HANDBOOK OF RISK AND CRISIS COMMUNICATION

Edited by
Robert L. Heath
H. Dan O’Hair

Routledge
Taylor & Francis Group
NEW YORK AND LONDON
2009
21
Crises and Risk in Cyberspace

Kirk Hallahan
Colorado State University

Since the mid-1990s, the Internet and related technologies have become integral parts of the way people and organizations communicate. Not surprisingly, these have become commonplace tools in crises and risk communication.

Today, Internet technologies include Web 1.0 tools such as e-mail, Web sites, chats and discussion boards (also known as newsgroups). More recent innovations include Web 2.0 technologies such as blogs (Web logs), wiki's that permit the collaborative creation of content, audio podcasts and video vodcasts, and social networking media. The latter allow users to maintain friendships (e.g., MySpace.com and Facebook), share music and video files, recommend and rate news (e.g., Digg.com), and post and stream videos (e.g., YouTube). Merging into the mix is cellular telephony. Cell technology uses over-the-air digital transmissions instead of networked coaxial cable connections and relies on hand-held phones or personal digital assistants (PDAs). Nonetheless, the converging systems now allow the exchange of the same varieties of content.

Technology is not an altogether new trend in crisis or risk communication. In the 1970s and 1980s, telephony, private telegraph systems, teletypers and facsimile machines, computerized data bases, audio and video conferences, and satellite news distribution were all recognized as potentially valuable tools in crisis and issues management (Calloway, 1991; Calloway & Keen, 1996; Heath, 1997; Ramsey, 1993). However, electronic communications are more important today than ever before based on high levels of adoption of and dependence upon personalized telecommunications devices by individuals. More than two-thirds of people in leading industrialized countries have Internet access in some form, while three-quarters of them use cell phones (Horrigan, 2007).

Crisis management and risk management operate in a new communication technology age (Heath & Millar, 2004, pp. 2–3) where new technologies have changed how organizations communicate with stakeholders and how people communicate with one another (Massey, 2004, pp. 245–246). Moore (2004) summed up the recent changes as a "seismic but dangerously neglected shift in the world of crisis" where "Constant enhancement in the ability of IT [information technologies] to merge rapid information exchange, opinion formation, and decisive stakeholder action will force crisis-hit companies to rethink crisis response strategies" (p. 29).

Information technologies found in and outside of cyberspace are organizing resources that can be deployed by organizations to manage crises and risk (Calloway & Keen, 1996; Calloway, 1991). Coombs (2007) noted the Internet can be a tool for environmental scanning and issue monitoring, for employee communications, for access to third-parties by organizations and media, and for assessing impact. Yet, the importance of cyber media has not yet been recognized universally. For
example, although communication with traditional media was identified as one of 10 best practices in crisis communications, direct communications with affected publics via the Internet or cellular communications was not addressed (Seeger, 2006).

New media technologies provide organizations with new options for dealing with crises, but also can be the sources of new varieties of organizational crises to which they must respond. At the same time, new media are used by people and organizations confronted with risks but also pose new risks for them. This review surveys current trends and the evolving research related to crises and risk as they relate to Internet- and cellular-based communications.

CRISIS RESPONSES

Early Online Crises


Several authors cited crisis communication as an important application in early books dealing with online public relations (Haig, 2000; Holtz, 1999, 2002; Levine, 2002; Middleberg, 2001; Phillips, 2000; Sherwin & Avila, 1997). The role of online media in crises also began to receive attention in other reviews within public relations (Baines, Egan & Jefkins, 2004; Bertolucci, 1999; Campbell, 2002; Doucette, 1998; Hallahan, 2001, 2004a; James, 2000; Guth & Marsh, 2005; Regester & Larkin, 2005; Shankman, 2000) and within the crisis management literature (Berkeley & Woolard, 2001; Boyd, 2000; Bucher, 2002; Caponigro, 2000; Sweetman, 2000; Mak, Malloard, Bui & Au, 1999; National Research Council, 1998; Neil, 2000; Seymour & Moore, 2000).

In large measure the importance of new technologies in crisis response reflects the integration of interactive media into the mix of media used by organizations generally and public relations in particular. The past two decades saw the rise of virtual management and teams that rely on computer networks to function. The result has been more structurally flattened (vs. hierarchical) postmodern organizations that are highly decentralized, interactive, collaborative and transparent (Boje, Gephart & Thatchenkery, 1996; Boone, 2001; Clegg, 1990). Virtually every managerial function has been computerized in some way, including conflict resolution (Ford, 2004).

Within public relations, interactive or digital media have become an integral part of the mix of media used in public relations (Hallahan, 2001) and have transformed the practice (Key, 2005; Pavlik, 2007; Ziegler, 2006). Although many organizations adopted Internet technologies cautiously (Hill & White, 2000; Johnson, 1997; White & Ramon, 1999), practitioners soon embraced and promoted the Internet (Gregory, 2004; Institute of Public Relations, 2000; Mickey, 1998). Practitioners previously had recognized the value of computers and data bases (Petriso & Wang, 1993; Ramsey, 1993; Thomsen, 1995) and quickly adopted the Net as a research tool (Gaddis, 2001; Lordan, 2001).

The importance of new technologies in crisis responses also reflects how technology changed journalism, including crisis coverage (Pavluk, 2003). News organizations quickly adopted computer-assisted reporting, e-mail contacts with sources, e-mail interviews, online newsgroups, Web conferences, RSS feeds from blogs and other sources, and cellular technologies as basic methods of newsgathering (Alfonso & Miguel, 2006; Callison, 2003; Duke, 2002; Hachigian & Hallahan, 2003; Hallahan, 1994; Porter, Sallot, Cameron & Shamp, 2001; Sallot & Johnson, 2006; Shin & Cameron, 2003; Woodall, 2006).

New Media in Crises Responses

Around the time the new millennium began, most organizations had addressed online communications in their general crisis planning (Few companies 2001; Hanna, 2005; Internet disaster recovery, 1997). Later research indicated a growing number of tools had been deployed in crisis responses by corporations (Perry, Taylor & Doerfel, 2003; Taylor & Perry, 2005). One recent study found that the Internet was employed in at least half of 175 surveyed crises and suggested that a series of best practices was emerging (Taylor & Kent, 2007). A separate study found that technology was incorporated in crisis preparedness planning: Practitioners are paying particular attention to e-mail and test messaging as a communication tool, and large organizations monitor the Internet at levels equal to broadcast media (Cloudman & Hallahan, 2006).

New media have proven valuable in both the anticipation of and response to crisis. For example, businesses have launched online campaigns to seek a favorable judgment in litigation or passage of legislation that would allow them to maintain business practices essential to their operations (Bounds, 2007; MP3.com launches, 2000). Online communications have been used in product recalls by companies, including Ford and Bridgestone, to avert potential crises (Copeland, 2000; Gibson, 2000a, b; Tillet, 2000). *Southern Living* even used the Web to withdraw the entire run of its April 2004 issue because of a problematic recipe that could explode "like napalm" (McKay &ollenkamp, 2004). Financial institutions similarly used the Web to educate bank customers and others about potential problems with Y2K problem as the year 2000 approached (DiNardo, 2002).

