Protecting an organization’s digital public relations assets

Kirk Hallahan

Department of Journalism and Technical Communication and Center for Research on Communication and Technology, Colorado State University, C-225 Clark, Fort Collins, CO 80523-1785, USA

Received 28 July 2003; received in revised form 12 March 2004; accepted 28 April 2004

Abstract

This review examines new legal and practical problems confronting organizations that arise out of misdeeds by Internet users outside or inside the organization. Five major culprits are identified: attackers, hackers, lurkers, rogues, and thieves. Implications for effective online public relations are discussed.

© 2004 Elsevier Inc. All rights reserved.

Keywords: Digital assets; Internet; Web; Attack; Hack; Lurk; Rogue; Trademark; Copyright; Laws; Regulation

1. Introduction

The advent of the Internet has dramatically changed the way public relations practitioners distribute information, interact with key publics, deal with crises, and manage issues. The Internet also has altered the legal environment in which public relations operates.

Recent changes in United States laws pose potential missteps that should be avoided by practitioners. For example, federal law now prohibits the distribution of certain types of unsolicited e-mails (CAN-SPAM Act, 2003). Practitioners who collect user information online must now adhere to online privacy protection and disclosure requirements depending on the circumstances (e.g., Children’s Online Privacy Protection Act, 1998; Fair and Accurate Credit Transactions Act, 2003; Fair Credit Reporting Act, 1970 as amended; Financial Services Modernization Act, 1999; Health Insurance Portability and Accountability Act, 1996). Similarly, the U.S. Securities and Exchange Commission’s Regulation FD (1999) requires publicly traded companies to avoid selective disclosure of information by providing access to a broader range of investors on telephone conference calls and webconferences.
All of these are potential legal problems that can be created by employees in carrying out their duties. The flip side of the coin involves the various legal headaches now confronting organizations that stem from the misuse of the Internet by unscrupulous or misdirected individuals. These users can destroy, disfigure, damage or diminish the value of an organization’s digital assets. Importantly, these problems stem directly from the interactive nature of online and new communication technologies (Bagby, 2003). Understanding these potential abuses and their possible consequences is becoming an imperative for practitioners.

2. Digital assets defined

Digital assets can be defined as intangible or non-physical assets of an organization, usually stored and disseminated via computer. Examples include all of the creative content produced by public relations professionals and distributed online (the focus of this review) as well as other organizational records, databases and proprietary software.

Digitized public information includes all data that describes an organization, its products and services and its operations. Organizations generally cannot claim exclusive title to public information (vs. private information, such as patents and trade secrets) because information is a public good or commodity that can be exchanged again and again without being depleted (Bagby, 2003; Baunal & Binder, 1998). But public information about organizations provides utility for users because it helps them choose whether to enter into an exchange or other relationship with organizations. Organizations similarly derive benefits to the extent that information about them is timely, accurate, complete and conducive to relationship building.

Digital data are the currency of the Internet age and are especially important for organizations to protect. Computing managers narrowly define digital assets as bytes and bits stored on computers that must be controlled by the organization. A somewhat broader view, more appropriate to public relations, suggests that computerized organizational information has no value unless it is shared and exchanged with others. Whereas the orientation of data processing managers might be to safeguard information, the emphasis in public relations invariably must be to share digital assets—but to do so safely and securely.

Public relations practitioners today find themselves in a brave, new Internet world. People develop expectations about organizations and assess an organization’s performance based upon subtle cues found within the online environment. These fragile relationships can be damaged when expectations are not met or when organizations appear to behave badly online. Practitioners must become informed about how others use or misuse informational or reputational data as well as about the rights of organizations to protect themselves.

3. Online threats to organizations

Organizations face challenges to digital asset security from five principal sources. These culprits can be characterized as attackers, hackers, lurkers, rogues and thieves.

3.1. Attackers

Attackers are critics or opponents of an organization who find online communications a convenient avenue to air disputes or complaints. Attackers are frequently cyberactivists, or individuals who iden-
tify social problems and then organize others to resolve their common concerns. Attackers also can be individuals with strictly personal complaints known as cybergripers (Hallahan, 2004).

