—but because of the attention they get.*[15]

Instant Activists

Holtz discusses another type of cybercrisis, the instant activist. Holtz describes instant activists as individuals and groups who lash out against an organization to damage its reputation and raise opinions against it. In the past these individuals didn't have the resources to reach a broad audience with their message; the internet has changed all that. While related to rogue Web sites, these activists can present their damaging messages through a variety of channels including email, Usenet, message boards, discussion groups, mailing lists, and IRC Chat. He cites two case studies in his book. The first deals with the attacks launched against Nutrasweet Kelco by an unorganized, unnamed activist group. He used the following real example of a posting to Usenet. (Errors are reprinted as they occur in the originals.)

[14] Middleberg, Don, Rogue Web Sites Pose Threat To Corporate Image, Tactics November 1996 Issue Highlights Special Report: Winning On The Web, http://www.prsa.org/tacfiles/novsp196.html

[15] Control the Rogues, Interactive Public Relations, http://www.ragan.com/html/main.cgi?sub=180&bum=0&Maga=&reach=8561&base=story&ma=IPR

> *Subject: Re: what's up with NutraSweet™*
> *From: Betty Martini betty@noel.pd.org*
> *Date: 1996/07/20*
> *Organization: Emory University, Dept of Math and CS*
> *Newsgroups: misc.health.diabetes*
> *Dear Jonas: Richard Wilson, widower of Joyce Wilson who went blind and died from NutraSweet™ says it kills fire ants instantly, and he used Equal. He was about to market aspartame as an ant killer because not only does it kill ants just like it killed the monkeys and rats in the studies, and his wife and other victims, but he thought he would make a point. Recently, someone wrote and asked for information on aspartame because she said she was doing a study of whether dogs and cats liked sugar or aspartame best. I thought it was a joke and wrote back and said: "You wouldn't really do that to pets, would you? This is a joke, isn't it?*
>
> *However, I am sending you all the information you requested and more on aspartame including independent studies." Then a few weeks later I get a letter from her saying it really wasn't a joke and they did do the experiment. They made two piles and neither the dogs or cats would touch the aspartame and then she said: "Would you believe even the ants wouldn't touch it!" Well, ants are pretty smart, aren't they? They won't knowingly consume poison! Humans should be so smart!*
>
> *Regards,*
> *Betty*[16]

Holtz goes on to explain that this message was part of an ongoing attack campaign she waged that consisted of 556 articles posted during 1996, 80 percent of which generated follow-up articles from other Usenet users. He continues that her single mindedness is an example of how Usenet can be used by an individual to generate an activist movement in a manner that simply was not possible prior to the development of Internet-based many-to-many communication.

Dealing With Instant Activists

Often, posts like the one above are considered a breach of netiquette and will be met with outright hostility by regular users of the channel they were posted in. However, this is not always the case and Holtz advises against letting others fight your battles for you. However, a follow-up post would only add credibility to the activist's accusations.

In a situation like this, Holtz advises posting your side of the story along with evidence to your company's Web site as Monsanto did in an effort to deal with the rumors about NutraSweet™.

> *In general, the majority of posts are clearly based in the opposition camp. As true believers, they will not be dissuaded by rational discussions undertaken by the company. Monsanto's best defense: Use its Web Page (at* www.nutrasweet.com*) to promote the healthful nature of its product. The section of the site that offers the health related information is not reactive. Instead, it is a simple presentation of facts, ranging from physician testimonials to official FDA records from the process the product underwent in order to get government approval. Though the activists will not be convinced, the consumer who stumbles upon the activist point of view will likely want to visit the NutraSweet page in order to see what the company has to say. Its authoritative information stands a good chance of negating the information that led consumers to check out the home page in the first place.*[17]

If the person became an activist due to a mistake or misunderstanding, Holtz suggests contacting him or her directly.[18]

However, Holtz states that companies who find themselves dealing with instant activists usually haven't undertaken two-way symmetrical communication with their audiences. He states that they are a symptom of a larger issue that needs to be addressed. In cases like this, Holtz states that instead of legal action, that it is "Far more effective to

[16] Holtz, Shel, Public Relations on the Net (New York, New York: AMACOM, 1998), p.181
[17] Holtz, Shel, Public Relations on the Net (New York, New York: AMACOM, 1998), p.182

move beyond the realm of the Internet and engage in a negotiation based communication effort that results in victory for both the activist group and your company, in the end turning the group into an ally. Holtz offers the following example in which Edelman Public Relations successfully negotiated the Star-Kist Seafood Company out of a situation where activists had brought the incidental deaths of dolphins in the tuna canning industry to the attention of consumers.

> *The company finally agreed with Edelman Public Relations that it should be the first tuna-canning company to announce a dolphin-safe policy - that it would buy tuna only from fishermen who adhered to standards that minimized the risk to dolphins. Edelman and Star-Kist met with representatives of key environmental groups as well as government leaders, before making the announcement. The actual press conference featured not only Star-Kist but environmental groups representatives who lauded the company's announcement.*
>
> *Edelman claims the resulting publicity generated nearly a billion impressions in a one-week period. Sales increased proportionate to the outpouring of customer support.*[19]
>
> Holtz goes on to state that while not every negotiation will result in a reversal of a company's position on an issue, direct negotiations can achieve positive results with the activist public that is attacking your organization.

[18] Holtz, Shel, Public Relations on the Net (New York, New York: AMACOM, 1998), p.191

[19] Holtz, Shel, Public Relations on the Net (New York, New York: AMACOM, 1998), p.190

Discussion Forum Attacks

Another form of cybercrisis that Holtz covers is the discussion forum attack. A discussion forum attack is similar and can in fact be a part of a campaign conducted by an instant activist, but more often or not is perpetrated by a disgruntled customer. He offers the following examples.

> *An electric utility manager bought a product that never worked right. When he contacted the customer service department of the company that made the item, he was put into voice-prompt hell and ultimately disconnected three times. After the third time, he took his frustration to a consumer newsgroup on Usenet.* [20]

Dealing With Discussion Forum Attacks

Shel Holtz offers the following four-step plan for dealing with a discussion forum attack.

Step 1. Assess The Potential Damage The Post Can Cause.

> *During a demonstration of DejaNews as a tool for finding newsgroup references to a company, an audience member asked if her company – a major airline – appeared anywhere in the articles available for searching. I entered her company's name and found several messages dealing with the airline, including one that called for a boycott. She was about to dash for the phone when a quick read of the article revealed there was no cause for alarm. The author was recently divorced, and his ex-wife had called the airline with instructions to transfer his frequent-flier miles*

to her account. His anger was the reason he was calling for a boycott. The few responses the article generated said basically, "You think you can start a boycott of one of the biggest business-travel airlines over this? Get a Life!"

Clearly, this article did not warrant any kind of response. The airline's interests were best served by simply ignoring it. You should evaluate each message about your company on the basis of:

- *Its content*
- *The number of responses the article generates*
- *The tone of the responses*

Step 2. Determine to Whom You Should Respond

If an article warrants a reply, determine how to reply-either to the individual who submitted the article or to the newsgroup itself. Often individual contact can result in a swift resolution to the situation, leading to a converted customer who sings your praises instead of damning your inadequacies. If the reference to your organization has become a general topic of discussion in a newsgroup, it may be more appropriate to make your statement to the entire group.

Tip: Keep Your Contact Virtual

Never make direct contact with an individual who has posted something to a discussion group or mailing list. (For instance, don't find the individual's phone number and make contact by telephone.) Someone who posts articles to discussion groups online perceives herself as

[20] Holtz, Shel, Public Relations on the Net (New York, New York: AMACOM, 1998), p. 193

participating in a virtual environment and expects all subsequent communications to come by the same means. Making voice contact can create a sense of disconnect that can alienate the individual, making it much more difficult to engage her than if you keep the discussion where it started-in cyberspace.

Step 3. Read the FAQs and Lurk Before Posting

Find the FAQs (Frequently Asked Questions) associated with the newsgroup before you say anything you may later regret. The FAQs contain all the pertinent information about a newsgroup, including the group's charter and all of the commonly asked questions that already have been addressed in discussions that have gone before.

Even after you have read the FAQs you should lurk for a while before submitting your own article. Lurking (reading posts in a newsgroup without participating) gives you the opportunity to make an assessment of the newsgroup. Is it a valid discussion area, or is it mostly teenagers sounding off? How seriously does anybody take anything posted here? How do people react to responses that disagree with what they have said?

Step 4. Don't Preach-Participate!

Newsgroups are virtual communities. They were well established before your company was mentioned and will continue to exist after the furor over the reference to your company has faded from memory. Members of the community expect new contributors to behave like other members of the community. If you storm into a newsgroup like some sort of authority

> *figure, you earn the community'' disrespect and possibly do more harm than good, even if you do manage to set the record straight.*[21]

Some individuals have tried "Seeding," posting positive responses about your organization under an alias that seem to come from external sources, to combat discussion group attacks. This shady tactic can backfire and harm your organization.

> *Mind the ethics of lurking and seeding. This is almost as sinister at it sounds. Lurking, of course, means you just peruse what others are saying. This is pretty standard for a public relations professional who wants to gauge what people are saying about a client. Seeding is when a person uses a fake name or identity to drop tidbits of positive information about a client, in the hopes of steering the conversation in that direction. This is more typical in chat rooms, but can also be done in discussion lists. Either way, by professional public relations standards this is manipulative, deceitful, and unethical.*
>
> *It can also be dangerous. In the summer of 1997, the Federal Trade Commission reported they would apply typical advertising laws to the Internet. Citing this practice in chat rooms, the FTC said that posting information as if it were from an unrelated third party can constitute deceptive advertising.*[22]

[21] Holtz, Shel, Public Relations on the Net (New York, New York: AMACOM, 1998), p. 194-195

[22] Sherwin, Gregory R; Avila Emily N, Connecting Online: Creating a Successful Image on the Internet (Central Point, Oregon: The Oasis Press, 1997), p. 130

Dissemination of False Information

In "Connecting Online: Creating a Successful Image on the Internet" Gregory R. Sherwin and Emily N. Avila discuss false rumors spread on the Internet.

> *The American Cancer Society handled a situation like this when an e-mail hoax circulated throughout the Internet. The e-mail told the sad story of a little girl who was dying of cancer. Her dying wish was to raise awareness of cancer, so the e-mail encouraged people to make many copies of the message and distribute them to friends, colleagues, Usenet groups and others. The e-mail went on to say that the American Cancer Society was sponsoring this project and would donate a certain amount of money toward cancer research for every message that was duplicated. As far as the American Cancer Society could tell, there was no such little girl and no such case. They posted a warning on their Web site (*http://cancer.org*) explaining this hoax. At the same time, the American Cancer Society encouraged those concerned about cancer to make a donation!*[23]

Another example of this type of crisis is discussed in the article "The Internet: The New Channel on the Crisis Radar Screen" by Don Middleberg.

> *"Warning-Forward- this is not a joke!" An estimated 100,000 people, mostly women and college students, in an affluent Ohio region received this E-mail just this past April.*

[23] Sherwin, Gregory R; Avila Emily N, Connecting Online: Creating a Successful Image on the Internet (Central Point, Oregon: The Oasis Press, 1997), p. 377

The message recounted the "true" story of a woman shopping at a local mall who came out to her car to find her tire was flat. A gentleman in a business suit graciously helped her change the tire but when he asked for a ride to his car, she felt uneasy and drove away. After driving to a local service station to get her tire fixed, she was told that nothing was wrong with the tire and it looked like someone had let the air out. Later she found a briefcase in her trunk, apparently left by the gentleman. When she opened the case, all that was in it was a butcher knife and some rope.