During the response phase of crises, standard planning practices today call for organizations to use e-mail, Web sites, discussion boards, and short-message services (Instant Messaging) to inform stakeholders and media about crises—which happened, instructions for actions, and reassurances about effort to solve problems. For example, Yum Brands effectively posted its own video—not merely a press statement—to apologize to the public after a widely circulated Web video depicted rats scurrying around one of its franchised restaurants undergoing renovations in New York City (Macarthur, 2007). Organizations have recognized the value of telephony and text messaging for groups where numbers are readily available, such as student and employee groups affected by the shootings at Virginia Tech (Irvine, 2006; Swartz & Hopkins, 2007; Yuan, Dade & Prada, 2007).

Organizations now understand that crises dramatically increase traffic to Web sites. For example, Hurricane Katrina generated 1.7 million search engine searches and 9 million visits to WeatherBug and the Weather Channel, while the Red Cross.org Web site saw a 32-fold increase in daily visitors during the crisis (Francisco, 2005). Web sites, e-mails and text messages are particularly valuable to present and maintain accurate perceptions of the organization; present timely, accurate, up-to-date information; facilitate the work of media; manage negative publicity; and direct the activities of staffs and others affected by a triggering event (Bagg & Pyle, 2001).

As a result both content and technological Webmasters and e-mail/text messaging specialists have become essential members of crisis response teams (Alvey, 2005) and organizations must consider alternative methods of communication when e-mail is not available (Krupa, 2002). Prudent organizations are ready to expand computing capacity through access to additional servers and/or alternative hot sites operated by third-party service bureaus that now specialize in emergency recovery services (Bird, 1997; Callan, 2002; Fried, 1995; Mason, 1991; Robinson, 2003; Wallace & Webber, 2004).
Best practices suggest that organizations create *in advance* templates (also known as *ghost* or *dark sites*) to replace a site’s home page whenever a major crisis occurs. Alternatively, organizations can establish microsites for managing crises and their aftermath. These are special-purpose sites with unique names and/or Web addresses (URLs) and can include victim assistance information (Middleburg, 2001). These complement phone banks of trained staff who answer telephone calls coming to previously designated phone numbers. Importantly, many organizations—or the survivors or families of victims—create special Web sites to commemorate a tragic event—a virtual forum for the survivors and others to express grief.

E-mail, intranets and extranets, and cellular telephones have proven to be valuable channels to collect intelligence from employers, customers and other interested parties during crises (Krupa, 2002). Electronic communications are particularly valuable for people in remote locations not affected by utility outages. Public discussion boards, for example, allow people to post questions or provide answers about missing people or property, or to make appeals for assistance. Social networking sites such as MySpace or Facebook can serve as similar function for registered members, such as the students at Virginia Tech (Kantor, 2007; Shneiderman & Preece, 2007). Following the 9/11 attacks, organizations used the public Internet (in lieu of their out-of-commission private intranets) to locate and organize employees and to resume operations (Kiger, 2001). Internet communications also complemented traditional media in communicating crisis news and updates to employees (Downing, 2004; Glass, 2002; Greer & Moreland, 2003; Wolfington & Wyatt, 2004, pp. 388–394).

The Internet has proven to be a powerful tool to organize disaster relief efforts. One of the earliest such applications was the Red Cross’s intranet, ARC Online, which fed updates on Hurricane Fran from its central office to affiliates across the country in 1996 (Deck, 1996). Relief agencies used the Internet to coordinate relief activities in the wake of the Indonesian tsunami and Hurricane Katrina (Coren, 2005; Still, 2005). Meanwhile, information technology has been recognized for its role in the management of emergency medicine (Matthew, 2005). Relief agencies such as the Red Cross and Salvation Army routinely use Web sites and make solicitations to prospective contributors via e-mail following major disasters. One of the easiest forms of collecting contributions is to set up arrangements with cellular firms so cell phone users can call a designated number and have their cellular account charged a specified amount, which is automatically forwarded to the designated charity (Buckman & Pringle, 2005).

Government and relief agencies are also seeking to understand how to utilize new communications technologies in disasters. During Hurricane Katrina, for example, the Federal Emergency Management Agency (FEMA) used a Web site to coordinate the donation of goods from the public. Sponsored research and other initiatives are under way related to geo-collaborative crisis management (MacEachern, Fuhrmann, McNeese, Cai & Sharma, 2005), improved inter-agency cooperation (Horan, Marich & Schooley, 2006; Batteau, Brandenburg & Seeger, 2006) and the enhancement of humanitarian relief networks (Genova, 2006; Stephenson, 2005).

**CRISSES CREATED IN CYBERSPACE**

While organizations use online communications to *respond* to natural disasters and human-generated crises created offline, new media can *create* crises for organizations in their own right (Fearn-Banks, 2007). Not surprisingly, the Institute for Crisis Management has added computer manufacturers to its list of the most crisis-prone industries (Woyke, 2007). Internet-caused crises are a special case of *technology-based crises*, which are typically rooted in the system’s complexity and the inter-connectedness of components in the system (Perrow, 1984, pp. 348–349). Such *cybercrises* involve triggering events that occur in cyberspace, create significant uncertainty, disrupt organizational operations, and might mar the organization’s relationships or reputation—either online or offline.
Online crises fall into three broad areas: 1) outages and unplanned disruptions in service, 2) harmful comments, hoaxes or rumors, and 3) outright attacks by detractors.

Outages and Unplanned Disruptions in Service

With the increased interdependence of users and organizations on information technologies, a particular problem involves system failures that interrupt business or other interactions. Organizations are under continuing pressure to maintain the _uptime_ or reliability of systems. Thus crisis management has become a priority for organizations (E-Business emergencies, 1999; Internetweek, 1999). Notable lapses in performance during the past decade included frequent disconnections of customers by Internet service providers (ISPs) during periods of heavy demand (Anthes & Wagner, 1996). Major e-businesses also suffered from user demands that exceeded system capacities—Charles Schwab in 1997, H&R Block in 2000, and TurboTax in 2007, to name a few (Dalton, 1999; Sullivan, 2000; Tax traffic swamps, 2000). In April 2007, owners of BlackBerry PDAs found themselves out of service due to a wayward system software upgrade. The result was a service crisis bungled by the company (Bulik, 2007; Meyerson, 2007).

Disasters that disrupt local electrical service have an obvious impact on the ability of organizations to maintain online systems in affected areas. Surprisingly, a National Academy of Science study showed that damage to the Internet was limited following the 9/11 attacks (Internet damage, 2002). Yet an electrical blackout in New York City only two years later illustrated dependability concerns (Harmon, 2003).

Systems are also subject to deliberate attempts to interrupt continuity—a vulnerability attenuated by the increased dependence by organizations upon just-in-time supplies delivery systems. Computer system operators must now be vigilant against computer hackers who try to break into systems for financial or political gain, as well as distributors of software program viruses and e-mail worms whose motivation might be the mere notoriety when such outages are reported in the press (Hallahan, 2004b). Although software viruses and e-mail worms are hardly new, the varieties of malicious software (malware) used to commit computer crimes are growing (Brandt, 2006; Richmond, 2006a) despite efforts to thwart criminals (Acohido, 2006; Acohido & Swartz, 2006a, b; Ante & Grow, 2006; Grow, 2005; Hamm, 2006).