Before the Internet, critics were often thwarted in efforts to attack organizations. Public indifference made mobilizing supporters an arduous task. Skeptical editorial gatekeepers dutifully screened out much defamatory, inaccurate or questionable information from sources. Ponderous government processes also made getting attention or action from lawmakers difficult.

Today, the Internet has accelerated the speed of attacks. The World Wide Web, discussion groups and chatrooms, electronic mail, and wireless communications have made it easy for organizers both to reach and to marshal large numbers of people (Coombs, 1998; Heath, 1998; Rheingold, 2002; Taylor, Kent, & White, 2001). At a cost of only several hundred dollars a year, opponents with only modest financial resources can buy computer-hosting services to gain access to a worldwide audience. Through adroit site registrations, web site metatags, bulk mailings to compiled lists, and mail forwarding campaigns targeting sympathetic supporters, activists and others can quickly develop a digital presence.

3.1.1. Legal issues
Although troublesome, attacks are a part of the free expression of ideas. In the landmark Reno v. ACLU case (1997), the U.S. Supreme Court struck down provisions of the Communications Decency Act (1996) and firmly established First Amendment protections for Internet communications. United States law effectively makes no distinction now between the Internet and other forums for free expression. If attacked online, an organization must demonstrate defamation or violation of a specific law. Because most attackers engage in the expression of opinion, and don’t usually maliciously or knowingly distribute false information, courts will weigh any damage incurred by an organization against an attacker’s First Amendment right to free expression.

Several forms of cyberattacks are of special concern to PR professionals. Attack sites are posted to criticize an organization (Holtz, 2002, pp. 293–299). Complaint sites are variations of an attack site, where the general public is encouraged to shares gripes about organizations. Spoof or parody sites are intended to make fun of a public organization, public person or situation (Isenberg, 2001, pp. 241–247). Although these sites sometimes resemble a targeted organization’s site, most site sponsors make it clear they are not trying to confuse users or misrepresent themselves as the targeted organization.

Attack sites, complaint, and parody/spoof sites are legal as long as they are not defamatory, don’t intentionally confuse a user’s initial interest, or are otherwise illegal. Three situations where online attacks might be illegal include hate speech, discriminatory language and terrorism. In the case of hate speech, courts upheld in Planned Parenthood v. American Coalition of Life Activists (2002) that activists cannot use the web to intimidate prospective clients of abortion clinics or threaten people with the use of force in violation of the Freedom of Access to Clinics Entrances (FACE) Act (1994). Similarly, racist or other discriminatory language could be actionable if in violation of civil rights laws (Isenberg, 2001, pp. 251–252; Wolf, 2001).

Special rules related to national security involving cyberterrorism are contained in the USA Patriot Act (2001), but are under challenge along with other aspects of the law.

If a statement is defamatory or illegal, one of the problems confronting organizations is the fact that many attacks on the Internet—in chatrooms, on bulletin boards and on some web sites—are anonymous. In McIntyre v. Ohio Elections Commission (1995), the court upheld the general right of anonymity in free speech. Finding defendants is further complicated by the Communication Decency Act (1996), which
specified, “No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider” (47 USC 230(a)(3)(B)(iii)). Thus, organizations are effectively barred from suing hosting services or ISPs that merely assume the roles of information distributors. Similarly, individuals who merely repost defamatory or other attacking content cannot be sued because they were not the originators (Isenberg, 2001, pp. 227–240).

Court rulings have protected the rights of hosting services and ISPs to not disclose the names of client users. Because of anonymity protection, organizations cannot engage in fishing expeditions and must be able to identify a party with specificity according to one New Jersey court ruling (Dendrite International, Inc. v. John Doe, No. 3, et al., 2001). More generally, several recent court cases have restricted the ability of parties in legal cases from serving subpoenas on ISPs to obtain user records (RIAA v. Verizon, 2003; Theofel v. Farey-Jones, 2003). Similarly, a growing number of states, including California, have adopted anti-SLAPP laws to prohibit Strategic Lawsuits Against Public Participation, which aim to intimidate prospective critics and discourage them from engaging in the free expression of ideas (Isenberg, 2001, p. 237).