Until an employee of one of the mall's merchants pointed it out to a mall manager, the mall was unaware of the rumor spreading to people throughout the neighboring communities, universities and local businesses. These professionals often flocked to the mall during lunch hours to eat and shop. Fortunately, the communications team at the shopping mall was able to contact appropriate authorities, confirm the fictitious nature of this "urban legend," and make a public statement on the local broadcast news that evening.[24]

Handling Dissemination of False Information

Handling false information disseminated by the Internet can be tricky and very costly. Often, the best way to handle it is through both traditional and online channels as in the following case.

Procter & Gamble had a major PR problem.

[24] Middleberg, Don; "The Internet: The New Channel on the Crisis Radar Screen", Middleberg News, http://www.middleberg.com/middlebergnews/bylines/newchannel.cfm?print_version=yes&

A rogue Web site had started a rumor that P&G's new household cleaner, Febreze, would poison your pet. That rumor had turned into a chain letter that was sent to thousands of P&G customers.

And if you doubt the power of an e-mail chain letter, think again.

"We see the most damage with these chain e-mails because it's friends passing the information to friends," says P&G spokesman Damon Jones. "So people are trusting those incoming messages."

At the height of the crisis, the chain letters were generating more than 1,500 calls and/or e-mails per day from P&G customers, who wanted to know if there was any truth to the rumor. In total, the company fielded more than 25,000 requests for information from customers, says Jones.

To refute the charges, P&G communicators launched a three-pronged PR campaign:

1) *A targeted letter campaign that distributed more than 60,000 letters to pet breeders and veterinarians, so that these industry experts would learn the truth—and hopefully spread the word that Febreze was safe for pets.*
2) *A Web site campaign, where they solicited statements from third-party organizations that refuted the rumor.*
3) *An aggressive TV and print ad campaign to reach out directly to consumers.*

The campaign worked so well that it is worth taking a look at each component.

The targeted letter was titled: Febreze Pet Safety—Procter & Gamble Responds to Internet Rumor. The purpose of the letter, according to Jones, was to let "industry counselors" know that the rumor was false, and to reinforce the product's safety.

The letter spells out the product's ingredients, and notes that the National Animal Poison Control Center considers Febreze safe to use in households with dogs and cats when used as directed.

That additional third-party reinforcement was one of the keys to the letter's success, says Jones.

To make the letter readable and easy to get through, Jones structured most of it like a Frequently Asked Questions (FAQ) document, like you find on the Web. Some of the "frequently asked questions" were:

What is Febreze?

Is Febreze safe to use around pets?

Is Febreze safe to use around birds?

To back up the letter, P&G also hit consumers with Web-site statements and an advertising campaign.

They posted statements on P&G's Web site from the American Society for the Prevention of Cruelty to Animals, the Humane Society, and the American Veterinary Medical Association. The company also created links to these independent sources to add credibility to its message.

And they launched an aggressive television and print campaign to reinforce pet safety. According to Jones, the campaign caused a 30

> *percent decrease in both customer calls and Web site inquiries. And that's a conservative estimate, says Jones.*
>
> *The three-headed campaign—targeted letters, Web site statements, TV and print ads—worked, but it wasn't cheap. P&G spent approximately $100,000 on the targeted-letter component of the campaign alone, according to Jones, which points out how important it is to take Internet rumors seriously.*
>
> *What can you do about online rumors? Not much, unfortunately. Because of their nature, it's almost impossible to determine who started the rumor, so legal action is almost always out of the question.*
>
> *The only thing you can do is try to stay on top of online rumors, and start refuting them as soon as they appear.*
>
> *Right now, P&G tries to stay on top of online rumors by developing relationships with the Web managers of "urban legend" Web sites. If they get a heads-up that someone is posting a rumor about a P&G product, they immediately post accurate information on the site to refute the rumor. The company also uses an outside company, The Delahaye Group, to monitor the Web and help respond to consumer concerns.*[25]

Two other famous cases, one involving Bell Atlantic and Proctor and Gamble's online battles with the persistent rumor of a company link to the Church of Satan have been handled in similar ways.

[25] "How to Take the Teeth Out of an Online Rumor" Interactive Public Relations, http//:www.ragan.com/html/main.cgi?sub=180&bum=0&maga=&reach=14789&base=story&ma=IPR

In September 1998, BellSouth saw false-informed discussions about its take on a confusing topic called Internet telephony.

Though company staffers responded on message boards, it also created an additional section on its corporate Web site to explain the term and who would be affected. It took about an hour to compile the content in-house, reports BellSouth's director of media relations Bill McCloskey. The section includes the company position, FAQ, key points, a diagram of Internet telephony, a letter to customers, and more. After the section was posted, the link was posted on message boards.

Result: The site generated more than 14,000 visitors in September, down to 1,600 in October, to less than 500 in November.

Also, Procter & Gamble dedicates an entire section—Trademark Facts—to refute the infamous rumor that P&G is associated with the Church of Satan, supposedly started on a talk show. The section provides links third party sites like urbanlegends.com and talk shows that explain the falsehood. The site also posts letters from the company's chief exec, talk show hosts like Jenny Jones and Phil Donahue, and religious leaders that offer support to stop the rumor.[26]

On-line Trademark Violation

On-line Trademark violation is the use of another organization or person's intellectual property without their consent. One frequent problem is Cybersquatting.

[26] "Tips to Cope With Cybersquatters and Content Republishers", The Ragan Report, http://www.ragan.com/html/main.cgi?sub=180&bum=0&maga=&reach=14789&base=story&ma=IPR

Cybersquatting is purchasing a domain name containing the trademarked name of a company or product and then attempting to sell said trademarked name to the company it belongs to at an exorbitant price when they attempt to create their Internet presence.

This is a direct result of people being able to purchase a domain name (Web site address) inexpensively from a domain name registration service.

An article in the on-line journal "Interactive Public Relations" discusses another type of cybercrisis, the on-line trademark violation.

> *Every week Sarah Deutsch worries about someone stealing Bell Atlantic's Web traffic.*
>
> *The infringements could be a competitor or someone using a form of bellatlantic.com to draw the traffic to another site, taking Bell Atlantic content and using it for their own site; or improperly including the company's name in metatags to lure search engine traffic to another site.*
>
> *Deutsch sees about 1,000 of these cases per year and Bell Atlantic, like many other companies, has created a virtual police force to protect the company's online assets. "We've done a pretty good job at policing online trademark issues simply because we see it as an essential part of our branding strategy. Brands need to be enforced online; if not, you'll lose them," warns Deutsch, vp and chief intellectual property councel.* [27]

The article offers the following tips to deal with on-line trademark violation.

> *Consider the following tips to manage your online reputation: Use third party trackers. Due to the increasing growth of unlawful domain*

[27] "Tips to Cope With Cybersquatters and Content Republishers", The Ragan Report, http://www.ragan.com/html/main.cgi?sub=180&bum=0&maga=&reach=14789&base=story&ma=IPR

name registration and coinciding implications, companies like Bell Atlantic, Washingtonpost.com, BellSouth Corp., Procter & Gamble, and others use online reputation management companies to follow message and news boards, identify trends, and more.

Bell Atlantic registered with domain watching service Thompson & Thompson two years ago after it began to see trademark infringements on the Web. At that time, 15-20 cases/week were found by internal staffers—with a steady increase since then.

The company hired Cyveillance six months ago for additional tracking. Recent problems include other sites using the company site's look and feel and other telecom companies using its name in metatags for searches in directories and search engines.

Similarly, Washingtonpost.com hired Cyveillance about one year ago to help deal with other sites republishing its content for commercial purposes. Because the site employs an advertising e-business model, lost or diverted traffic means lost ad revenue.

BellSouth uses Issue Dynamics to help track message boards and news sites for rumors.

Hire/tap in-house staffers to monitor the Web.

Bell Atlantic uses three full-timers and outside counsel to monitor and respond to trademark issues. Also, Washingtonpost.com charges one employee to monitor the Web half-time with all 200 employees keeping an eye on the Web's discussion and news boards.

3) An aggressive TV and print ad campaign to reach out directly to consumers.

The campaign worked so well that it is worth taking a look at each component.

The targeted letter was titled: Febreze Pet Safety—Procter & Gamble Responds to Internet Rumor. The purpose of the letter, according to Jones, was to let "industry counselors" know that the rumor was false, and to reinforce the product's safety.

The letter spells out the product's ingredients, and notes that the National Animal Poison Control Center considers Febreze safe to use in households with dogs and cats when used as directed.

That additional third-party reinforcement was one of the keys to the letter's success, says Jones.

To make the letter readable and easy to get through, Jones structured most of it like a Frequently Asked Questions (FAQ) document, like you find on the Web. Some of the "frequently asked questions" were:

What is Febreze?

Is Febreze safe to use around pets?

Is Febreze safe to use around birds?

To back up the letter, P&G also hit consumers with Web-site statements and an advertising campaign.

They posted statements on P&G's Web site from the American Society for the Prevention of Cruelty to Animals, the Humane Society, and *the American Veterinary Medical Association. The company also created links to these independent sources to add credibility to its message.*

And they launched an aggressive television and print campaign to reinforce pet safety. According to Jones, the campaign caused a 30 percent decrease in both customer calls and Web site inquiries. And that's a conservative estimate, says Jones.

The three-headed campaign—targeted letters, Web site statements, TV and print ads—worked, but it wasn't cheap. P&G spent approximately $100,000 on the targeted-letter component of the campaign alone, according to Jones, which points out how important it is to take Internet rumors seriously.

What can you do about online rumors? Not much, unfortunately. Because of their nature, it's almost impossible to determine who started the rumor, so legal action is almost always out of the question.

The only thing you can do is try to stay on top of online rumors, and start refuting them as soon as they appear.

Right now, P&G tries to stay on top of online rumors by developing relationships with the Web managers of "urban legend" Web sites. If they get a heads-up that someone is posting a rumor about a P&G product, they immediately post accurate information on the site to refute the rumor. The company also uses an outside company, The Delahaye Group, to monitor the Web and help respond to consumer concerns.[25]

[25] "How to Take the Teeth Out of an Online Rumor" Interactive Public Relations, http//:www.ragan.com/html/main.cgi?sub=180&bum=0&maga=&reach=14789&base=story&ma=IPR

Two other famous cases, one involving Bell Atlantic and Proctor and Gamble's online battles with the persistent rumor of a company link to the Church of Satan have been handled in similar ways.

> *In September 1998, BellSouth saw false-informed discussions about its take on a confusing topic called Internet telephony.*
>
> *Though company staffers responded on message boards, it also created an additional section on its corporate Web site to explain the term and who would be affected. It took about an hour to compile the content in-house, reports BellSouth's director of media relations Bill McCloskey. The section includes the company position, FAQ, key points, a diagram of Internet telephony, a letter to customers, and more. After the section was posted, the link was posted on message boards.*
>
> *Result: The site generated more than 14,000 visitors in September, down to 1,600 in October, to less than 500 in November.*
>
> *Also, Procter & Gamble dedicates an entire section—Trademark Facts—to refute the infamous rumor that P&G is associated with the Church of Satan, supposedly started on a talk show. The section provides links third party sites like urbanlegends.com and talk shows that explain the falsehood. The site also posts letters from the company's chief exec, talk show hosts like Jenny Jones and Phil Donahue, and religious leaders that offer support to stop the rumor.*[26]

<u>On-line Trademark Violation</u>

[26] "Tips to Cope With Cybersquatters and Content Republishers", The Ragan Report, http://www.ragan.com/html/main.cgi?sub=180&bum=0&maga=&reach=14789&base=story&ma=IPR

On-line Trademark violation is the use of another organization or person's intellectual property without their consent. One frequent problem is Cybersquatting.