The most extreme form of disruption involves _cyberterrorism_, which involves the creation of weapons (malicious software and electromagnetic weapons) intended to disrupt the physical world, often for political purposes (Barnes, 2003, pp. 260–261; Embar-Seidon, 2002; Keegan, 2002; Matusitz, 2005; Stanton, 2002). Despite a lack of any evidence, press reports about the bombing of the Murrah Federal Office Building in Oklahoma City in 1995 claimed the bombers used the Internet to communicate their plans. Following the event, discussion boards (personal Web sites were in their infancy) were rife with malicious rantings (Barnes, 2003, p. 261).

Federal officials acknowledged the United States' cybervulnerabilities as early as 1997 when a commission called for the creation of a National Infrastructure Protection Center (U.S. Department of Justice, 1998; Sauter & Carafano, 2005). A small-scale preview of the potential danger occurred in the Big Hack Attack of 2001, where Chinese and American hackers commandeered sites in each others' countries following the collision of an American spy plane and a Chinese jet. The incident resulted in the shutting of sites in both countries by hackers but mostly involved minor _cybergraffiti_ (Smith, 2001). Today, _Internet jihad_ refers to the use of online technologies by political extremists in the Middle East (A world wide web of terror, 2007).

Following 9/11, the United States saw renewed warnings about cyberterrorism (Schwartz, 2001), and many organizations stepped up their vigilance (McMahon, 2000; Murray, 2004; Quinley & Schmidt, 2002; Thomas & Loaders, 2000). The 9/11 attacks led the U.S. government to remove already widely available public information from government agency Web sites (Fox, Rainie & Madden, 2002; Lehmert, 2002; Reporters Committee, 2003). The military also beefed up its Internet
Harmful Comments, Hoaxes and Cyber-Rumors

Although preceded by a very similar event more than year before (Roper, 1995), the first major cybercrisis is generally acknowledged to be the user revolt in 1994, when giant computer chip manufacturer Intel ignored comments in a computer discussion group that its new Pentium chip contained a flaw that resulted in errors when making advanced mathematical calculations. Intel did not act until the controversy made its way into the trade and business press, and IBM—its largest customer—announced it would suspend use of Intel chips as components in its personal computers (Marlow, 1999, pp. 169–174; Burgelman & Grove, 1996; Emery, 1996; Hallahan, 2008, pp. 62–63; Hearit, 1999).

As the Intel case showed, the Internet is a powerful communications channel that can create awareness among albeit small and fragmented audiences. However, Internet communications also can set the public agenda in cyberspace and beyond (Dzwo, 1998; Dzwo, Roberts, Baker & Sutherland, 1999; Roberts, Wanta & Dzwo, 2002). Internet communities can moderate public opinion and thus can be contingent factors for how an organization might respond to a crisis (Cho & Cameron, 2006; Kim & Shin, 2005).

Advocates of Internet communication argue that the Internet is today’s equivalent of Jürgen Habermas’ public sphere (Coultry & Curran, 2003; Gimmel, 2001; Habermas, 1962/1989; Motion, 2001; O’Donnell, 2001). Benefits cited include the facilitation of community (Badaracco, 1998; Rheingold, 1993), dialog between organizations and their constituents (Ainsworth, Hardy & Harley, 2005; Heath, 1998; Kent & Taylor, 1998), and the promotion of social corporate responsibility (Coombs, 1998). However, critics point out the Internet is not truly egalitarian but, instead, is an oligarchy of public opinion (Schild & Oren, 2005).

Due to easy access and the Internet’s power to dissemination information quickly and broadly, organizations can be thrown into disarray from comments online in the same way organizations can be hurt by negative publicity in traditional media. Only its ability to quickly reach highly segmented audiences directly makes the Internet more powerful than traditional media. Examples abound of how e-mails have disclosed information unflattering or incriminating information about government officials and organizational executives (Abrahamowitz, 2007; Hagan, 2007; Rundle, 2007), both intentionally and unintentionally. Many of these comments were made by users who mistakenly believed their writings were private. E-mail forwarding can spread negative information in the same fashion that viral marketers use the Internet to create “buzz” about new products and services (Warren & Jugenson, 2007).

Bulletin boards and chats continue to draw diastrites. In one example in 2007, U.S. retailer Home Depot saw 4,000 angry posts from customers following negative remarks by the moderator in an MSN comment room. Another 10,000 disgruntled customers e-mailed the company (Conlin, 2007). Although bulletin boards and chat rooms are intended to encourage and facilitate the free exchange ideas, online anonymity or pseudonymity often emboldens users to be nasty and to make comments they would not in face-to-face exchanges (Fost, 2007; Noveck, 2007; Simpson, 2005). Reader vitriol in 2006 led the Washington Post to discontinue accepting comments from readers on its ombudsman’s blog (Seeley, 2006a). Because many chats are no longer monitored, the chances are greater than with traditional media that inflammatory or crisis- triggering comments will go unchecked.

Blogs have become fixtures in cyberspace that allow individuals to express personal and organizational opinions (Flynn, 2006; Holtz & Demopoulos, 2006; Kline & Burnstein, 2005; MacDougall, 2005; Reese, Rutiglianac, Kidek & Jaekwan, 2007). Blogs can be used to promote the blogger’s self-interest—such as Paris Hilton’s blog where the overly publicized actress appealed for public
forgiveness and leniency following a drunk driving conviction in 2007 (Mutter, 2007). However, many bloggers serve as astute and thoughtful observers and commentators on the public scene—and serve as third-party social influencers on various topics in the same way that the press was believed to accord explicit or implicit third-party endorsements (Gillin, 2007; Lenhart & Fox, 2006). Soldiers have even used blogs to share their experience in war (Burden, 2006). Although millions of blogs have been established, only about 20% of them are really active, i.e., updated at least quarterly (Green, 2007). Blogs are easily monitored by both organizations (Green, 2007; Nair, 2006a) and by news media (Dylko & Kosicki, 2006) through RSS (real simple syndication) software. Blogs have also become the source of revelations about missteps by government officials and media. For example, the Clinton-Lewinsky scandal made headlines in 1998 only after blogger Matt Drudge revealed Newsweek had “spiked” (withheld) the story. Similarly, Dan Rather resigned as news anchor after bloggers revealed CBS’s faulty sourcing in its coverage of President Bush’s military record (Nair, 2006a).

Hoaxes are also an unintended consequence of the free exchange of ideas in cyberspace. One small California company, for example, averted a crisis only because of its quick response following distribution of a fake news release announcing the company’s CEO had resigned, that the company was under investigation by the Securities and Exchange Commission, and that its earnings would be restated (Barney, 2000). Hoaxes also can involve spoof sites intended to parody or lampoon well-known people or organizations (Ossinger, 2006). Similarly, with the advent of collaborative media such as Wikipedia (Tapscott & Williams, 2006), so-called “dirty tricks” can be performed without any extensive knowledge of how the system works. Examples include the hoax played by a Tennessee businessman to alter John Seigenthaler Sr.’s biography in Wikipedia to falsely report that the former journalist and government official was involved in the assassination of John F. Kennedy and Seigenthaler’s former boss, Robert F. Kennedy (Goodin, 2005; Seigenthaler, 2005; Seelye, 2005). Other notable incidents involved their staffers altering biographical and other information on U.S. Senators (Wikinews investigates, 2006).