Libel laws in other countries—notably Australia, Canada, and the United Kingdom—are more stringent and afford organizations greater protection than in the United States. For the most part, the most solid defenses from attacks in the United States are based on technicalities. For example, organizations might have recourse if a disgruntled employee attacks an organization using information obtained illegally or in violation of a confidentiality clause in an employment contract. Similarly, attackers might be pursued if they use information obtained while in a fiduciary relationship and thus violate of client confidences.

One important arena to watch is the recently passed legislation to regulate unsolicited e-mails (CAN-SPAM, 2003). Spam is generally defined as an undesired commercial message (Janal, 1998, pp. 155–161). However, many people consider spam undesired messages of any type, including political messages from a candidate or cause. Many politicians and activists argue that political communications should be exempted from efforts to regulate spam. The precedent cited is the exemption for political candidates and charitable organizations under the U.S. Federal Trade Commission’s (2003) so-called opt-out provision in the National Do Not Call Registry authorized under the Telemarketing and Consumer Fraud Protection Act (1994). Others argue that e-mail users should be able to turn off service from any undesired sender. The latter might become one tool to reduce attack e-mails.

3.1.2. Protection

What actions—other than litigation—should an organization pursue if attacked? One obvious tactic is to contain attacks. Organizations should routinely monitor what’s being said about them on web sites, bulletin boards, chat rooms and online news services. Available tools include web monitoring services, electronic clipping services, search engines and agent robots. Organizations need to track claims, monitor the spread of attacks or rumors, and respond appropriately (Hallahan, 2004). But as with the case of offline attacks, calling attention to attackers could exacerbate problems by providing them visibility and legitimacy.

Attorneys sometimes issue letters threatening legal action, but such initiatives often have no legal foundation. Although certain attackers might be scared off by the mere threat of costly litigation, others will not. Threats also can backfire by generating negative publicity or unintended leverage for attackers to rally sympathy and support.
3.2. Hackers

Hackers are computer nerds and others who intentionally break into an organization’s computer system to alter content or disrupt operations. Hacking involves an invasion of the privacy of an organization versus a user (Burlington, 1999; Erbschloe & Vacca, 2002; Flynn, 2000; Gralla, 2002; Miller, 2002). Hacking or cracking is a weapon of mass disruption that has become a major concern in today’s era of terrorism and information warfare (Hutchinson & Warren, 2001; Nichols, Ryan, & Evan, 2000; Schwartau, 2000). Some black hat hackers are politically motivated; others engage in illegal activities for financial gain (Water, 2003) and have become celebrities in their own right (McClure, Scambray, & Kurtz, 2001; Schiffman, 2001). By contrast, organizations hire white hat hackers to help them identify and close potential security breaches (Nichols et al., 2000). Hacking can include web graffiti (defacing content). Other mischief involves producing denial of service (DoS) errors or crashing a system by generating thousands of dummy transactions (packet flooding). More serious breaches include theft of trade secrets, software, personal identities (obtaining and then misusing personal information about people), and financial resources (such as unauthorized electronic funds transfers). Still more threatening problems are infecting files with destructive viruses, redirecting transactions to another computer (IP address spoofing), or disarming a computer altogether. Hacking also can involve intrusion into e-mail systems where worms allow unwitting mail users to send thousands of messages that clog up computer systems (Bank, 2004).

Hacking is a growing problem for society (Gunkel, 2000) and affects public relations three ways. First, content can become defaced or altered, resulting in confusion or lost business. Second, hacking mars an organization’s relationships with users and can result in civil claims or criminal liabilities (Pink, 2001). Third, hacking can create public ridicule and reputational headaches. Indeed, many hackers are publicity hounds who seek attention.

3.2.1. Legal issues

The principal U.S. law to deter hacking, the Computer Fraud and Abuse Act (1986), was amended by the USA Patriot Act (2001). The CFCA makes it felony for outside parties to intentionally damage a protected computer by transmission of code, to access a protected computer without authorization, or to cause other damage of any kind. The USA Patriot Act amendments clarified the meaning of damages and intent, specified that computers domiciled outside the United States are covered, expanded the civil damages that can be pursued, and provided protections for hardware, software and firmware companies. The USA Patriot Act also allowed governments to use wiretaps to monitor Internet users and permitted law enforcement officials to intercept communications of computer trespassers without a warrant.