Cybersquatting is purchasing a domain name containing the trademarked name of a company or product and then attempting to sell said trademarked name to the company it belongs to at an exorbitant price when they attempt to create their Internet presence.

This is a direct result of people being able to purchase a domain name (Web site address) inexpensively from a domain name registration service.

An article in the on-line journal "Interactive Public Relations" discusses another type of cybercrisis, the on-line trademark violation.

> *Every week Sarah Deutsch worries about someone stealing Bell Atlantic's Web traffic.*
>
> *The infringements could be a competitor or someone using a form of bellatlantic.com to draw the traffic to another site, taking Bell Atlantic content and using it for their own site; or improperly including the company's name in metatags to lure search engine traffic to another site.*
>
> *Deutsch sees about 1,000 of these cases per year and Bell Atlantic, like many other companies, has created a virtual police force to protect the company's online assets. "We've done a pretty good job at policing online trademark issues simply because we see it as an essential part of our branding strategy. Brands need to be enforced online; if not, you'll lose them," warns Deutsch, vp and chief intellectual property councel.* [27]

The article offers the following tips to deal with on-line trademark violation.

[27] "Tips to Cope With Cybersquatters and Content Republishers", The Ragan Report, http://www.ragan.com/html/main.cgi?sub=180&bum=0&maga=&reach=14789&base=story&ma=IPR

Consider the following tips to manage your online reputation: Use third party trackers. Due to the increasing growth of unlawful domain name registration and coinciding implications, companies like Bell Atlantic, Washingtonpost.com, BellSouth Corp., Procter & Gamble, and others use online reputation management companies to follow message and news boards, identify trends, and more.

Bell Atlantic registered with domain watching service Thompson & Thompson two years ago after it began to see trademark infringements on the Web. At that time, 15-20 cases/week were found by internal staffers—with a steady increase since then.

The company hired Cyveillance six months ago for additional tracking. Recent problems include other sites using the company site's look and feel and other telecom companies using its name in metatags for searches in directories and search engines.

Similarly, Washingtonpost.com hired Cyveillance about one year ago to help deal with other sites republishing its content for commercial purposes. Because the site employs an advertising e-business model, lost or diverted traffic means lost ad revenue.

BellSouth uses Issue Dynamics to help track message boards and news sites for rumors.

Hire/tap in-house staffers to monitor the Web.

Bell Atlantic uses three full-timers and outside counsel to monitor and respond to trademark issues. Also, Washingtonpost.com charges one *employee to monitor the Web half-time with all 200 employees keeping an eye on the Web's discussion and news boards.*

Educate cybersquatters or eyeball-diverters about content use restrictions as part of cease and desist warnings.

Washingtonpost.com typically begins its process with a warning to content republishers. Staffers educate these people about the site's content sharing options, where permission and compliance with specified terms are required. If that doesn't work, a cease and desist letter follows. This works 95 percent of the time, according to senior vp of business affairs and general counsel Caroline Little.

The remaining five percent typically end up in threatened lawsuits. One case goes back about two years ago with TotalNEWS, who framed site content, meaning the news site took content and used its own ads around it.

TotalNEWS settled in favor of Washingtonpost.com. A second, similar case is currently in litigation.

Bell Atlantic typically starts its process with a cease and desist letter. It has sent out thousands in the past two years. If nothing happens and the situation may be harmful to the brand, it threatens a lawsuit. In most cases, the cybersquatter stops here, reports Deutsch.[28]

Web Site Emergencies

[28] "Tips to Cope With Cybersquatters and Content Republishers", The Ragan Report, http://www.ragan.com/html/main.cgi?sub=180&bum=0&maga=&reach=14789&base=story&ma=IPR

The final category of cybercrisis to be discussed in this section is the "web site emergency." Web site emergencies can be caused by a variety of reasons, some malicious, some accidental.

In fact, a recent report by the Computer Security Institute states that Internet attacks against Web sites are on the rise.

> *Results from the Winter 1999 survey: 91 percent of the 521 respondents operate firewalls, but 57 percent of companies still claim the Internet is a "frequent point of attack." That's up from 37 percent in CSI's 1996 survey.*
>
> *Web site attacks span a range of abuses. Of those reporting unauthorized access or site misuse, 98 percent reported "vandalism," 27 percent cited financial fraud, and 25 percent reported stolen "transaction information."*[29]

An article titled "When Your Web Site Disappears," published in the on-line journal Interactive Public Relations, discusses a case concerning the failure of the Los Angeles Housing Authority's Web site during a time of crisis.

> *McQuade attempted to surf the Internet to find out if the story had already hit any online outlets, and if the crisis was being discussed in newsgroups. He also planned to post the news release on the agency's Web site. But he kept getting server errors each time he tried to access HACLA's site. "At first I suspected it was the computer I was on, because*

[29] "Security Group Reports Increasing Internet Attacks", Interactive Public Relations, http://www.ragan.com/html/main.cgi?sub=180&cooked=950503-OJOPM-IT&prof=&origsite=http://www.ragan.com&origcount=&origsub=180&origloc=main.cgi&sub=180&bum=0&maga=&reach=10391&base=story&ma=IPR

MIS was installing a new Sun 5000 system and it was interfering with everything from payroll to e-mail and the direct Web connection," he says. "But the next evening I tried it from home from my wife's computer, and again server error messages popped up. First thing in the morning I confronted the MIS director, who told me that the entire Web site had been deleted, and he was trying to contact the contractor to see if they had it backed up. The contractor told him no.

The immediate effect was that no information was going out and no questions or information were coming into the site. Any email arriving was either deleted or went unanswered until the site was back up.[30] While this case was accidental, others are not.

This week's attacks, on the other hand, bombarded various high-traffic sites with an overflow of information, effectively shutting down normal operations. How do the perpetrators send so much data so quickly? Apparently, the most recent assaults are not typical denial of service pranks, which generally are sent from only one or two computers at a time. "These people scan the Internet for vulnerable systems, and they hack into those systems, and then use hundreds of those computers, remotely, to send the attack," says McClure[31].

[30] "When your Web Site Disappears", Interactive Public Relations, http://www.ragan.com/html/main.cgi?sub=180&bum=0&maga=&reach=5723&base=story&ma=IPR

[31] "Classic Hackers Decry Heavy-Handed Upstarts" CNN.com, http://cnn.com/2000/TECH/computing/02/09/hackers29.a.tm/

The recent publicity of hacker-run "denial of service attacks" on sites like Yahoo, eBay and CNN.com have awakened many people to the security problems that many Web sites have.

> *Clearly something has to be done, because the stakes are so high. The attacks on Yahoo, eBay, Amazon.com and E*Trade earlier this month cost approximately $1.2 billion, according to The Yankee Group, A Boston consulting firm. This figure comes from estimating lost revenues, loss in market capitalization due to falling stock prices and how much money will be spent on upgrading security systems.*[32]

While "denial of service" attacks are a public relations problem, hackers that alter the content of a Web site are more common.

> *When a site has been hacked, its appearance is often altered by chest-beating hackers who leave the cyber equivalent of a "Kilroy was here" scrawl.*[33]

While most hackers generally only attempt to test their skills and the security of a Web site, there are malicious hackers out there who are motivated by greed.

> *An anonymous computer hacker stole credit card numbers from an Internet music retailer and posted them on a Web site after an attempt to extort money from the company failed.*

[32] "Avoiding Future Denial-of-service attacks", CNN.com, 2-2-2000, Http://www.cnn.com/2000/TECH/computing/02/23/isp.block.idg/index.html

[33] "Avoiding Future Denial-of-service attacks", CNN.com, 2-2-2000, Http://www.cnn.com/2000/TECH/computing/02/23/isp.block.idg/index.html

> *The retailer, CD Universe, brought in Internet security specialists Monday to shore up its Web site, as the FBI tried to track down the hacker and customers contacted credit card companies to see if their cards were compromised.*[34]

Every form of hacking is a major concern for PR practitioners of public relations for organizations with an on-line presence. These hacks can not only bring a halt to an organization's operations, but also undermine the trust that their audiences place in them.

> *After all, seeing a multibillion-dollar web site brought to its' knees by a group of not-so-bright pranksters doesn't inspire a whole lot of confidence on Wall Street – or among consumers and advertisers.*[35]

Since an organization's Web site is its face on the Internet, it is important for public relations professionals to take an active role in ensuring the security of their organization's site.

Handling Web Site Emergencies

Web site emergencies usually fall outside of the responsibility of public relations professions and into the realm of information technologies. However, public relations people should be in contact with their organizations IT people and kept abreast of security measures and security breaches as they happen.

Technology changes rapidly and advances in both hacking and security are continually changing. Therefore, it is impossible to compile an exhaustive list of tips and techniques that can be used to stop all attacks on and failures of Web sites. However, this

[34] "Rebuffed Internet Extortionist Posts Stolen Credit Card Data", CNN.com. 1-10-2000, Http://www.cnn.com/2000/TECH/computing/01/10/credit.card.crack.2/index.html/
[35] "Classic Hackers Decry Heavy-Handed Upstarts", CNN.com, 2-9-2000, Http://www.cnn.com/2000/TECH/computing/02/09/hackers29.a.tm/

researcher has compiled a few ideas that may help protect your site or quickly restore functionality in case of a Web site emergency.

The most basic and possibly most important parts of Internet security are the passwords used by individuals who access and maintain the site. Most people pick a word, number or date that they can easily remember. If it's easy to remember, it's easy to hack. In fact, no password is completely unhackable.

> *Think your password is safe because it isn't "password"? If it's in the dictionary, there is software that will solve it within minutes. If it's a complex combination of letters and numbers, that may take an hour or so. There is software that will hijack your desktop and cursor--and you won't even know about it. Hacking doesn't require much hardware; even a Palm Pilot can do it. What protection do you have? "Minimize enticements," say the teachers. If you don't want to be a victim of information rape, in other words, don't let your network give out so many details to strangers.*[36]

In case your site is hacked and goes down, it is vital that you have a backup ready to replace the site if it has been defaced or its server damaged.[37] It is a good idea to keep the backup on a separate server with a different Internet address so that if you are a victim of a "denial-of-service" attack you can switch over to the other server.[38]

There are ways to safeguard against a denial of service attack. These methods do work, but are costly and impact on the performance of a Web Site.

[36] Taylor, Chris "Cracking the Code", Time.com, March 1999, http://www.time.com/time/digital/feature/0,2955,22179-3,00.html

[37] "When your Web Site Disappears", Interactive Public Relations, http://www.ragan.com/html/main.cgi?sub=180&bum=0&maga=&reach=5723&base=story&ma=IPR

[38] "'Dark Sites' Provide Immediate, Ready-Made Crisis Communication", Interactive Public Relations, http://www.ragan.com/html/main.cgi?sub=180&cooked=952193>C?GOT&prof=&origsite=http://www.rag

> *ISP's have a technique that could be used to choke off denial-of-service Web attacks, but it's not clear if business users will benefit from it any time soon.*
>
> *By using address source filtering at edge routers, ISPs could prevent large numbers of "fake" IP packets from flooding targeted sites. In the near term, filtering is the only solution to prevent denial-of-service attacks on a large scale, says John Pescatore, a research director at Gartner Group, a Stamford, Conn., consulting firm.*
>
> *While most ISPs agree filtering could nearly eliminate the assaults, they are hesitant to install the safeguard because of the heavy price and uncertainty about the longevity of the fix.*
>
> *So why aren't ISPs using filtering? The primary reason is performance will suffer, says Kelly Cooper, Internet security officer at GTE Internetworking. "Filtering at the edge of the network will take a significant amount of router processing power."* [39]

General Recommendations For Handling Cybercrises

One of the keys to effectively handling cybercrises is knowledge of what is being said about your organization on-line.

an.com&origcount=&origsub=180&origloc=main.cgi&sub=180&bum=0&maga=&reach=7540&base=story&ma=IPR

[39] Pappalardo, Denise "Avoiding Future Denial-Of-Service Attacks", CNN.com, 2-23-2000, http://www.cnn.com/2000/TECH/computing/02/23/isp.block.idg/index.html

> *One of the most important things you can do to gain insight into public perception and prevent a "cybercrisis" is to monitor the Internet on behalf of your clients.*[40]

There are a variety of resources organizations can use to monitor their image on the Internet.