Rumors involve (often untrue) information passed on from user to user without verification of facts and without a verifiable source—and are particularly difficult to trace online (Kibby, 2005). One study suggests that at more than two-thirds of publicly held companies have been targets of rumors in Web-based chats or bulletin boards and that half of these companies have received queries about information or rumors appearing in chat or message board threads (Ryan, 2004). Among major brands that have been the targets of crisis-triggering rumors during the past decade are Procter and Gamble, Tommy Hilfiger, Kentucky Fried Chicken, Nieman Marcus, Microsoft and Costa Rican bananas (Fearn-Banks, 2007, pp. 95–99).

**Attacks.** Rumors can be shared unwittingly by users who believe the information to be true, but many rumors and uncorroborated information is circulated by people who purposely want to point out misbehaviors or to defame others. Attack Web sites were created as early as 1996 when critics of Ford Motor Company created a Web site called FlamingFords.com and activists created an anti-McDonald’s Web site called Msconcept.org (Middleberg, 1996). Similar feuds continue today targeting large companies such as Coca-Cola (Coombs, 2007, p. 31) and Wal-Mart (Fearn-Banks, 2007, p. 7; Kabel, 2006).

Although trademark laws in many countries dissuade detractors from using organization’s names in site addresses, attack Web sites proliferate. Many of these homosite derivatives add the suffix “-sucks.com” to their names (Farrell, 2000). Other rogue sites carefully select Web site names or addresses that sound deceptively similar to the names or Web addresses of targeted organizations (Fearn-Banks, 2002, 2007; Hallahan, 2004b; Holtz, 2002, pp. 291–305; Phillips, 2001). A goal is to distract gullible users searching for legitimate sites on search engines (Pelline, 1997). Attack, spoof and rogue sites have augmented with through the creation of heavily trafficked public complaint or gripe sites where individuals can vent against specific companies (Appleman, 2001). Complaints illustrated with videos also appear on YouTube (Hart, 2006).
Attack and rogue sites, as well as *cybersmears* (Cázarzé, 2002; Crawford, 1999) and hate e-mail (Barnes, 2003, pp. 262; Levin, 2002), underscore the important role that new media have assumed in politics, the discussion of public issues and the exercise of power in modern societies. One study found that almost two-thirds of online community members involved in social issues through the Internet say those issues were new to them when they began participating on the Internet. More than 40% of online community members reported they participate more in social activism since they started participating in online communities (USC Annenberg Digital Future Project, 2007).

Politics has been transformed by the Internet (Chadwick, 2006; Klotz, 2001) with the advent of candidate and issue Web sites and e-mail (Valla, 2007), streaming video and Webcasts (Fine, 2006), sponsored and independent blogs (Craig, 2007; MacDougall, 2005; Schatz, 2007) and social networking sites where voters can exchange ideas with candidates and others (Vargas, 2007a; Seelye, 2007). As result, new specialists have emerged: online political operatives (OPOs) and online political advertising consultants (Vargas, 2007b, c).

Not surprisingly, social activists such as MoveOn.Org have gained notoriety for their use of new media, while groups such as NetAction.Org specialize in training activists on Internet strategies and tactics in the tradition of radical community organizer Saul Alinsky. Cyberactivists use distributed networks (Arquilla & Ronfeldt, 1998) to advance their cause, enlist followers, and affect legislation and the public affairs agenda (Kolko, 2003; Lerbinger, 2006; Nelson, 2006). They also strive to effect organizational and social change more generally (Brabbs, 2000; Coombs & Holladay, 2007, pp. 70–73; Cyberadvocacy, 2000; Ford & Gill, 2001; Gillespie, 2000; Harkinson, 2001; Hick & McNutt, 2002; Hill & Hughes, 1998; Holtz, 2002; Kim & Shin, 2004; Meisner, 2000; Now, a gaddy, 2000; Rauch, 2006; Thomas, 2003; Turnbull, 2001; Youngblood, 2006). Online movements are especially evident at the global level (Bennett, 2003; Dartnell, 2006; Hick, Hapin & Hoskins, 2000; Rogers, 2003; Warkentin, 2001) and include use of new media by marginalized groups (Mitra, 2004; O’Donnell, 2001) as well as groups characterized as outright anarchists (Atton, 2002; Whissent, 2000).

How should organizations respond (Shortman, 2003)? The rise of cyberactivism has led to the development of models for classifying cyber attacks (Ye, Newman & Farley, 2005/2006) and assessing and prioritizing online threats from an issues management perspective (Coombs, 2002). While some argue that it is possible for organization to control or create a symbolic "space" in which to address cybercritics (Courtright, 2007; Kent & Taylor, 1998; Smudde, 2005), others argue all online crises are political and thus an "enemy" is involved inevitably (Chrysler CEO rips, 2002; Dezenhall & Webber, 2007). The result is a combative mentality punctuated with metaphors such as firefighting (O’Keefe, 1997, pp. 341–369), cyberwarfare (Aftab, 2005) and nail ‘em! (Dezenhall 2003, pp. 156–168).

The trend has also focused attention on the online techniques used by activists groups to maximize their advantage and their use of new media. Researchers have examined the use of *message framing* by activists (e.g., Collins, Zoch & Walsh, 2005), *dialogic communications* (Taylor, Kent & White, 2001) and *hate language* (Barnes, 2003, p. 262; Levin, 2002). As an example, see Allen et al. (chapter 22, this volume).

**RISK RESPONSES**

The rise of cyberactivism underscores the reality that these new media provide a readily accessible channel for people to respond to risks, which are defined here as perceived hazards or threats to a person’s physical, psychological, social, political or economic well-being. With increasing frequency, the public turns to the Internet or cell phones to learn details of crisis-and risk-related events. Members of the general public with little or no prior involvement with responsible organizations attempt to find out what happened, how organizations are responding, and how the consequences might affect their lives. More involved publics—people with whom the organization has established
relationships, goodwill and trust—might use new media to reconcile new information with their extant knowledge.

Beyond crises, users also rely on new media to cope with routine problems in their lives. The Internet and cell phones thus operate as risk management tools that are readily available and convenient. Various private, not-for-profit and governmental agencies also use the Internet and related media in risk education programs. A good example is the Ready.Gov Web site, where the federal government promotes personal emergency preparedness to adults and kids (Coombs & Holladay, 2007, pp. 96–97). Campaign designers increasingly integrate new media into public information programs and have developed an emerging body of knowledge about successful strategies and tactics (Bortree, 2007; Lieberman, 2001).