3.2.2. Protection

Public relations professionals need to anticipate and plan for hacking incidents by arranging for regular backups and archiving of content and by planning how they will respond to disruptions in service. Few public relations crisis plans today specifically address computer malfunctions, despite the increasing reliance of organizations on computers for information delivery and e-commerce. PR professionals must recognize the tradeoff between the desire for free access and system integrity (Hallahan, 2004). Organizations can reduce their vulnerability to hackers by developing detailed plans for access to critical information, by installing hardware and software screeners, by employing password and related security procedures, and by educating employees and users. Employee education is especially important.
because many hackers gain entry into organizations by using subversive social engineering—they merely ask low-level employees seeming innocent questions about access, procedures and content. Hackers are often helped by disgruntled employees, paid informants, coerced or compromised employees, former employees, casual or pseudo-employees, or business associates (Nichols et al., 2000).

Besides outside intruders, a particular threat to many PR departments involves hacking attempts from inside the organization—unauthorized access to Intranet systems, mail or other computer systems where sensitive information or proprietary documents and graphics are stored. PR managers need to examine whether people outside of the department should have access to the unit’s mail system, or whether the use of imaging and other document systems should be restricted.

3.3. Lurkers

Lurkers are legitimate or authorized users of an organization’s information resources—visitors to web sites, subscribers to listservs, recipients of e-mail and users of an organization’s intranet. However, their motives are not always readily evident and might be questionable.

Lurkers, for example, can be competitors who can collect an enormous amount of competitive intelligence via the Internet (McGonagle & Vella, 1998). Lurkers also include professional research firms, analysts, recruiters, brokers and others seeking information that might benefit their clients or themselves. Public relations people traditionally have emphasized the free and widespread distribution of organizational information. Practitioners want people to have access to information—and in cases such as the press, to share it with others (Hachigian & Hallahan, 2003). But lurkers represent a potential economic drain on organizations by stealing information, personnel or other intelligence—and force organizations to ask themselves how much information should be made available online.

3.3.1. Legal issues

Lurking is not a criminal offense—provided that the information is obtained legally. This is an area in which the law is least developed. Potential problems include the followings.

3.3.1.1. Impersonation. Many lurkers who are only seeking detailed information about an organization want to keep their identities secret. While anonymous speech is protected, impersonation by users has not been addressed. What constitutes fraudulent activity in this regard? As one famous New Yorker cartoon suggests, it’s often impossible to know who a particular Internet user really is—he or she actually might be a dog (Reed, 2000).

3.3.1.2. Downloading. Many lurkers download and retain indefinitely massive amounts of information. Use of web content carries with it an implied license to use the content (Web Law FAQ, 2003). But such an implied license should not allow people to use content in whatever way they choose. Fair use guidelines in the federal copyright laws suggest that some limitation on the overall amount of downloaded material might be appropriate. But should owners also be able to prohibit commercial (vs. personal) use? Or impose limits beyond one-time use? These are not easy questions.

3.3.1.3. Financial disclosures. U.S. securities laws mandate that publicly traded companies avoid manipulative and deceptive practices, particularly insider trading (Securities Act of, 1934, amended 1951). Although the SEC has encouraged companies to take advantage of new technologies (U.S. Securities and
the agency has not addressed what diligence publicly traded companies should follow to protect potentially material information that might be uncovered innocently by lurkers in an electronic databases. Lurking employees could easily become inside traders if they use the information for their own financial gain. Negligence also could create criminal liabilities for the company or its officers for failure to control access. In a similar way, organizations must protect themselves from unscrupulous lurkers who accidentally expose trade secrets (Klosek, 2003, pp. 128–129).