> *If you do not already have an Internet monitoring strategy in place, the following provides twelve online resources that can help give you and your client a flavor for what is out there.*
>
> *1. DejaNews - Searches all Usenet newsgroups for messages dating back to 1995. DejaNews also allows you to search archives by author and retrieve useful author profiles.*
>
> *2. Alta Vista - Offers the widest array of powerful searches, including phrase searching, links retrieval, URL and domain searches.*
>
> *3. ForumOne - Archives transcripts and postings from on-line forums, such as The New York Times, Washington Post, US News & World Report, Time, People, Yahoo and Excite.*
>
> *4. The Electronic Library – Archives hundreds of magazines, newspapers, newswires and other mediums (books, photos) in full text.*
>
> *5. Edgar Online - Supplies instant access to SEC filings on public companies. Also try the Hoover's database full of detailed corporate profiles. Journalists use these resources and so should you.*

[40] Middleberg, Don "Internet Vigilance: Where to Look for What is Being Said About Your Client Online" 1-17-2000, http://www.middleberg.com/middlebergnews/bylines/vigilance.cfm?print_version=yes&

6. News Sites - Several news sites, such as The Wall Street Journal, CNN, and ABCNews.com, have proprietary search engines and extensive news archives. Make sure to monitor key chat areas linking from these sites' news stories whenever your client is in the news. These chats can be used to gauge consumer reaction and provide important audience insight.

7. Commercial Services - Message Boards and archived chat transcripts on AOL's Business News Network and Personal Finance Channel are good places to start checking out the subscription services. CompuServe's Business Management Forum provides insightful industry commentary and the Research Forum supplies volumes of corporate data.

8. FedWorld - Delivers a comprehensive inventory of information disseminated by the Federal Government.

9. Thomas - Archives federal legislative records on the Internet.

10. Business and Finance Sites - TheStreet.com, Motley Fool, and StockChat have ongoing discussions, archived postings and real-time news about investment options.

11. Web Compass - Web software that lets you develop customized client profiles and search hundreds of search engines on the Web at the same time.

12. Wise Wire - Delivers customized content from the entire Internet, learns your interests and uses readers opinions to distribute quality information.[41]

[41] Middleberg, Don "Internet Vigilance: Where to Look for What is Being Said About Your Client Online" 1-17-2000, http://www.middleberg.com/middlebergnews/bylines/vigilance.cfm?print_version=yes&

Depending on the size of their organization, public relations practitioners may wish to hire an external service external or an in-house expert to monitor the Internet.

> *That's why you need to keep an eye on what's being said about your company or client online at all times. And when something potentially damaging is said, you need to respond and if necessary, correct any mistruths. 'Companies have established home pages, online marketing tools, and intranets,' Harrower says. 'But they still haven't grasped the idea that this is a method of establishing one-on-one communications with that end consumer.'*
>
> *Lukaszewski says companies should consider hiring services such as eWatch www.ewatch.com and MarkWatch www.markwatch.com. Both monitor all newsgroups, Web sites and chats, looking for certain key words and topics. 'You can subscribe to that kind of service for a very small amount of money,' he says, estimating it to cost between $200 and $300 per month, plus per-hit charges.*[42]

These monitoring service are used by a variety of organizations, some even reselling the service to others and monitor competitors.

> *'Internet monitoring is a good way to track word of mouth or buzz,' says Gabriella Clough, senior knowledge manager at Burson-Marsteller in New York, which resells the eWatch service under the brand name QUIKeclip. 'Our clients use Internet monitoring services mostly for*

[42] "Facing an Online Crisis: Use the Internet to Detect and Squelch PR Catastrophes", Interactive Public Relations, http://www.ragan.com/html/main.cgi?sub=180&bum=0&maga=&reach=1353&base=story&ma=IPR

> *precautionary purposes--to see if something is affecting different stakeholder constituencies, for example, during a labor dispute.'*
>
> *Burson-Marsteller clients also use Internet monitoring to track what their competitors are saying on their Web sites. Using a service is an easy way to do competitive monitoring fairly quickly, rather than having to go to each Web site individually,' she says.*[43]

If a monitoring service discovers a cybercrisis, Daniel Janal of Scambusters.org offers the following tips.

> *1. Monitor the newsgroups and search engines at least once a week. Check for company names and product names. If your company is very visible, check the names of the CEO or president as well.*
>
> *2. If you find postings in newsgroups, read all the messages about the subject and determine if you need to respond. In some cases, the issue dies, or smarter minds call the poster to verify his information. This happens a lot in stock newsgroups!*
>
> *3. If you think you need to respond to set the record straight, dive right in! Newsgroup netiquette forbids advertising in newsgroups, but not the honest exchange of information. In fact, if you don't state your side of the story, people might assume that silence is assent!*
>
> *4. Contact the original poster directly and see if you can work out the problem. Maybe there was some miscommunication that went haywire. Many people are reasonable. In fact, some of the biggest fans for*

[43] "Are People Talking About You On The Internet?", Interactive Public Relations, http://www.ragan.com/html/main.cgi?sub=180&bum=0&maga=&reach=7545&base=story&ma=IPR

companies were once people who had customer service problems that were set straight. Before you call or write, see if the person posted other messages in other newsgroups. DejaNews provides links to all messages the person posted. If you read the messages, you might begin to see how you can develop rapport with that person, or if the person is whacko! One search I conducted for a client showed the e-mailer to have belonged to several hate groups! That case would require a different strategy than if he belonged to professional scientific organizations.

5. If you find a rogue Web site, see if you can talk to the Webmaster and find out what the problem is. If they (the webmaster of the rogue site) received bad customer service or bought a faulty product, take note. They probably speak for many people who have had similar problems with your company. In this case, your problem is really inside your company. If you straighten that out, the page will probably die out. If you don't, the page will live forever, like U.S. Worst, an attack page for U.S. West, a telecommunications giant. People can post their own horror stories on the site, or find out the home phone number of the chairman of the company so they can complain directly to him!

6. It is hard to threaten a rogue Web site master because they (sic) are protected by the First Amendment, which guarantees freedom of speech. However, they are subject to the same laws of libel as in the real world. So if they are spreading false information, and they know it is false, then you could bring suit against them to shut them down.

> *7. Be sure to copy the pages onto your computer and print them out on paper. This is your evidence. If you don't and they remove the offending material, you won't have any proof of the libel. Programs like WebWhacker and WebBuddy can copy entire sites, including the text, pictures and HTML.*
>
> *These tips should help protect your company - and you - from attacks on the Internet.*[44]

Don Middleberg of Middleberg and Associates offers the following general tips for handling cybercrises.

> *1. Know your Internet audience. Be aware of the newsgroups and message boards in which your customers participate. Learn the "netiquette" of online communities before joining and avoid getting flamed later.*
>
> *2. Monitor Internet news and discussion. Create an "early warning alert" system to be sure you are the first to detect misinformation instead of the last! Consider using an Internet clipping service like eWatch, or implementing a comprehensive Internet monitoring strategy.*
>
> *3. Respond to Internet rumors quickly and consistently. Inaccuracies spread like wildfire online. Ignoring them and hoping they go away will only serve to fuel the fire.*
>
> *4. Address issues locally. Make sure you respond to a rumor or inaccuracy in the medium it was introduced. If an event affects only customers in an isolated region of the country, your Web site might not be*

[44] Janal, Daniel, "How to Deal With Lies About Your Company (and You) on the Internet", 2-5-99, http://www.scambusters.org/Scambusters29.html

> *the best place to post information. Avoid calling someone who has posted in a newsgroup - consider sending an E-mail.*
>
> *5. Put online crisis procedures and policies in place before crises strike. Companies that have to scramble to learn how to communicate online when a crisis strikes cannot respond efficiently and may delay the crisis management process. Being educated and proactive can minimize damage.*
>
> *6. Think before you call in the lawyers. Corporate heavy-handedness is widely disdained on the Internet. The letter that your legal counsel might want to send could end up on the front of someone's Web page.*[45]

George McQuade of the Los Angeles Housing Authority offers these additional tips to safeguard your organization.

> *'There is a clear and present danger of becoming too dependent upon your Web site for communication with the public and employees,' McQuade says. Make sure you have other means of communication, should an emergency arrive, he advises. HACLA's 'Employee Grapevine' is a toll-free, emergency 24-hour hotline, which dials through a phone trunk center outside of California.*
>
> *McQuade offers some further tips for using technology during a crisis:*

[45] Middleberg, Don "The Internet: The New Channel On The Crisis Radar Screen" 1-16-2000, http://www.middleberg.com/middlebergnews/bylines/newchannel.cfm?print_version=yes&

** Back up your site! 'We never learned who erased it. It could have been an inside job, but the lesson learned was we had barely backed up the Web site,' McQuade says.*

** Back up all news releases on other employees' systems. HACLA PR pros send completed releases to each other via e-mail.*

** Establish a home office with necessary tools to work out of your home, such as a basic computer, printer, and fax machine.*

** The media are using the Internet more, and you'd be surprised who's up all night cruising the Internet for news stories--so don't let that crisis release wait until morning. 'Sometimes the traditional ways don't gräb the attention of assignment editors who receive more than 200 paper faxes per day,' McQuade says.*

** Arm yourself with lots of evergreen positive stories or PR events you can launch with little effort on the Internet. 'I placed more than a dozen stories on the Web site giving the agency a positive light within two weeks of the crisis,' McQuade says.*

** Learn the capabilities of the MIS department. 'MIS might have a technical solution to help you solve your crisis communication just by setting up facilities or stations and people to man them,' McQuade says.*

** Ask for help. There are a host of volunteer agencies and interns or students at the local university who would love to gain experience and help during a crisis--physical or computerwise, McQuade says. 'Help* *them on slow days and do PR for them, and you'd be surprised what happens when you need help,' he says.*

** The No. 1 rule is stay calm, 'even if you feel like you're going to have a nervous breakdown. Presentation is everything, and if you appear to be calm, the people around you will feel that way, and so will your boss. And the media will be less likely to prey,' McQuade advises.*[46]

Cybercrises are mainstream problems causing public relations societies to issue bulletins to their members with tips on how to handle them. Consider the following advice from a bulletin issued by the Public Relations Society of America.

- *Research and assess the situation.*
- *Do not ignore or underestimate the problem. It is essential to treat an Internet attack like a true media crisis. You must respond.*
- *Try to reach the source or individual who is attacking your company on the Internet and establish a dialog.*
- *Communicate your side of the story to that source with the intent of clearing up misunderstandings, misleading information or inaccuracies.*
- *Listen. If possible, try to find common ground.*
- *Be ready to respond immediately, preferably on your own Web page and to the on-line media, as well as traditional media outlets.*

Legal Issues To Consider

[46] "When your Web Site Disappears", Interactive Public Relations, http://www.ragan.com/html/main.cgi?sub=180&bum=0&maga=&reach=5723&base=story&ma=IPR

> *The nature of the Internet allows people to publish any information they want, virtually without consequence, no matter how offensive, inaccurate, or vulgar. In light of this, a careful public relations plan should be considered before taking legal action.*[47]

If a practitioner needs to post information quickly or to repair a hacked site, some public relations professionals recommend building a "Dark Site." A dark site is a fully designed web page ready to be used at a moment's notice.