In managing personal risks generally, people engage in both information-seeking and information sharing. Situational theory, which has been widely studied in public relations, posits that people will engage in active information seeking (vs. passive information processing) when confronted with a problem—particularly when problem recognition and cognitive involvement are high and constraint recognition is low (Grunig, 1997). Publics are formed around issues as people share ideas, opinions and emotions with others. New media facilitate this process by making it easy to find information and by linking together people separated by geographic distance. Other theorists rely upon structuration theory to suggest that very process of collaborating online can create publics or social organizations. Electronic environments allow people to communicate freely in an unregulated, uncensored, public environment (Cozier & Wittmer, 2001). The result has been referred to as communities (Feenberg & Barney, 2004; Hallahan, 2004c; Rheingold, 1993), networks (Castells, 2000) and, most recently, social networking..

Information-Seeking

When confronted with uncertainty, people either avoid or seek information (Case, Andrews, Johnson & Allard, 2005; Palenchar & Heath, 2007, p. 125; Seeger, Vennette, Ulmer & Sellnow, 2002). One obvious source of information is the traditional media, which have been augmented with Web sites mobile phone services operated by newspapers, magazines and broadcasters as well the growing array of other online news aggregators such as Yahoo! News, Digg, Reddit and Slashdot and specialized news sources. For example, Al Jazeera, the independent Arab television network based in Qatar, operates an English language Web site as a way to present an alternative Arab perspective to English speakers worldwide (Auter, 2006).

The late 1990s saw heavy public reliance on the Web for news about the death of Princess Diana in 1997 (Sorkin, 1997, Tedesco, 1997), the Clinton-Lewinsky scandal (Rosen, 1998/1999; White House crisis, 1998), and the Kosovo war (Guensburg, 1999; Malushi, 1999).

The 9/11 attacks in 2001 were seminal events that demonstrated the power of the Web to supply news to people facing risk (Blair, 2002; Martin & Phelan, 2003; Palser, 2002; Rappaport & Alleman, 2003; Seeger, Vennette, Ulmer & Sellnow, 2002; Vengerfeldt, 2003). Although not the initial source of information (Kaniljan & Gale, 2003) and despite delays by newspapers in covering the event on their Web sites (Randle, Deveport & Bosson, 2003; Salaverria, 2005), nearly one-third of Americans went online to search for information (Rainie, 2001). Many users found the Internet a superior source compared to traditional media (Jones & Rainie, 2002; Kellner, 2004; Spence et al., 2006). Topics searched online closely paralleled topics covered in traditional media (Aikat, 2005; Frith & Aikat, 2003). Internet use led to a greater connectedness and a broader range of civic activities following 9/11 (Kim, Jung, Cohen & Ball-Rokeach, 2004), and people who participated in online discussions also were more likely to participate in similar community activities offline (Dutta-Berman, 2006).

Web search engines are used by roughly one-fifth of Americans on a typical day and allow users to readily locate virtually any topic available in text, image, audio or visual formats (Fallows, 2005; Rainie, 2005). When searching for health information online, most users begin with search
information with their
effects in their lives. The
dily available and con-
new federal (Coombs & Holladay,
10to public information
tsful strategies and tac-
t-seeking and informa-
tions, poits that people
when confronted
 Yönetim are high and
s as people share
s by making it easy to
Other theorists
line can create publics
freely in an unregu-
as been referred to as
1), networks (Castells,

Case, Andrews, John-
ser & Sellnow, 2002).
mented with Web
sters as well the grow-
ddit and Slashdot and
vision network based
ative Arab perspective

veal of Princess Diana
en, 1998/1999; White
r of the Web to supply
2; Rappoport & Alle-
though not the initial
ers in covering the
n, nearly one-third of
found the Internet a
liner, 2004; Spence et
itional media (Aitkroader range of civic
ople who participated
ity activities offline

cal day and allow us-
ual formats (Fallows,
zers begin with search

engines; 80% of Americans have used search engines to search on at least 1 of 17 health topics (Fox,
2006). At the same time, 36% of online adults consult Wikipedia (Rainie & Tancer, 2007) for vari-
ut topics.

Today, 1 out of 6 Americans accesses news online. But among "high powered" Internet users
(defined as active users with broadband connections) more than 70% go online for news in a typical
day (Horrigan, 2006). Alternatively, users can go directly to organizations that are covered in the
media. Today, organizations use direct communication to bypass media (Hallahan, 1994) and can
incorporate a variety of tools—blogs, transcripts, e-mail messages and links to search engines—to
counterbalance negative publicity received in the mainstream press (Seelye, 2006).

Emerging evidence suggests that online news complements rather than displaces traditional
news consumption (Dutta-Bergman, 2004). Users are more likely to follow their own interests
(Tewksbury, 2003) and employ selective exposure when seeking utilitarian information (Knobloch-
Westerwick, Carpenter, Blumhoff & Nickell, 2005) or topics involving political opinion (Best,
Chmielewski & Krueger, 2005). Researchers have conducted analyses of how online (versus tra-
ditional) media cover such highly visible risks as severe acute respiratory syndrome (SARS—Lee,
2005a, b; Tian & Stewart, 2005), genetic cloning (Hyde, 2006), and the Iraq War (Dimitrova, Kaid,
Williams & Trammell, 2005; Schwabbe, 2006).

Online news is considered rich in mobilizing information, i.e., supplying information that aids
people to act on attitudes they already hold. However, evidence suggests the amount of mobilizing
information is no higher in online versus traditional news (Hoffman, 2006). Other research suggests
the availability of mobilizing information does not lead to risk avoidance (Samarajiva, 2004).

Information Sharing

Responses to major disasters covered in the news illustrate the interactive nature of new media,
which enables users to both receive and create content shared with others. Indeed, the web has be-

come a coping mechanism (Associated Press, 2007a).

The 2004 Indonesia tsunami prompted numerous tourists and residents to post messages on
both text and video blogs (vlogs)—and was considered a breakthrough event for consumer-generated
content and for citizen journalism on the Web—a trend that had begun the previous year in
the wake of Hurricane Fran on east coast of the United States (Palser, 2004). (Subsequently, many
mainstream media adopted crowdsourcing to encourage audiences to submit images and informa-
tion via the Internet and cell phones.) As had been evidenced in earlier disasters, people displaced
by the tsunami and Hurricane Katrina in 2005 used the Internet to search for survivors and regain
or maintain contacts with friends and family (Dewar, 2005; Hafner, 2005; Moore, 2005; Regaldo
& Mintz, 2005; Schwartz, 2004, 2005). The process was facilitated by the quick establishment of
cybercafes in the devastated areas (Internet café, 2005; Katrina public web, 2005). Public access
terminals were augmented with the Web-based tracing services operated by entities such as the Red
Cross to help locate missing persons. Research documents how online communities can emerge
following news or a disaster such as the Gujarat earthquake in India (Kodrich & Laituri, 2005) and
Hurricane Katrina (Procopio & Procopio, 2007).

Online information sharing is popular because many people are interested in establishing a
personal presence or identity on the Web (Hunt, 1996; Killoran, 1999) and are not reticent to share
personal information or assist others. To illustrate, user Juan Mann posted a clip on YouTube offer-
ing "Free Hugs" to strangers. Meanwhile, user Ryan Fitzgerald offered to talk to anyone who called
him on his cell phone—an offer to which 5,000 people responded (Associated Press, 2007b).