3.3.1.4. Cyberstalking. At some point, lurking for information can evolve into the stalking of an organization’s senior officers or employees. Stalking could include merely eavesdropping on an individual’s activities or obtaining details about a person’s personal life. More serious stalking can involve annoying correspondence, harassment or threats. Federal laws prohibit the electronic transmission of threats in interstate or foreign commerce (Criminal Law and Procedures Technical Amendments Act, 1986) and prohibit direct voice communications from an anonymous caller to annoy, abuse, harass or threaten a person (Telecommunications Act, 1934). Children are also protected from sexual stalkers (Protection of Children from Sexual Predators Act, 1998). However, federal law does not address intrastate violations, nor communications involving private telephone or Intranet systems, nor stalking that might occur on bulletin boards or chat rooms because direct, oral communication is not involved (Cyber-stalking.net, 2003; U.S. Department of Justice, 1999). Although proposed federal legislation was never adopted by Congress in 2000, 44 states in the United States (and several other major countries) have anti-stalking laws that apply to online activities (Working to Halt Online Abuse, 2003).

Electronic harassment, such as the distribution of pornographic images or lewd e-mails, has led employers to discipline or terminate employees. But the mere monitoring of another employee’s actions is not necessarily illegal or actionable under the Electronic Communication Privacy Act (1986). The ECPA law gives organizations the right to control use of private telephone and electronic mail systems, but an employee generally must violate a published policy, such as inappropriately overriding access or authorization codes, to be culpable.

3.3.1.5. Robotic lurking. Organizations today are finding confidential or sensitive documents appearing on search engines such as Google and Yahoo! that use automated web crawlers or agent technology to catalog web content. Sometimes mislabeled “Google hacking,” this electronic lurking usually is not targeted against specific organizations. Upon arrival at a server, web crawlers routinely identify accessible documents using robots.txt files created by the server’s operator. However, improperly configured servers, holes in security systems, and human error can lead to materials becoming public that were not intended for viewing. Once captured and cached on search engines, these materials become nearly impossible to draw back into secrecy (Noguchi, 2004). Robotic lurking is now legal and is being actively encouraged in books about hacking (Calishain & Dornfest, 2003; Hemenway & Calishain, 2003; Hock, 2004).

3.3.1.6. Spyware. Electronic lurking has been made easy by the advent of spyware, or software unwittingly downloaded by users without their consent. Also known as spybot or tracking software, spyware or adware software can be installed on personal computers when employees click an option to download free web tools or software.

Cookies are the most common form of adware and can retain useful for users, but are not usually normally a security concern because users can accept or reject cookies and can disable them easily. Other techniques include the use of web bugs. These barely visible images (usually only 1-pixel) that trigger
tracking of users whenever the image on which they appear is downloaded. Information captured can include the IP address, the type of browser, a time stamp and any previously created cookies related to the page. Trojan applications, the most extreme form of spyware, can provide a remote user full control of another computer and harvesting data, address books or documents.

Most of these drive-by downloads are used by online advertisers to channel banner and pop-up ads to users with particular interests based on visits to or time spent on other Internet sites. Although most spyware does not hack into an organization’s proprietary data system, spyware obviously divulges valuable corporate intelligence about the online activities of an organization’s staff (Cexx.org, 2004; Spychecker.com, 2004).

3.3.2. Protection
PR departments concerned about lurkers both outside and inside the organization must recognize that all control is lost once information is posted online. Organizations should adopt clear policies about proprietary or sensitive materials and review content carefully and regularly. Less, rather than more, might be a useful rule-of-thumb.

One method to deter lurkers is to ask users to register and/or to receive a password. However, such techniques also can discourage legitimate users—people organizations want to reach online. Many reporters, for example, resist password-protected registered sites (Hallahan, 2004). Less obtrusive methods of monitoring lurkers include encryption, digital signatures, and fingerprint/eyeprints (Janal, 1998, pp. 35–41).

Organizations are wise to discourage or prohibit the disclosure of employees’ personal names or work locations. Similarly, the e-mail addresses and phone numbers of senior officers should not be unpublished to reduce security risks. Indeed, several web search engines (such as Map Quest) enable stalkers to find street addresses by simply typing in a telephone number.

Lurking can be monitored, to a limited extent, through web visitor logs. Daily access to a web site can be an indicator of lurking. Addresses can be traced; access can be blocked if a users’ activities are suspicious. But serious lurkers will quickly find other avenues of access. Alternatively, posting terms of use policies might provide some protection. Robotic lurking must be addressed by regular updating of robots.txt files.