> *Edelman Worldwide is working to reduce the time it takes to post a crisis Web site by building 'dark sites' for clients. The sites are filled with product or company information that would be relevant in case of a crisis. They're posted on a secure intranet until a crisis breaks--then they go 'live' without delay.*
>
> *'We create the dark sites in a password-protected kind of staging area,' says Michael Holland, senior account supervisor in Edelman's New York crisis management practice. 'For example, say the client is a pharmaceutical company in the medical device area. We would post some background about the product, some clinical studies, or the actual FDA approval. We could also get some third-party endorsements on the site. Say it was a company that produced an artificial knee; we'd have testimony from a leading orthopedist who actually uses the implants.'*
>
> *The site resides on Edelman's Internet server--but can't be accessed by anyone without a private URL and password. If a crisis hits,*

[47] Middleberg, Don "How To Avoid A Cybercrisis", Nov. 1996, http://www.prsa.org/tacfiles/novsp196.html

> *the site goes 'live' and ditches the password protection. Edelman then spreads the word about the site to relevant media and other stakeholders in the crisis, such as analysts and customers. 'We might send out a fax or an e-mail, letting the journalists or other people know about the product recall or event--and letting them know they can turn to the Web site for more information,' Holland says.*[48]

No matter how hard a public relations practitioner plans and drills for handling a cybercrisis, something unexpected may happen and do irreversible damage. To combat this, some insurance companies have started to offer insurance for online public relations disasters.

> *A new company, InsureTrust.com LLC, offers risk management services and insurance policies to meet these needs. The company claims to be the first firm that offered an Internet insurance policy, which it did in 1997. The Atlanta-based company today provides risk management services in addition to Web insurance for companies ranging in size from startups to major global firms.*
>
> *InsureTrust.com's services vary in cost depending on the size of the company and complexity of the computing system, Web site, and e-commerce systems to be protected. But prices start at about $100,000 for first-year management of insurance policies and the full range of risk assessment and planning services—which reviews the security of network operations centers, firewalls, computing security hardware and software,*

[48] "'Dark Sites' Provide Immediate, Ready-Made Crisis Communication" Interactive Public Relations, http://www.ragan.com/html/main.cgi?sub=180&bum=0&maga=&reach=7540&base=story&ma=IPR

> *and other companies to whom you might outsource certain comouter services. Subsequent-year charges can be greater or smaller, depending on the growth of the company and the change in scope of its Web and e-commerce activities.*[49]

[49] "New Service Offers Protection For Online PR Disasters" Interactive Public Relations, http://www.ragan.com/html/main.cgi?sub=180&bum=0&maga=&reach=10390&base=story&ma=IPR

CHAPTER 3

Procedures

The researcher used four sources for this thesis: 1) a search of pertinent on-line databases offered through the Rowan University Library; 2) a search through various public search engines available on the Internet; 3) an e-mail survey; 4) interviews via e-mail.

Literature Review:

Several pertinent databases offered by the Rowan University Library were the starting point for this thesis. Lexis-Nexis, WebSpirs and the Virtual Academic Library Environment of New Jersey (VALE) were searched for relative topics. The key words used for this search were "cybercrisis," "cybercrisis management," "public relations," "Internet," "crisis public relations," "online," and "hacking." This search produced more than 100 relevant articles. The library card catalog was also searched using the same key words, turning up nothing relevant.

The researcher then searched various Internet search engines including Yahoo.com, NorthernLight.com, Dogpile.com, 37.com, AltaVista.com and the online bookstore Amazon.com. Again the key words "cybercrisis," "cybercrisis management," "public relations," "Internet," "crisis public relations," "online," and "hacking" were used. The web search produced several hundred articles on the topic and three books. Individual web sites for PR practitioners and agencies were visited to obtain cybercrisis management information.

Primary Research

From the research, a non-probability e-mail survey was conducted to provide background for interviews with experts in the field of cybercrisis management. Sampling was done on a volunteer basis. An invitation was sent to four listservs that cater to the public relations community. These listservs were PRForum, PRQuorum, PRBytes, and Image Management.

After tabulating the results of the survey, a series of interview questions were sent to the ten individuals who stated that they or their organizations have handled a cybercrisis. Of those ten, only three responded. Since three was considered too small a respondent number, additional responses of individuals who have handled cybercrises were solicited from organizations through cold-calling and emails.

The results of the survey as well as the interviews appear in chapter four.

After comparing the results of the survey with the responses from the survey and literature review, the researcher compiled key concepts, information and techniques into a guide for public relations professionals to use when faced with a cybercrisis.

CHAPTER 4

Results

This chapter contains the results and knowledge gathered through a survey and a series of interviews conducted by e-mail about cybercrisis management.

The first part of the chapter contains the results of the survey, while the second half lists the responses to the interview questions by public relations practitioners who have handled cybercrises.

Survey Results

The survey was sent to 60 volunteers solicited from an email posted to various on-line public relations listservs. Of those 60, 49 responded to the original survey resulting in a return rate of 82 percent.

1.) Does your organization/practice maintain an Internet presence? (E-mail, Web Site, Monitoring service, etc.) n=49

Every single respondent to the survey stated that their organization or practice maintained some form of Internet presence.

2.) Does public relations play a role in your organization's/client's on-line presence?

n=49

Answer	# of Respondents	Percentage
Yes	47	96
No	2	4
No on-line presence	0	0

The majority of respondents stated that public relations played a role in their organization's/client's on-line presence.

3.) In your opinion, what role does Public Relations play on the Internet? n=65

Answer	# of Respondents	Percentage
Brand/Image	13	20
Media Relations	12	18.5
Public Information	9	13.8
Web Site Content	8	12.3
Crisis Management	6	9.2
Investor Relations	5	7.7
Two-Way Asymmetrical Communication	4	6.2
Two-Way Symmetrical Communication	3	4.6
Traditional Public Relations Role	2	3.1
One on One Communication	2	3.1
Networking	1	1.5

Respondents stated various roles that public relations plays on the Internet. The role that respondents stated the most was branding and imaging. The second most occurring role was media relations.

4.) On a scale of 1 – 5, how important is the Internet to your organization/clients? n=49

Rank	Number of Respondents	Percentage
5 - Very Important	23	47
4	16	32.7
3	8	16.3
2	1	2
1 - Not Important	1	2
Average = 4.2	N/A	N/A

The average ranking of importance of the Internet to respondent's clients was 4.2. This number indicates the relatively high level of importance that the Internet plays in the operations of their organization/clients.

5.) Do you or does someone else monitor Internet traffic for mentions of your organization/client? n=49

Note, one person used both an external and an internal source to monitor the net.

Answer	Number of Respondents	Percentage
You/Your Organization	29	59.2
Do Not Monitor the Internet	11	22.5
Outside Resource	9	18.4
Non-Response	1	2
Total that Monitor the Internet	38	77.6

The highest number of respondents stated that they or a member of their organization monitor Internet traffic for mentions of their organization/client. The second most numerous response was that their organization does not monitor the Internet; 77.6 percent of respondents practiced some form of Internet monitoring.

5b.) If monitored, how often do you or your outside resource monitor Internet traffic?

n=38

Answer	Number of Respondents	Percentage
Every Day	8	21.1
Once a week	6	15.8
Occasionally/No Regular Frequency	6	15.8
Once a Month	5	13.2
Twice a week	5	13.2
More than once a day	3	7.9
Twice a month	2	5.3
Non-Response	2	5.3

The largest percentage of those who monitor the Internet stated that they do so every day. However, the number of individuals who monitor the Internet once a week tied with those who don't follow any set-monitoring schedule.

6.) Have you or your organization ever handled an image crisis on the Internet? n=49

Answer	Number of Respondents	Percentage
No	39	79.6
Yes	10	20.4

About a fifth (20.4 percent) of respondents stated that they or their organization have handled an image crisis on the Internet.

6b.) If yes, how severe was the potential to damage your organization/client's reputation?

n=10

Rank	Number of Respondents	Percentage
1 – Little Damage Potential	1	10
2	0	0
3	4	40
4	1	10
5 – High Damage Potential	3	30
Non-Response	1	10
Average Rank = 3.5	N/A	N/A

The average rank of potential damage to the organization/clients that respondents represent was 3.5. The highest number of respondents stated that the potential damage was a 3, while the second highest stated that the potential damage was a 5, High.

7.) Have you ever prepared an Internet related crisis management plan? n=49

Answer	# of Respondents	Percentage
No	39	79.6
Yes	9	18.4
Non-Response	1	2%

About four fifths (79.6 percent) of respondents stated that they have not prepared an Internet related crisis management program.

8.) Place an X in place of the line next to the three most potentially damaging cybercrises.

Most Dangerous by # who thought they were the most damaging. n=136

Type of Cybercrisis	**Number of Respondents**	**Percentage**
Damaging news story posted by reputable Web site	35	26
Web site hijacking/hacking	32	24
False information spread via e-mail	22	16
False information spread via message board	15	11
Rogue/activist web site	12	8
Chat group flaming	5	4
Mass flame e-mailing	5	4
False information spread via Usenet	4	3
Usenet flaming	3	2
Message board flaming	2	1
Write in- Complete web presence breakdown	1	1

The cybercrisis that was considered to do the most potential damage was "Damaging news story posted by reputable Web site." The second most damaging was considered to be "Web site Hijacking/hacking." The third most damaging was False information spread via e-mail. Rogue/activist Web sites ranked 5th, despite the amount of attention paid to them by cybercrisis experts in the press.

9.) In your opinion, what is the most vital component in any on-line crisis management plan? n=62

non-response = 3, not included in n.

Answer	**# of Respondents**	**Percentage**
Ability to respond quickly	18	29
Monitoring the net	11	17.7
Anticipating Crises before they happen	7	11.3
Pre-approved content/Dark Sites	6	9.7
Establishment of authority/responsibility	4	6.5
Understanding of the Internet	4	6.5
Security	3	4.8
Traditional Crisis Management	2	3.3
Feedback from users	2	3.3
Establishment of Confidence	1	1.6
Trustworthiness	1	1.6
Easy access for authorized spokespeople	1	1.6
Constant communication of facts	1	1.6
Competent tech support	1	1.6

Respondents stated that the most important component in any on-line crisis management plan was the ability to respond quickly to these challenges. The second most important component was monitoring the Internet.

Interview Results

The interview was emailed to ten individuals who responded in the survey that they or their organization have handled a cybercrisis. After a series of several reminders, five responses were received. However, several responses were incomplete. Therefore a series of cold-calls and emails were made to various organizations that have handled cybercrises.

Practitioners were asked a series of questions about the specific situation they or their organization has handled. Answers ranged from short paragraphs to lengthy statements

Due to the sensitive nature of potential answers to these questions, confidentiality had to be promised. Therefore, respondents have been given a letter designation.

Question 1)

Briefly, describe the cybercrisis or cybercrises that you or your organization have faced in general terms.

Respondent A.)

Confidential situation. Client's product was being slammed via chat rooms, web site.

Respondent B.)

A possible breach in security/access to listserv by an outside source.

Respondent C.)

It may not fall into the category of crisis, but we are asked about Internet-spread health rumors all the time.

Respondent D.)

Y2K and the "love bug" virus.

Respondent E.)

(Removed to preserve confidentiality) as an entity and some of the officers have been the target of much derision on a Yahoo message board. Some messages have included personal attacks on current employees by name. These comments included questioning professional judgment, presupposing personal vendettas and questions of sexual orientation.

Respondent F.)

Problem was an online bill pay vendor who had not updated its' e-Commerce process for Y2K. Customers who used the online bill service and downloaded account files encountered date problems that put checks out of sequence.

Question 2)

What do you feel was the key component that contributed to handling this/these crises?