Discussion boards, chats and blogs that enable readers to add comments are devoted to a my-
riad of special topics—including how people can avoid or solve problems with products or services.
Other personal problems about which people freely share information range from dating and sexual
relationships to parenting, grieving and debt management (Leland, 2007).

Health and nutrition are areas where new media have been particularly important in helping
people manage risk. Telemedicine encompasses a wide range of activities from emergency triage to long-distance diagnosis by physicians and transmission of medical images and data (Turner, 2003). Among its most important applications, however, are disease prevention, public health education, and relationship building between medical providers and patients and at-risk populations (Springton & Laricey, 2003, p. 551). People increasingly engage in self-diagnosis and obtain information before and after consulting physicians from medical Web sites such as the pioneering Medscape.com (Tanne, 1999) and WebMD (Stoltz, 2006), as well as Web sites operated by nonprofit and governmental agencies, medical providers and insurers interested in promoting wellness (Weintraub, 2006).

Online patient groups have become important components in health care by serving as channels for social support and research (Landro, 2007). Discussion boards and chats operate as online health communities devoted to a broad range of topics (Maloney-Krichman & Freeno, 2001). Recent research about online health groups has focused on information sharing about topics such as bovine spongiform encephalopathy or “mad cow disease” (Richardson, 2001), sleeping disorders (Weisgerber, 2004), syphilis and HIV (Anderton & Valdiserri, 2005; McFarlane, Bull & Reitmeier, 2002; Shenoff, 2006), vegan diets (Sneijder & Te Molder, 2005), and alcoholism (VanLear, Sheedhan, Withers & Walker, 2005). For a general discussion about the analysis of computer-mediated discourse, see Herring (2001).

Consumer preferences for user-generated content (also known as consumer-generated media) explain the vital role of interactive Web 2.0. More than one-quarter of online consumers now submit a rating or review or a product or service or contribute to a discussion board (Haven, 2007), and one-half of users are either creators or readers or such comments (Parr, 2007). User-generated content drives many of the fastest growing Web sites such as MySpace, Facebook and You Tube (Burns, 2006; Never Ending Friendship, 2006)—a trend expected to continue on the Web (In-Stat, 2006) and to expand to mobile phones (Stone & Richtel, 2007). This same trend is expected to continue in the arena of user-generated news with sites such as Digg.com and Reddit.com (comScore Media Matrix, 2006).

Research consistently suggests that consumers prefer obtaining information from peers online (Altsch, 2007; Leggatt, 2007). In the case of online news, for example, users employ the same criteria to assess online and traditional news stories (Sundar, 1999). However, experimental research showed the same stories were more liked and perceived to be of higher quality when attributed to other users compared to stories attributed to news editors, computers or the user himself/herself (Sundar & Ness, 2001). Beyond user satisfaction, research suggests that collaboration enhances article quality in Wikipedia (Wilkinson & Huberman, 2007).

RISKS CREATED IN CYBERSPACE

Both individuals and organizations now find themselves coping with a variety of new risks that did not exist prior to the advent of cyber-communications. Although many of these risks do not involve triggering events associated with a crisis, they can create levels of uncertainty and disruption in the lives of people and entities.

Risks for Individuals

People express concerns about various aspects of using the Internet. This has been demonstrated in a personality trait labeled Internet anxiety, a special case of fears or concerns about a person’s ability to successfully use computers (Joiner et al., 2005; Joiner, Duffield, Gavin & Maras, 2007; White & Scheb, 2000; Zhang & Zhang, 2002). More specifically, however, six key risks exist for individuals in cyberspace.

Disclosure risk involves the embarrassing revelation—whether accidental or intentional—of
mailings, postings or other information that reveal indiscretions, unethical behaviors or character shortcomings (O’Hara, 2006). The misstep might have occurred years ago, but survives in electronic files only to be released due to a lack of system security (Barr, 2006; Pagararo, 2007; Zambroski, 2006) or due to the deliberate actions of others (Greenhouse & Barbaro, 2006). Former U.S. Representative Mark Foley and BP chief executive John Browne are two examples of prominent people ousted from positions of power because of sexual scandals (Jesdav, 2006; Kidman, 2007). For ordinary individuals, current and prospective employers enjoy easy access to a wealth of information through organizational intranets and e-mails, personal Web pages, chats, bulletin boards and blogs. Information has been used by employers to terminate present or avoid hiring potential employees (Dell & Cullen, 2006; Lambert et al., 2005; Nashashima, 2007; Stone, 2006). These reference checks are facilitated by search engines, for-profit services (Hart, 2007), and Web sites where people can complain about the misbehavior of others (Alvarez, 2006; Saranow, 2007).

Deception risk involves not knowing the sources of information or being able to easily verify information. Deception can be as simple of misunderstanding content, but often involves information that is deliberately incomplete or fragmentary. Today’s users must become cyber-literate to assess the veracity of online content. Deception also includes the use of devices that distract attention—including pop-ups and spam (Palmer, 2006). Purposeful deception takes various forms (Hallahan, 2006). Examples include digital manipulation of images (Hafner, 2004), and schemes to gain more prominent listings on search engines (a technique euphemistically referred to as search engine optimization). Other recent examples include anonymous self-serving attacks on competitors (Kesmodel & Wilkie, 2007; White, Lubline & Kesmodel, 2007), fake blogs or flogs (Barabaro, 2006; Siebert, 2006), astroturfing or the use of fake grassroots campaigns and front organizations (Ahrens, 2007; Greenberg, 2007), fake ads for fictional characters on MySpace.com (Holmes, 2006), and anonymous video postings (Regalado & Scarrow, 2006).

Crime risk involves deception aimed at extracting economic, political or other losses from users, particularly vulnerable groups such as seniors and youth (Dibble, 1998). One private study suggests that 86% of targeted cyberattacks are aimed at consumers (Richmond, 2006). According to the FBI, auction fraud was the most commonly reported online offense, followed by non-delivered merchandise-payments (Federal Bureau of Investigation, 2007). Other swindles include e-mail scams such as the infamous Nigerian mail scam (Fearn-Banks, 2007, pp. 5–6) and fake online appeals that have become commonplace after major disasters (Gray, 2005; Krebs & Mayer, 2005).

Although the problem is actually more pervasive offline than online, identity theft is a growing concern (Bryan-Low, 2005; Cullen, 2007; Ellis, 2006; Mattioli, 2006; Nierengarten, 2006; Swartz, 2005; Vaca, 2003; Vascecellaro, 2005b). Among techniques commonly used to obtain valuable details about individuals are phishing—sending e-mails from fictitious but familiar- or official-sounding e-mail addresses that instruct people to buy online or disclosure personal information (Shin, 2007). A variation of this scam is vishing, which requires online users to leave a voice mail message on the telephone (LaValle, 2006). Other techniques involve spyware or adware (including "empty spam" messages) where thieves embed software in users’ computers without the users’ knowledge to capture keystrokes or passwords (Elgin, 2006; Hallahan, 2004; Krebs, 2006; Zeller, 2006).