3.4. Rogues

Rogues are operators of web sites or e-mail addresses who deliberately attempt to take advantage of an organization, often by misrepresenting themselves to other Internet users. Rogues come in several stripes.

A rogue web site is a site established with a domain name (also known as a Uniform Record Locator or web address) that is similar to a legitimate organization’s web site but purposely tries to confuse users. The best-known example is whitehouse.com, a porn site intended to be confused with whitehouse.gov. Some rogue sites are created to siphon business away from a legitimate organization. Other rogues merely want to generate traffic (Janal, 1998; pp. 35–51; Holtz, 2002, pp. 291–305).

Some rogue sites are actually attack sites. The deception occurs because of their use of URLs similar to that of the targeted organization. Ford.org, for example, was a web site operated for several years by consumer activists and so named to be confused with Ford.com. Many early attack sites began by including the names of specific organizations in their web addresses, but recent threats of legal action discouraged such practices. Today, complaint sites such as sucks500.com are more generic and avoid trademark problems. However, these sites capture users via search engines by prominently including
the name of targeted organizations in metatags or the first several lines of a site’s text. One appellate court ruled that use of another company’s name in the metatag of a web site is legal as long as the name is reasonably necessary to identify a product featured on the site and not intended to confuse users (Playboy Enterprises, Inc. v. Terri Welles, 2002).

Another rogue is the cybersquatter, who purchases available site names and then resells the registration rights to organizations that want to use that name for legitimate business purposes (Isenberg, 2001, pp. 77–87; Silver, 2000). Cybersquatting is tantamount to extortion because squatters exploit buyers by charging exorbitant prices. Abuses are exacerbated by the fact that URLs are registered for short periods of time—only one to three years. Owners frequently forget and allow registrations to lapse. Meanwhile, web registration firms and ISPs have created a vigorous secondary market in which people can reserve in soon-to-expire domain names.

Fan sites, another thorny type of rogue site, are created by users, customers, audience members or others who are infatuated with a particular subject. Promoters of movie, book, television and music properties should want to encourage such authentic forms of word-of-mouth endorsement. But many fan sites cross the line by misappropriating copyrighted material and by diverting traffic from officially sanctioned sites that generate revenue by selling products (e.g., branded merchandise) or services (e.g., downloadable music). Many fan sites also can pose problems because they sponsor bulletin boards or chatrooms where moderators and users can express derogatory comments. Opinions expressed by the operators of these sites probably are protected speech under the “fair comment and criticism” tenet of defamation law (Janal, 1998).

Phishing involves e-mail frauds by third parties who impersonate legitimate organizations in order to steal a user’s personal information or identity. Spammers use regular e-mail and spammers use instant messaging (Sorow, 2003) to send out annoying but otherwise legitimate junk e-mails. By contrast, phishers deceive users and impugn the good name of organizations by using what appears to be a familiar e-mail address that users don’t notice is misspelled or is otherwise odd. Ploys include asking e-mail recipients to open an attachment, to enter a site using one of their existing user names and passwords, to send contributions to an ostensibly worthy cause, to confirm shipments (for merchandise already received), or to otherwise provide personal information. Financial institutions and merchandisers are particularly vulnerable to phishing expeditions (Anti-phising.org, 2004; Hanrahan & Fry, 2004).

3.4.1. Legal issues

Rogues most often run afoul of the trademark protections afforded organizations under the Lanham Act (Federal Trademark Act, 1946). Here the law is fairly clear: Rogues cannot use a trademark or name without the permission of an owner. Obviously, most organizations are not going to grant permission if their trademarks might be misused or diluted.

The U.S. Anti-Cybersquatting Consumer Protection Act (1999) protects organizations against cyber-squatting, although various other trademark precedents, such as the Federal Trademark Dilution Act (1985), also have been used to fend off cybersquatters. The ACPA expanded U.S. trademark laws to specifically prohibit practices where a domain name registrant exercises “a bad faith intent to profit” from a trademark. The protection is accorded only if the registrant registers, traffics in or uses a trade name that is distinctive, famous or specifically protected by law (such as certain Olympics marks) at the time that a new domain name registration is sought (Isenberg, 2002, pp. 77–87; Silver, 2001).