Respondent A.) Responsiveness and willingness of client to take action. Was able to show the allegations were false; still had some emotional baggage to deal with.

Respondent B.) Immediate action. Immediate response to media queries.

Respondent C.) The nature of this scenario is that it is spread through e-mail and as such, it never goes away. One such Internet rumor has been going around at least two or three years. Although no reputable body has ever given it credence, we and other companies are still asked about it both through consumer calls and the mainstream media.

The key to handling these has been to engage the FDA, as an independent outside body, to take a stand and relay the facts.

Respondent D.) Y2K: Preparation, anticipating possible problems and developing solutions, making sure the bank was up-to-date/compatible from a technology perspective (computers, servers).

Love Bug: The fact that our Information Systems department was aware of the situation and communicated globally via e-mail about the warning, its effects and preventive remedies on how not to be a victim.

Respondent E.)

We had to put the impact of the message board in perspective. As a medium, it serves and is fed by employees let go post-acquisition and short-term investors looking to make a quick dollar on (Confidential) stock. (Confidential) is an aggressive bank that is growing through acquisition, which results in the elimination of some jobs. (Confidential) also is a stock that, as were other financial stocks in the past years, flying high before financials fell out of favor on Wall Street. Some investors are holding (Confidential) stock at 1998 prices; others are looking for the types of returns that came from mergers and acquisitions.

It's generally felt that some current employees contribute anonymously, and the chairman has chided us for that. But generally, we're considering the comments on the Yahoo message board an electronic form of graffiti and are ignoring it.

Respondent F.)

(Confidential) was persistent in contacting the highest level executives at the vendor, urging them to remediate the situation immediately. There were three, three hour conference calls with nine representatives from both companies including business and technical Internet managers. A remediation procedure and schedule were developed.

Question 3)

What would you or your organization do differently if the situation/situations were to happen again?

Respondent A.)

We need to be able to better monitor the Internet all the time, 24x7, to see what's going on that might concern our clients, to alert our clients, and to be able to propose appropriate strategies.

Respondent B.)

Streamline the approval chain for release of information.

Respondent C.)

Because this has been a repeated occurrence, we've gathered more and more information each time it has come up. Other companies are engaging outside experts to serve as spokespeople. We've chosen to gather facts provided by reputable outside groups and send people there for comment. They wouldn't believe us, but it may mean more coming from a health group outside the industry.

Respondent D.)

Nothing. The crisis management process works, as long as it is communicated to employees in an expedient manner.

Respondent E.)

I think our response was appropriate. Given the anonymous nature of the message board, I'm not sure what we could have done that wouldn't have fanned the flames of discontent further.

Respondent F.)

Vendor claimed to be Y2K ready. Perhaps pre-Y2K testing of the vendors' products and services could have performed.

Question 4)

What was the biggest obstacle you or your organization had to overcome in handling the situation/s?

Respondent A.)

Finding out about the problem in time to do something before it is totally out of hand was the biggest obstacle. Another was a lack of in-depth expertise among current staff, which is more traditionally oriented.

Respondent B.)

Coming to a consensus on a response, and exact steps for taking action.

Respondent C.)

There have been two large obstacles. One, since it is spread by e-mail, everyone who receives it assumes it is new. Two, no one believes the industry.

Respondent D.)

N/A

Respondent E.)

Getting executives caught up on this specific message board and chat in general was clouded by the perceived immediacy of the problem. Web in general and chat specifically, are not technologies or media that they're familiar with.

Respondent F.)

Vendor's senior managers were not immediately available which delayed response. In addition, when contacted, they tried to transfer the responsibility to yet another vendor.

Question 5)

Is there any further information that you think would be of help to someone encountering a cybercrisis?

Respondent A.)

If you are an agency or major company, you need to have a few employees, at least, who "live" on the web, who know how to get around, stay ahead of the knowledge curve, and who can translate that into effective counsel for clients.

Respondent B.)

Have an action plan on hand covering this potential!

Respondent C.)

The nature of the crisis can be very different. Some come from one identifiable source, like a specific web site. The e-mail variety is much harder to identify because it comes from many different sources and people pass it on to everyone they know. It's also difficult to judge how much weight to give to the issue until possibly many months later.

This type of issue, if it is not based on fact, can only be as important as the number of people who see it and believe it. That is very difficult to measure.

Respondent D.)

Expedient communication through the proper channel is key (e.g., global e-mail, audix messages, etc.).

Respondent E.)

I think it's important to take stock of a crisis and measure it before determining a course of action. We had several proposals on the table, from writing to Yahoo and posting the letter to flooding the board with messages in order to push the nasty ones out of the database. One can understand where those ideas come from. Once we took stock of the quality of the content and the reach of the medium, we could determine there was little impact from the comments.

Respondent F.)

Expedient communication through the proper channel is key (e.g., conference calls, global e-mail, audix messages, etc.) and keeping a current list of vendor contacts.

Rather than label the problem a Y2K issue, the vendor posted a message via its online Internet link that an update was being made to the current system for more efficient performance, to avoid alarming or panicking customers.

Chapter 5

Conclusions

After analyzing previously published information, conducting a survey and several e-mail interviews, this researcher has come to a variety of conclusions about cybercrisis management.

The Importance of Public Relations on the Internet

The primary conclusion of this researcher is that public relations plays a large role on the Internet that will only grow as time passes. Every single respondent to the survey worked for a client or organization that had an on-line presence. Public relations plays an important role in this on-line presence as evidenced by the fact that 96 percent of respondents stated that public relations plays a role in that presence. Additionally respondents ranked that Internet presence as very important to their organization or client.

The role that public relations plays in that presence is varied. However, most stated that public relations is mainly involved in branding and imaging, media relations, public information and web site content. This echoes the predictions of public relations professionals in the review of literature conducted by this researcher.

The Percentage of Practitioners/Organizations Facing Cybercrises

The growth of the Internet and its importance to the operations of organizations also increase an organization's susceptibility to a cybercrisis. Twenty percent of respondents stated that they or their organization have faced a cybercrisis that could do moderate to high damage to their organization. This may not seem like a large number, but considering that the Internet has only been an accepted mainstream media for the past three years, this is a large number. The number of organizations that face a cybercrisis can only grow as more and more organizations and individuals enter cyberspace.

Of those interviewed who had faced a cybercrisis, the types of cybercrises varied. There was one instance each of a Rogue Web site and flaming in chat rooms, four cases of "Web site emergencies/hacking, one case of false rumors spread via the Internet, and finally one case of message board flaming.

Damage Potentials of Selected Cybercrises

The cybercrisis that was ranked as doing the most potential damage by respondents was a "Damaging news story posted by reputable Web site." This is an extension of a traditional type of crisis that public relations professionals potentially face offline. This type of crisis often snowballs and is quickly picked up by traditional media. Due to its potential size and range, this researcher feels that it is beyond the scope of this research project to fully explore it.

The second most potentially damaging cybercrisis was having an organization's Web site hijacked, hacked or damaged in some way. This is a relatively new subject brought to light in the past few months. As such, very few experts in the field have written about the subject. More attention needs to be paid to this subject by public relations professionals.

False information spread over the Internet, through both e-mail and message boards, was considered a large threat and should be taken seriously by public relations practitioners. Surprisingly, Rogue/Activist Web sites, the subject of the most attention of experts in the field, were ranked as having only a moderate damage level by those surveyed.

Preparedness of Organizations

Despite the potential for the growth of cybercrises and their high damage potential, very few individuals have ever prepared an Internet related crisis program. The fact that only 18 percent of surveyed individuals have prepared a plan shows that many organizations are either unaware, unconcerned or not taking cybercrises seriously despite experts' recommendations.

One good thing that organizations are doing that experts recommend is monitoring the Internet. Seventy eight percent of those surveyed stated that the organization or client they represent monitors Internet traffic to determine what their image is and discover potential problems.

The majority of those who monitor the web do so every day; however the separation of ranks was very broad and there doesn't seem to be a real commonality on the rate at which monitoring is done.

Respondents stated that the most vital component in any plan to handle a cybercrisis is the ability to respond quickly. This is important, because as reflected in the literature review, cybercrises start quickly and spread quickly. Public relations professionals need to respond quickly to them to contain their damage.

The second most important component is monitoring the Internet. This reflects what was revealed in the literature review and is a vital component in ensuring that PR practitioners are able to respond quickly.

Another important aspect of an online crisis management plan is anticipating crises before they happen. Planning for crises before they happen is a traditional crisis management technique and should be part of every crisis plan. The next important aspect goes hand in hand with this.

Dark Sites were ranked fourth on the list and are an extension of planning for crises before they happen. By taking the time to prepare response and position pages as well as backing up their site, practitioners are able to react to crises much faster than if they had to write all the content or rebuild the site from scratch.

Recommendations of Experienced Practitioners

Those interviewed who handled cybercrises gave various key components to handling the situations they faced. Four of the interviewees stated that they felt that the ability to act quickly was an important factor in handling the cases they faced. The second factor most often stated by interviewees was anticipating crises and planning for them in the prodromal stage. One individual suggested that the key to handling a cybercrisis was to look at each instance separately and determine the best course of action or inaction. Another interviewee recommended using outside organizations to lend credibility to your message.

Those interviewed gave a variety of things that they would do differently if the cybercrisis would occur again. One respondent reinforced the need to monitor the Internet by stating that he or she would monitor it around the clock. Another respondent stated that planning for the event along with running drills would help them prepare for the situation if it were to pop up again. An additional respondent said that they would streamline the approval process so they can act sooner in the case of a recurrence. Two individuals felt that they handled the situation as well as they could have.

The obstacles faced by interviewees were varied. One individual stated that learning about the problem in a timely manner was an obstacle combined with a lack of expertise among the organization's staff. This echoes the importance that monitoring Internet traffic plays in cybercrisis management. Another obstacle stated was coming to a consensus and coming up with exact steps for taking action. Another stated that they were unable to get in touch with those responsible for the technology involved. Having a plan prepared for crises like these would have aided them in reacting faster to the situation. Another obstacle pointed out a specific problem posed by false information spread by e-mail. The respondent stated that messages received via e-mail are automatically considered brand new, even if they have been circling the Web for years. Another obstacle reported was the way that their executives responded directly to false information posted about themselves without heeding netiquette and lending credibility to their attackers. This shows that before you act, you need to be familiar with the specific cyberculture relating to the problem.

The experts interviewed offered the following suggestions to those who handle cybercrises. The first respondent suggested that you need to be, or have on staff, someone who knows the Internet and its culture well. You need to "live" on the Web to fully understand it. Another respondent stated that organizations should take cybercrises into account when creating crisis management plans, possibly creating individual ones for those that are recurring. Two individuals stated that you need to look at each occurrence individually to determine your course of action, that each cybercrisis has individual characteristics. One individual went on to state that false information spread via e-mail is worse than a rogue Web site because you don't know who is responsible for spreading the rumor. Two individuals stated that expedient communication through the proper channels is important to handling cybercrises.

Tying It All Together

Cybercrisis management is a growing function of the public relations industry. While every case is different, some specifics can be generalized to all cases. One, traditional crisis management skills are the bread and butter of cybercrisis management. Without traditional understanding of crisis management technique, cybercrisis management cannot be done. Two, Having the ability to respond quickly to the situation is necessary due to the speed at which information spreads on the Internet. Three, monitoring the Internet is necessary to manage your organization's image and learn about situations quickly to contain the damage that they may do. Fourth, having a crisis management plan that takes into account the Internet and cybercrises is necessary in today's business world. Finally, public relations practitioners need to understand the Internet, its subcultures and netiquette to properly perform their duties on-line.

Recommendations for Further Research

This researcher feels that this field is in its infancy and much more research needs to be done before the knowledge can be considered mature.