Other examples include outright deception, such as the major electronic retailer found to operate an intranet that mimicked sites of major competitors to show customers competitive prices—only the prices shown were deliberately inaccurate and equal to higher than the store’s prices (Gombossy, 2007). Separately, government officials are concerned about consumer protection issues more generally and trafficking in illegal commodities. A particular problem involves the purchase of unauthorized pharmaceuticals and the safety of Internet pharmacies (Fox, 2004; U.S. General Accounting Office, 2004). Securities regulators are concerned about trading losses by “day trading” among investors and stock manipulation in penny stocks and other equities (Nakashima, 2007b).
Research in marketing has focused on the question of risk-taking and trust in e-commerce. With the expanded use of secure transaction and online payment systems (Grow, 2006), researchers have explored on issues such as development of trustworthy systems (Schaffer, 2004; Whitworth and De Moor, 2003), warranties (Lwin & Williams, 2006) and social aspects of online shopping (Blake, Valdiserri, Neuendorf, & Powers, 2006). In particular, e-marketers have strived to develop a conceptual understanding as well as scales to measure online trust (Camp, 2001; Eggert, 2006; Fogg, 2003; Forsythe, Liu, Shannon & Gardner, 2006; Garbarino & Strailevitz, 2004; Lacohee, Phippen & Fennell, 2006; Littler & Melanthiou, 2006).

Privacy risk is the largest single concern among online users (Hallahan, 2006; Holtzman, 2006). About two-thirds of Americans say they don’t trust Web sites even if the site has a posted privacy policy (Jumarkar, 2002). In the late 1990s, problems with disclosure of personal information led to major problems for computer giants such as AOL and DoubleClick (Crisis Rx, 2000; This just in, 1997) and resulted in the establishment of guidelines by the Direct Marketing Association and other trade groups (Hallahan, 2006). Although privacy disclosures are valuable, research has raised questions about their effectiveness because such notices are often ignored by users (Milne & Culnan, 2004). Many leading American technology companies favor passage of a stronger privacy laws at the federal level to avoid an emerging crazy-quilt of discrepant state rules (Hart, 2006).

New forms of privacy invasion continuously emerge. One example is the easy accessibility of satellite imagery, such as Google’s Street View, that depicts the details of neighbors, streets, and public buildings—down to people’s backyards (Helft, 2007). The privacy problem has been confounded in the United States by the Bush administration’s position that it was authorized to engage in surveillance of suspected terrorists without warrants or other oversight under the 2006 renewal of the USA Patriot Act adopted following the 9/11 attacks (Eggen, 2007; Risen & Lichtblau, 2005). Meanwhile, government Web sites are tracking visits to U.S. government sites in violation of the 2003 government directive (McCullagh, 2006) and engage in data mining activities without oversight (Lichtblau, 2005; Nakishima, 2007a).

Addiction risk involves an array of allegedly compulsive or anti-social behaviors involving Internet use—including excessive time spent online overall, game playing, viewing pornography, pathological behaviors in chatrooms, and gambling (Grohol, 2005). Internet addiction disorder was labeled by Dr. Ivan Goldberg as a spoof in 1995, but received serious attention in response to growing concerns about the impact of the new medium as it was quickly adopted. More than 20 research articles and several books were published in the late 1990s. (For a review of the current state of research, see Yellowies & Marks, 2007.)

Alternative explanations for addiction can be found in communications research suggesting that users merely attempt to manage impressions online (O’Sullivan, 2000), or lose their anchor to reality as they become engrossed in the flow of the online activity (Webster, Trevino & Ryan, 1993) and to abandon or lose their sense of personal identity (Simpson, 2005; Walther, 1996; Walther & Tidwell, 1992). Such behaviors might be explained by the more limited nonverbal and social cues associated with online communications (Barnes, 2003).

At least three research centers operate in the United States and China to study or treat the malady, and but researchers are sharply divided on the question. Dr. Kimberly Young of the Center for Internet Addiction (www.netaddiction.com) has pushed for inclusion of IAD in the 2012 revision of the American Psychiatric Association’s Diagnostic and Statistical Manual of Mental Disorders. However, in separate actions in 2007, the American Society of Addiction Medicine opposed calling overuse of Internet and video games a true addiction and the American Medical Association called for further research on video game overuse (Internet addiction disorder, 2007; Video games no addiction for now, 2007).

Exploitation risk involves users being taken advantage of, including the prospect if incurring physical harm. Critics argue that the rise of new technologies, particularly the easy access to por-
t in e-commerce. With 06), researchers have
04; Whitworth and De line shopping (Blake, ved to develop a con-
; Eggert, 2006; Fogg,
04; Lacoohe, Phippen
an, 2006; Holtzman,
the site has a posted are of personal infor-
Click (Crisis Rx, the Direct Marketing
usions are valuable,
are often ignored by nies favor passage of
lt of discrepant state
easy accessibility of neighbors, streets, and oblem has been con-
der the 2006 renewal
n & Lichtblau, 2005).
es in violation of the tivities without over-
baviors involving viewing pornography, addiction disorder was
in response to grow-
more than 20 research f the current state of
research suggesting r lose their anchor to
ino & Ryan, 1993) er, 1996; Walther & erbal and social cues
tudy or treat the Young of the Center in the 2012 revision of Mental Disorders.
al Association called Video games no ad-
prospect if incurring e easy access to por-
nography, has perpetuated a culture created by the mass media that promotes abuse, exploitation and violence against women and children, both online and offline (Gillespie, 2000). In addition to perpetuating a culture where women are objectified and marginalized, teenage and adult women can be tracked online by cyberstalkers who engage in harassing and sometimes aggressive behavior (Jenkins, 2007; Hallahan, 2004b). Importantly, women have used also deployed the Internet as an advocacy tool to overcome such abuses (Passariello, Johnson & Vranica, 2007).

Children are vulnerable to cyberbullying by peers (Willard, 2007), deception by commercial concerns related to products sold online, and sexual exploitation. Children are especially at risk because they are frequently incapable of making judgments about the appropriateness of age-related content, the veracity of information, or the identity and truthfulness of sources (Holloway & Valentine, 2003; Shade, 2002). Easily lured into exhilarating Web sites and chatrooms filled with pornographic content (Zimmer & Hunter, 2003), one in five children report having received unwanted sexual solicitations online. The exploitation problem has been exacerbated with the emergence of social networking sites, where 55% of online users have created online profiles (Lenhart & Madden, 2007; Zeller, 2005). Teens generally are not shy about disclosing the most intimate personal insights about themselves (Nussbaum, 2007), and both Facebook and MySpace have been forced to restrict disclosures of about online activity and personal identifying information (PII) by members (Hansell, 2006; Nogouchi, 2006). Fortunately, higher levels of risk perception among teens appear to lead to less willingness to provide information (Yuom, 2005). Laws have been passed by virtually every major western industrial nation outlawing the trafficking or possession of child pornography in efforts to eliminate child abuse by pornographers. Several online public information campaigns against sexual abuse and pedophilia have been launched by advocacy groups (Arnoldo, 2001; Coombs & Holladay, 2007, pp. 94–95).