Disputes about domain names can be arbitrated under the Uniform Domain Name Dispute Resolution Policy established by the international governing body that oversees web names. The Internet Corporation
for Assigned Names and Numbers (ICANN) established this program because so many disputes cross international jurisdictions (Isenberg, 2002, pp. 87–98).

3.4.2. Protection

As both a legal and public relations policy, organizations must vigorously protect their trademarks and their brand equity. Routine monitoring of web sites and news groups is an important method to contain abuses by rogues.

Public relations practitioners who become involved in online branding and web addressing issues also need to consider carefully how to avoid abuses by rogues. Prudence suggests organizations should register: (a) alternative suffixes, e.g., .com, .net, .org, .info, (b) misspellings of their organization’s names (if applicable), and (c) international domain extensions to protect them from use/misuse by others. Registrants also must consider whether other trademark holders could pre-empt their trademark rights to a URL not in use.

3.5. Thieves

Thieves are online operators and users who rob organizations by downloading intellectual property. Digital technology has made stealing easy for thieves and has prompted nations around the world to re-examine their laws related to fair use of intellectual properties (National Research Council, 2000; Saunders, 2001). Although software is now protected as a literary work (Computer Software Copyright Act, 1980; No Electronic Theft Act, 1998), most public relations practitioners are concerned about the theft of content. Common content thieves include:

- counterfeiters who seek commercial gain by reselling content online or in another form;
- private parties who share files containing images, audio or video and thus avoid paying royalties to copyright holders;
- information purveyors who pass off content as their own in order to avoid the cost of creating or obtaining their own;
- web site sponsors who repurpose (reformat) content for their own purposes using linking and framing. Commercial operators, for example, might frame someone else’s web site with advertising. Meanwhile, noncommercial operators might surround another organization’s web site with disparaging comments (a variation of an attack site).

3.5.1. Legal issues

Many public relations practitioners do not consider most of the materials they create to be of sufficient long-term value to copyright them. However, many organizations use borrowed creative works that they should protect. Publicists and others representing artists, for example, want to make sure that promotional materials are not resold or reused for entertainment fare in their own right (Zorich, 1999) and are obligated contractually and ethically to protect others’ copyrighted material.

Congress passed the Digital Millennium Copyright Act (1998) in response to two treaties passed by the World Intellectual Property Organization. In addition to updating and extending protections under the Copyright Revision Act (1976). DMCA provided artists with the right to imbed digital identifiers in copyrighted material. These identifiers are commonly referred to as digital object identifiers (DOIs), watermarks or fingerprints. All rely upon stenographic (science of hiding information) technologies
DMCA makes it a crime to produce, market or use devices that detect, distort or remove these markers. Not surprisingly, several important copyright issues are not resolved fully. One deals with the right of one web site operator to link (insert hyperlinks) directly to files domiciled on another site. Here another’s asset is being merely used, but not acquired. Although site owners might not be able to prohibit hyperlinks, some experts suggest the inclusion of a link license agreement on web sites (Klosek, 2003, pp. 132–140; Web Law FAQ, 2003).

Another thorny issue deals with the use of firm or trade names. Web site operators or bulk e-mailers clearly would be in violation of the trademark laws if they used an organization’s logo on a site without permission. A site operator also could be prosecuted if a text link contained malicious or defamatory comments. However, it is not clear that the courts are prepared to bar simple text links—particularly if no confusion of initial interest is created and the use of the link is necessary to express an idea or support a claim (Bilalaw, 2003; Web Law FAQ, 2003).

3.5.2. Protection

Public relations practitioners should use care in posting copyrighted materials their clients do not wish to have duplicated by others. When in doubt, leave it out. A disclaimer or terms of use statement should appear on web sites and preferably be repeated or linked on every page. Similarly, when previously copyrighted material is deemed beneficial to post, a copyright notice should be prominently featured with each copyrighted item. PR practitioners also might consider the use of watermarks or fingerprints that permit the identification of stolen property (ImageProtection.net, 2003; Seybold, 2003).