This researcher noticed a dearth of case studies on cybercrises other than rogue Web sites. Therefore, this researcher recommends picking a type of cybercrisis other than a rogue Web site and conducting a case study on it. Vitally needed are case studies on the public relation ramifications of Web site hacking and other emergencies.

Another point of interest would be to pick an organization and monitor the Internet for references to that organization over a period of time. The researcher should then chart the trends that emerge and profile the on-line image of the organization.

For additional study, this researcher recommends conducting a study on a particular type of cybercrises. The researcher should contact individuals on both sides of the crisis, and interview them about why they launched the attacks and how they handled them to compile a guide for handling each individual type of cybercrisis.

Finally, this researcher feels that the quantitative and qualitative sections of this study should be repeated in three years to determine how involved the public relations community is involved in the on-line world.

Chapter 6

A Guide to Cybercrisis Management

Introduction

Cybercrisis management are buzzwords that are popular in the public relations industry these days. There is no real consensus on what the term actually defines. Some take it to mean handling crises through the Internet, while some take it to mean a crisis specific to, or starting on the Internet. For the purpose of this guide, the latter definition is what is meant by cybercrisis.

There are many types of cybercrises. In fact, a cybercrisis you face may fall into many different categories. There is no one solution and you should look at every case individually. What may be vital to act upon in one case, may be best served by ignoring in another.

Cybercrisis management is in its infancy. Very little is known about the form and function of how they work and how they effect an organization's image. This guide is not meant to be the definitive guide to cybercrisis management. Rather it should be used as a reference to generate ideas to handle crises and lessen the damage that they do. Additionally, due to the nature of the Internet, some of the information contained in this guide may be out of date by the time you read it.

Quite a bit of information in this guide is taken from sources already used in this thesis due to the small number of writings and information on the subject.

The Role of Traditional Crisis Management

The first thing you have to have to handle a cybercrisis is an understanding of traditional crisis management. Without this understanding, there is no way to handle a cybercrisis successfully.

There are scores of books on handling crises. If you do not know the basics of crisis management, read no further. Put this guide down and read about traditional crisis management techniques before you go any further. Without this background you will be unable to handle a cybercrisis.

This guide does not contain traditional crisis management techniques. If this guide were to discuss traditional crisis management, there would be very little room left for cybercrises.

If you do have an understanding of traditional crisis management, continue reading. I hope that the information contained in these pages will help you out of any tight spot you are in.

Monitoring the Internet

Professionally, almost every organization that employs public relations uses a clipping service of some type. These clips are used for many different purposes. They are routinely used to gauge the success of the public relations program and to determine the image that the media is promoting about the organization. Despite the acceptance of clipping services, very few organizations monitor the Internet as rigorously as they do traditional media.

This is a mistake.

The Internet needs to be monitored with just as much scrutiny as other forms of traditional media. This is due to the speed at which information travels on the Internet. Literally, a news story posted to the Internet can travel around the world in seconds. In fact, many of the biggest scandals that have filled the airwaves lately were born on the Internet. If you need proof, just ask cigar aficionado Bill Clinton about the power of the Internet.

Monitoring the Internet is a very boring and tedious job. It is also time consuming. There are really only two ways to do it right, one hire a full time staff member to monitor the Internet. Or two, hire an Internet monitoring service. I'd suggest doing the latter because it is more cost efficient and is more likely to produce results.

Internet monitoring services have begun to appear all over the place. They all vary in the exact services they provide and in cost. Additionally, some traditional clipping services such a Burrelle's have added Internet monitoring to their list of services. Some of the more recommended Internet monitoring services are:

- eWatch- http://www.ewatch.com
- CyberScan- http://www.clippingservice.com
- Burrelle's- http://www.burrelles.com/
- CyberAlert- http://www.cyberalert.com/
- Webclipping.com- http://www.webclipping.com/

Additional clipping services can be found by entering any Internet search engine and doing a search for "clipping services."

Netiquette

The culture of the Internet varies greatly. The Internet is not only international, but was an underground medium for a long time before the commercial world caught on to its potential. Many of the people who became attracted to it would be considered to have views that deviate from cultural norms. These people are now the gatekeepers of the flow of information on the Internet. You have to be careful what you say and do. If something you do makes the wrong person angry, no matter how well protected you think your site is, chances are good that it will be damaged by an attack.

The Internet's culture is anti-big business and celebrates the individual. You have to be very careful when responding to a Cybercrisis because some actions may be viewed as "picking on the little guy" and give more credibility to the cause of your problem.

This works both ways. If an individual causing your organization trouble breaches "netiquette," his or her actions will be undermined by a wave of negative responses.

Netiquette varies from place to place. Message boards, e-mail, discussion groups, IRC, and other things all have specific behaviors that are expected. These are miniature communities and every one is different.

In a case where you are unfamiliar with the etiquette associated with something, try to find the FAQ (a list of Frequently Asked Questions) and lurk; read a few days worth of postings or messages, before you act.

Rogue Web Sites

Rogue Web sites have received more attention by the public relations industry than any other type of cybercrisis. This is with good reason.

The nature of the Internet allows people to create their own Web site that can reach thousands for little to no cost. These Web sites can be anything from a page about themselves, a "fan site" that relates to a person, place or thing they like, or a more sinister "attack site" that lashes out at someone or something. Often, an individual's site contains a little bit from each.

Cybercrisis management guru Shel Holtz describes "Rogue Web Sites" as unofficial sites that address a company, product or entity owned by another group. Rogue Web sites are further subdivided into "fan sites" and "attack sites."

Fan sites should be left alone unless they use copyrighted material, represent the object in a misleading way and or damage the ability of the property's owner to earn a profit from it. In fact, fan sites can be a positive thing and can actually help promote the subject of the site. Some industries, particularly the electronic gaming industry, actively support fan sites, providing them with graphics and content. In fact, some fan sites have been bought by organizations and turned into official sites.

For more tips on fan sites, see pages 11-14 of this thesis.

Attack sites are another matter. Instead of being a celebration of something, attack sites seek to damage their target. Attack sites are created by a variety of individuals for a variety of reasons. Anyone from an irate customer to an activist group can launch an attack site.

The first response most organizations have when facing an attack site is to call in the lawyers. This is a mistake. An organization cannot win a case in court because someone says something negative about it. Most attack sites are protected by the first amendment. McDonald's failed to realize this and lost multiple millions of dollars in a futile attempt to shut one rogue Web site down.

In fact, calling in the lawyers to deal with almost any cybercrisis can be a mistake, since it draws unwanted attention to the crisis at hand and gives the appearance of the "Big Guy" picking on the "Little Guy."

The best way to deal with an attack site is to e-mail the creator of the site and attempt to resolve the situation directly. Don't go in with your guns blazing; try to resolve the situation peacefully first. Often, the attack site could be the result of a mistake or misunderstanding. For sample e-mails, see pages 16-18.

If faced with a Rogue Web site, the following tips suggested by Holtz may help.

- Examine the damage potential of the site before you decide on a response
- E-mail the author to find out why he or she launched the attack.
- Attempt to resolve the differences
- Post your side of the story and address all issues on your organization's Web site.
- Provide the author with material that more accurately reflects your organization's side of the story.
- If all other avenues fail, it may be time to call in the lawyers. Before you do so, gauge the amount of damage the site is doing against the damage that could result from a lawsuit.

For more information on Rogue Web sites, see pages 11-20 of this thesis.

Instant Activists

The fact that Rogue Web sites are so prevalent on the Internet is the result of individuals called "instant activists." Instant activists are individuals who before the Internet didn't have the means to lash out against an organization. Now, with the advent of the Internet, these individuals can reach thousands, if not millions with their negative messages.

Their attacks are not limited to attack sites. In fact, these activists often coordinate attacks through e-mail, Usenet, message boards, discussion groups, mailing lists and IRC with their attack site.

When faced with a coordinated attack by an instant activist(s), the best course of action is to contact the activist and attempt to work out a peaceful solution.

For more information on Instant activists, see pages 20 through 23 of this thesis.

Discussion Forum Attacks

Discussion forum attacks are attacks that can be part of a coordinated effort by an instant activist, but more often than not are perpetrated by disgruntled customers. Although discussion forums are typically taken to mean a type of bulletin board, the specifics of handling them can be applied to Usenet, other bulletin boards, listservs, and any other piece of internet technology that allows for messages to be posted publicly and read by numerous individuals.

Shel Holtz offers the following suggestions for handling discussion forums.

- Assess the potential damage the post can cause. Often the post will be recognized as "the rant of a kook" and disregarded. Sometimes, the post will have been a breach of netiquette and will be slammed with negativity. Even if these two best case scenarios happen, there will still be individuals who will give the posting credibility and will take up its cause. Therefore, you should evaluate each message according to its content, the number of responses the article generates and the tone of the responses.

- Determine who you should respond to. You need to decide if you should respond to the individual or the whole group. If you catch the offensive message early on, or if it is the result of a mistake, it's best to contact the original poster. Often clarifying the situation privately will allow the individual to save face and reverse his or her position by issuing a retraction statement. However, if handling it privately fails, or the topic has been a major topic of discussion in the group it is best to address the entire group. Holtz goes on to suggest that you keep the contact virtual. Use the internet to contact the individual; don't attempt to call on the phone.
- Read the FAQs (Frequently Asked Questions) and "Lurk" before posting. As discussed in the section on netiquette, do a little research before you post. In public relations it is important to research your audience to craft messages for them. This is the same. Reading the FAQs and "lurking" will allow you to decide how best to address the group. Failure to do this and jumping blindly into the fray can have disastrous repercussions.
- Don't Preach; Participate. Don't expect the members of a discussion group to honor whatever position you play in the organization that you represent. You are not an authority figure; you are at best an equal, and at worst a corporate flunky attacking one of their own. Don't attempt to plant false messages that support your organization under an assumed name. This is false advertising and you will get caught.

For more information on discussion group attacks, see pages 24 - 27

Dissemination of False Information

Almost everyone who has an e-mail account has received one piece of e-mail asking that it be forwarded it to several of their friends. While the majority of these e-mails do little more than annoy the recipient, some have a more sinister purpose. Substantial quantities of these e-mails are written with the sole purpose of damaging the reputation of a person or organization.

Often, these rumors wind up being posted on a discussion board, listserv, message board and occasionally brought up in IRC. These messages spreading false information are virulent and spread like the plague. They often hide their true nature behind an altruistic facade. The fact that they appear to originate from an altruistic source combined with people forwarding them to their friends and loved ones gives them perceived credibility. The fact that they are also constantly being forwarded causes people to perceive them as new. These two factors combined make these messages a nasty piece of work.

Handling Dissemination of False Information

The best way to handle false information disseminated by the Internet is through the Internet and through traditional media channels such as television and print.

1. Never attempt to fire back with an e-mail asking people to forward it to their friends. This is a severe breach of netiquette.
2. Post a section on your organization's Web site that addresses the rumors and has signed letters and testimonials from third parties that refute the rumor. Include a

FAQ, (Frequently Asked Questions list) that addresses the specifics of each allegation.

3. If your organization has intermediaries that are responsible for disseminating your product to customers (such as doctors, pharmacists, retail representatives) send them a letter explaining the situation and asking for their cooperation in dealing with this problem.
4. Launch an aggressive television and or print ad campaign to address the rumors.

For more information on dissemination of false information, see pages 27-33 in this thesis.

On-line Trademark Violation

On-line trademark violations can range from illegal reproduction of copyrighted material on unofficial sites to "Cybersquatting." Cybersquatting is generally run into by businesses as they are about to take their first steps on the Web. Often when these organizations try to register their company name as their domain name, they find that someone already owns their name and wants to charge them an outrageous price for that domain name.

Occasionally, someone will set up a site with an address that's close to or a derivative of the name of a well-known company or organization in an attempt to steal traffic from that site. These are usually common misspellings and or abbreviations.

Another form of on-line trademark violation is the republishing of copyrighted material. If you find that someone is either cybersquatting or republishing materials your organization owns, you must act. If you fail to act, it is possible to lose control over the intellectual properties you own.

These are the only cybercrises where it is advisable to seek legal counsel and if resistance is strong enough, go to court.

In June 2000 there was no copyright and trademark law specific to the Internet. Because of that, traditional copyright and trademark law is applied to the Internet. However, this may change in the near future as there are several bills gathering support in Washington.

Handling On-Line Trademark Violations

The most important aspect of handling both types of on-line trademark violations is monitoring the Internet. You need to find these cybercrises as soon as possible. The longer you let them lie, the harder they will be to defeat in court. See the section on Internet monitoring for more information.

The following procedure should provide you with a framework to handle on-line trademark violations.

Cybersquatting:

- Send the owner of the offending site an e-mail or letter explaining that they are violating your trademark. Offer to purchase the site for a reduced sum.
- If the owner of the domain name doesn't accept your offer, have your organization's lawyers contact the owner and threaten him or her with a lawsuit. Follow this up with an offer to purchase the domain name at a slightly higher price.
- If the squatter refuses, weigh the cost of taking the offending party to court against the asking price. If it is less expensive to pay the asking price, pay it. If not, let your lawyers handle the situation.

Content Republishing:

- Send a warning to the individual who is republishing your copyrighted materials, noting that the publishing is in violation of your organization's content sharing options. Make sure to inform them about specific terms of permission and terms of compliance with your organization's policies.
- Send a cease and desist letter.
- If that fails, let the lawyers handle it.

For more information on on-line trademark violations see pages 33-36 of this thesis.

Web Site Emergencies

Web site emergencies cover a broad range of crises that impact the performance and operation of your organization's Web site. It is important to keep your site up and operating successfully because it is your organization's face on the Net.

One of the most important aspects of this is to develop a good relationship with the person or persons responsible for maintaining your site. You want them to inform you instantly about anything that affects your site's performance and security. You need to have them inform you of any operational measures and make sure that they keep up on the latest security trends to keep your site safe.

No mater what you do to prepare, something will eventually happen. Your Web site will be hacked and you will experience trouble with the equipment that powers it. Unfortunately, there isn't much you can do to prevent Web site emergencies because of the rate at which technology changes. The rate technology changes on the Internet often forces companies to release products without fully testing them, producing bugs, security holes and other disasters waiting to happen. Because of this, you should always have a backup.

Routinely backup your Web site to a separate system and server if possible. Try to do this every day if possible. Make sure that the server cannot be reached from the Internet, but can "go live" if need be.

Keeping Your Web Site Up And Running

As a public relations professional you don't need to know all of the specific technical details to keep your site up and running, but there are a few things that you should be sure your organization routinely does.

- Back up your Web site - This is the most important thing you must do. Make sure this is done every time something is changed.
- Make sure all your equipment is routinely maintained and is running the most current drivers available.
- Make sure the software that drives your web presence is up to date and has all patches and service packs installed.
- Always have the people responsible for the Web site report to you when they make changes.
- Finally, personally check your Web site several times a day. If you have trouble, try to reload it two or three times immediately. If the site doesn't come up, something is wrong. Contact those responsible for the site immediately.

Keeping Your Site Secure

Chances are, your site will be hacked or attacked by someone. There are no foolproof defenses on the Internet, and the most secure programs and firewalls always have a weakness. Making sure your software is as up to date as it can be is the best defense.

- Think like a Hacker, or hire one. The best computer security specialists are hackers. They know how to safeguard a system from break-ins and know how to search for and find loopholes. In short, fight fire with fire.
- Keep up to date on goings on in the hacker world. Check Web sites like:

  http://www.2600.com/

  http://fullcoverage.yahoo.com/Full_Coverage/Tech/Hackers_and_Crackers/

  http://www.hackernews.com/

  http://www.microsoft.com/security/default.asp

  These sites will keep you up to date on the latest, techniques, holes, tools and strategies hackers use.
- No password is uncrackable. Use passwords that are composed of random digits and numbers, preferably at least seven digits long and case sensitive. For example: G3rJ03K0f. The time to crack a password like this can be several hours, compared to several minutes with simpler ones.
- Keep all your software up-to-date. Don't skimp on purchasing upgrades.
- Always backup your site. If possible, have an alternate server on a different network that can go live and replace the hacked or attacked site in a few minutes.

What To Do When Everything Fails

If your site goes down, and it will, the best thing you can do is to fix the problems and get the site up and running again. While the site is down, try to put up a page that says "We are sorry for the inconvenience. Please bear with us while we upgrade our servers." This way, you make the situation seem like it was planned and not the result of an attack or system failure. This is ethical, because while you are fixing the damage, you actually are upgrading the system.

For more information on web site emergencies, see pages 36-42 of this thesis.

General Recommendations For Handling Cybercrises

This section contains general tips and techniques for handling cybercrises.

1. Monitor the Web- This is the most important thing you can do. Try to hire an outside service to do this for you. Unless you can afford specific software, personnel and equipment to do this, hiring an outside resource is more cost effective and will have better results.
2. Know your audience- Have someone on staff that sleeps, eats and breathes the Internet. Cyberculture is very particular and members of on-line groups can easily spot an outsider. When in doubt "lurk" and read the (FAQs).
3. Plan - develop a crisis plan that encompasses all types of cybercrises you have faced, or potentially will face.
4. Create "Dark Sites"- create pre-approved content on a secure server that is ready to go live at a moment's notice. Dark sites should contain information about procedures, evergreens, policies, potential corporate embarrassments, and most importantly, an up to date backup of your Web site.
5. Keep Contact Virtual- it is a breach of netiquette to contact individuals through non-internet channels if the problem is on the Internet. Use the channels they use.

6. Set up procedures to streamline the approval process. In most cybercrises you only have minutes to act. Make sure that you can act in that precious time and not need to take several hours to go through the "proper channels."
7. Develop a good relationship with your MIS department. Make sure you are on good terms with them and that they feel free to talk to you and keep you up to date on what is going on.
8. Call in the lawyers only as the last resort. Calling in the lawyers can increase media coverage that a cybercrisis receives, harming your reputation further.
9. If all else fails, have insurance. Companies are starting to offer Insurance policies to protect against certain types of cybercrises. This is an especially good idea if you represent an e-commerce site.

For more general tips on cybercrisis management, see pages 42-54 of this thesis.

Appendix A

Bibliography

"Are People Talking About You On The Internet?", Interactive Public Relations, http://www.ragan.com/html/main.cgi?sub=180&bum=0&maga=&reach=7545&base=story&ma=IPR

"Avoiding Future Denial-of-service attacks", CNN.com, 2-2-2000, Http://www.cnn.com/2000/TECH/computing/02/23/isp.block.idg/index.html

Basso, Joseph, "How Public Relations Professionals are Managing the Potential for Sabotage, Rumors, and Misinformation Disseminated Via the Internet by Computer Hackers"
IEEE Transactions on Professional Communication, Vol. 40, No. 1 March 1997 p. 28-33

"Classic Hackers Decry Heavy-Handed Upstarts", CNN.com, 2-9-2000, Http://www.cnn.com/2000/TECH/computing/02/09/hackers29.a.tm/

Control the Rogues, Interactive Public Relations, http://www.ragan.com/html/main.cgi?sub=180&bum=0&Maga=&reach=8561&base=story&ma=IPR

Coombs, Timothy W., "The Internet as Potential Equalizer: New Leverage for Confronting Social Irresponsibility" Public Relations Review, Vol. 24, No. 3, p.289-303

"'Dark Sites' Provide Immediate, Ready-Made Crisis Communication" Interactive Public Relations, http://www.ragan.com/html/main.cgi?sub=180&bum=0&maga=&reach=7540&base=story&ma=IPR

"Facing an Online Crisis: Use the Internet to Detect and Squelch PR Catastrophes", Interactive Public Relations, http://www.ragan.com/html/main.cgi?sub=180&bum=0&maga=&reach=1353&base=story&ma=IPR

Holtz, Shel, Public Relations on the Net (New York, New York: AMACOM, 1998)

"How to Take the Teeth Out of an Online Rumor" Interactive Public Relations, http//:www.ragan.com/html/main.cgi?sub=180&bum=0&maga=&reach=14789&base=story&ma=IPR

Janal, Daniel, "How to Deal With Lies About Your Company (and You) on the Internet", 2-5-99, http://www.scambusters.org/Scambusters29.html

Middleberg, Don "How To Avoid A Cybercrisis", Nov. 1996, http://www.prsa.org/tacfiles/novsp196.html

Middleberg, Don "Internet Vigilance: Where to Look for What is Being Said About Your Client Online" 1-17-2000, http://www.middleberg.com/middlebergnews/bylines/vigilance.cfm?print_version=yes&

Middleberg, Don, Rogue Web Sites Pose Threat To Corporate Image, Tactics November 1996 Issue Highlights Special Report: Winning On The Web, http://www.prsa.org/tacfiles/novsp196.html

"New Service Offers Protection For Online PR Disasters" Interactive Public Relations, http://www.ragan.com/html/main.cgi?sub=180&bum=0&maga=&reach=10390&base=story&ma=IPR

Middleberg, Don "The Internet: The New Channel On The Crisis Radar Screen" 1-16-2000, http://www.middleberg.com/middlebergnews/bylines/newchannel.cfm?print_version=yes&

Moore, Edward H, National School Public Relations Association 46th Annual Seminar, Baltimore, Maryland. July 20, 1999

Pappalardo, Denise "Avoiding Future Denial-Of-Service Attacks", CNN.com, 2-23-2000, http://www.cnn.com/2000/TECH/computing/02/23/isp.block.idg/index.html

"Rebuffed Internet Extortionist Posts Stolen Credit Card Data", CNN.com. 1-10-2000, Http://www.cnn.com/2000/TECH/computing/01/10/credit.card.crack.2/index.html/

"Security Group Reports Increasing Internet Attacks", Interactive Public Relations, http://www.ragan.com/html/main.cgi?sub=180&cooked=950503-OJOPM-IT&prof=&origsite=http://www.ragan.com&origcount=&origsub=180&origloc=main.cgi&sub=180&bum=0&maga=&reach=10391&base=story&ma=IPR

Sherwin, Gregory R; Avila Emily N, Connecting Online: Creating a Successful Image on the Internet (Central Point, Oregon: The Oasis Press, 1997),

Taylor, Chris "Cracking the Code", Time.com, March 1999, http://www.time.com/time/digital/feature/0,2955,22179-3,00.html

"Tips to Cope With Cybersquatters and Content Republishers", The Ragan Report, http://www.ragan.com/html/main.cgi?sub=180&bum=0&maga=&reach=14789&base=story&ma=IPR

Uzumri, Mustafa V; Snyder, Charles A, " Information Technology and Accelerated Science: The Case of the Pentium Flaw" California Management Review, Vol. 38 No. 2 Winter 1996 p. 44-63, 20 pp.

Weise, Elizabeth (1999) Web hijack turns Turk into sensation. USA Today. Found on: www.usatoday.com/life/lds050.htm

"What to do when a crisis hits—and how you can prevent it"
Interactive Public Relations,
http://www.ragan.com/html/main.cgi?sub=180&bum=0&maga=&reach=8558&base=story&ma=IPR

"When your Web Site Disappears", Interactive Public Relations,
http://www.ragan.com/html/main.cgi?sub=180&bum=0&maga=&reach=5723&base=story&ma=IPR