Organizations should monitor Internet content for potential copyright or trademark infringements or dilution in the same way they monitor for rogue activities. Generally, trademark and copyright owners must demonstrate their diligence in protecting their intellectual properties. This includes but is not limited to avoiding genericide, which occurs when a proprietary name evolves through everyday use into a generic term for a category of products.

Fortunately, U.S. law allows organizations to obtain quick redress for online copyright infringements. In order to limit the legal liability of Internet service providers when their clients illegally post copyrighted materials, the Digital Millennium Copyright Act (1998) created a “safe harbor” provision where ISPs can designate agents to receive complaints. Once an agent receives a notice containing information specified in the statute, the ISP is required to “expeditiously” remove or disable access to the allegedly infringed material until the dispute is resolved (Isenberg, 2002, pp. 41–45; Klosek, 2003, pp. 140–143).

Several linking practices are suggested to reduce infringement problems. One is to design an organization’s web site so that links can be made only to a home page, not secondary pages—a troublesome practice known as deep linking (Klosek, 2003, pp. 132–134). Another is to clearly label all pages with the organization’s name in order to bar others from passing off content as their own. Images can be provided with low resolution or visible ownership markers that make them less attractive to steal. Image tags for particularly popular items also can be changed periodically and replaced with nuisance images that discredit poachers (Web Law FAQ, 2003).

Theft is not limited to copyrighted material. Organizations often compile materials in formats that cannot be protected through copyrights, such as lists and directories. Misuse can be restricted by requiring passwords or one-time access codes, or by charging fees using the organization’s secured e-commerce capability. Disclosures or purchase agreements should state restrictions and outline fair use and permissible practices.
4. Implications for public relations practice

Public relations professionals today clearly must recognize and understand a variety of new legal issues stemming from the interactive nature of new communications technologies. In some instances, practitioners might need to become experts in order to cope directly with particular problems confronting their client organization.

To do so effectively, practitioners must forge a good working relationship with IT (information technology) professionals in their organizations to address security and related problems (Grupp, 2000; Holtz, 1998, 2002, pp. 357–361; Margaritis, 2000). Their technology lexicon needs to include ideas such as access control, identification and authentication, firewalls, virtual private networks (VPNs), public key infrastructures (PKIs), and secure socket layers (SSLs) that encrypt and authenticate information. PR staffers (or user analysts assigned to work with them) also need to understand how systems administrators can employ intrusion detection, vulnerability scanners, virus controls, system architecture and managed security services to prevent and respond to problems (Janal, 1998; NetManage, 2003; Proctor & Brynes, 2002; Spinello, 2003).

Public relations professionals and their employer organizations also need to recognize more fully both the tangible (financial) and intangible (reputational) value of digital assets. One technique to do this is to conduct periodic audits of an organization’s online intellectual properties. The process includes determining the extent and location of holdings, verifying ownership rights, identifying vulnerabilities or exposure, reviewing current policies, and imposing practices and policies that limit access (Blonder, Charney, & Gold, 2001; Huhn, 2000; Janal, 1998; KPMG, 2002; Lipton, 2000). Most organizations should establish clear policies that include public relations-created content along with digital assets managed by other units. PR managers also need to address digital assets in their contingency or crisis plans. In the case of attacks and hacks, organizations must recognize the potential damage to digital assets are important potential risks that have financial and reputational consequences (Gunkel, 2001; Hutchinson & Warren, 2001). The Internet represents both a new source for crises and a new tool for crisis management. Uninterrupted access to the Internet in a time of crisis is critical in today’s era, whether the triggering event occurs online or offline (Hallahan, 2004).

Effective protection of an organization’s digital assets include: (a) engineering, (b) enforcement, and (c) education (see also Lipton, 2000). Organizations must invest in hardware and software protections that will enhance security and reduce vulnerabilities. Organizations need to be diligent to assure policies are followed and abuses are prosecuted or otherwise curtailed. Finally, organizations must involve everyone in the organization in the preservation of its computer-based intangible assets.

References