Exclusion risk involves risks related to having no or only limited access to Internet or cellular communications and thus not being able to fully participate in society. The problem of the “digital divide” between information-haves and have-nots places individuals at risk of not having access to information that might be required as a matter of right or might be required, for example, in order to vote or conduct business with government (Coulthy, 2004; Dance, 2003; Hindman, 2000; James, 2003; Kuttan, 2003). The potential societal risks are unintended knowledge gaps among people in society (see Newirth, chapter 20, this volume)—a social threat that has led some critics to call for universal access for all Americans.

The digital divide in the United States and globally is largely an artifact of socio-economic factors. Yet others would contend it is also a matter of personal choice. One recent study proposed and found significant support among experts for a scenario in which, by 2020, people left behind by accelerating information and technologies might form a new cultural group of technological “refuseniks” who self-segregate and commit acts of terror or violence in protest against technology (Anderson & Rainie, 2006, pp. 59–66). Thus, the elimination of disparities is an important social concern for both disenfranchised individuals as well as society as a whole.

Risks for Organizations

Organizations engaged in e-commerce and other types of exchanges such as fund-raising confront unique problems stemming from their limited knowledge of the people with whom they are dealing in cyberspace (Halpern & Mehrotra, 2000). While fraud is the most egregious concern, other examples abound. Individual investors can now lend money to others via sites such as Prosper.com (Kim, 2007). Businesses also can lose control of information about products—witness the leaks related to content of the final Harry Potter novel prior to its official release in 2007 (Trachtenberg & DeAvila, 2007).

Janal (1998) was the first book author to focus attention on the reputation-related risks to organizations in the new world of online communications. Hallahan (2004b) later focused on the need
to protect an organization's digital assets and argued that organizations confront risks from five principal sources: attackers, hackers, lurkers, rogues and thieves. He also outlined the ethical and legal problems confronting organizations (Hallahan, 2006).

Importantly, many risks for organizations have the potential to escalate into full-blown crises but never do so. An error by an employee in the Alaska Department of Revenue, for example, led to the deletion of all computerized records related to the $38 billion Alaska Permanent Fund. However, officials were able to reconstruct the files from 300 cardboard boxes of paper records, and public concern was minimized (Oops!, 2007).

Cyber-risk containment for organizations requires a combination of engineering, enforcement, education and encouragement.

**Engineering.** One study in 2001 by Jupiter Media Matrix found that 70% of companies surveyed described their level of cyber-risk as "low" or "medium" (Statemen, 2001). Since then organizations have invested heavily in enhanced computer security systems in the aftermath of 9/11 (Held, 2002; Kliem, 2003; Sager, 2001; Schwartz, 2002). Nonetheless, a Conference Board report five years later found that the United States was poorly prepared for a major disruption of the Internet (Vara, 2006a). Particularly vulnerable are the most popular Web sites (Larkin, 2007; Goo, 2007), colleges (Markelein, 2006) and the federal government (GAO says, 2004; Gross, 2007; U.S. General Accounting Office, 2005). The nation's goal is to avoid the nationwide cyber attack that crippled governmental, financial, media and corporate Web sites in Estonia in Spring 2007 (Rhoads, 2007).

**Enforcement.** Enforcement includes the establishment and pursuit of consistent organizational policies regarding communications technology practices (Flynn, 2001). Managers need to establish routine Web site and related audits to determine both the extent of holdings and potential risk vulnerabilities (Hallahan, 2004b). This requires melding physical security and information security functions—a task sometimes difficult (Vara, 2006b). Organizations must be vigilant in pressing criminal and civil charges against perpetrators of crime who pose risks (Goldfarb, 2006). Plagiarism appears to be increasing (Goldborough, 2004), along with brandjacking. The latter involves fraud, counterfeiting and other abuses against businesses such as cybersquatting (Klapper, 2006), false association, pay-to-click (PTC) fraud, domain kiting or tasting, objectionable content, unauthorized sales channels, and phishing (MarkMonitor, 2007). Legal remedies are often difficult because of jurisdictional differences across cyberspace (Bryan-Low, 2007; Hallahan, 2004b, 2006).

**Education.** Education requires enlightening users of an organization’s systems about potential risks. Responsibility begins with organizational directors who must be increasingly involved in policy pertaining to risk-related issues (Hicks, 2001; Vispoii, 2006). Employees and others must be instructed about potential risks and scams, such as cyber-blackmail (Argenti & Forman, 2003; Warner, 2003). Security experts note that employees create significant risks for organizations through misdeeds or misjudgments. Many staffers are unwittingly duped by hackers who use social engineering to gain the confidence of staff while extracting seemingly innocuous information or cooperation (Brandt, 2006; Totty, 2006). Particular problems for business involve the unintended disclosure of proprietary information or trade secrets to lurking competitors engaged in legal competitive intelligence or illegal industrial espionage. Publicly traded firms also must be watchful to avoid the premature release of material information that might influence investors’ purchase or sale of equities without providing for prompt and full disclosure to all investors as required under federal securities laws (Hallahan, 2006). All types of organizations must be concerned about the violation of various privacy laws pertaining to employees, customers, students, and patients and creditors. Many educational and membership organizations face a particular challenge in enlisting cooperation from users over whom those organizations exercise little control (Marklein, 2006).
Encouragement. Encouragement includes enhancing the self-efficacy of organizations and users to show they can make a difference in containing cyber-risks. Among the most important efforts in this arena are efforts for large complex organizations to develop crisis plans that encourage risk containment (Andrijevic & Horowitz, 2006; Vijayan, 2004). Various major corporate insurance underwriters have developed actuarial models of cyber-risks and encourage best practices as part of offering cyberliability insurance (Boyle, 2000; Lindhe, 2000; Mukhopadhyray, Saha, Chakrabarti, Mahanti, & Podder, 2005). Beyond education about risk avoidance, an organization’s users must understand the importance of risk reduction. Organizations can facilitate this process by developing usable systems (Hallahan, 2001b; Kesmodel, 2006) that foster self-efficacy among users. Risk reduction can be further encouraged through public policies that encourage investment and incentives so organizations manage and discourage cyber-risks (Gross, 2007; Krebs 2007a, b).

CONCLUDING OBSERVATIONS

This review suggests that people’s uses of new communications technologies have undergone significant changes over past decade. No one quite knows for certain how the Internet will evolve, despite the best prognostications by experts (see Anderson & Rainie, 2005). New applications, new technologies and new concerns will undoubtedly emerge.

Not surprisingly, the study of crises and risks in the context of cyberspace is an emerging field that blends research on crises and risk with the emerging field of informatics (how people use computers) and captology (the use of computers as persuasive technologies; Fogg, 2003). In keeping with Coombs’ (1996) observation about the state of crisis communications in general, more conceptual and empirically-based investigation is required.

Despite these changing circumstances, it is clear that new technologies have much to offer organizations and individuals as resources in dealing with crises and risks. This is particularly true for mobile communications devices, which are just now beginning to be exploited as organizational communication tools. This is also especially true for younger generations who have grown up as digital natives (vs. their elders, digital immigrants) and are fully comfortable with Internet and cellular technologies (Prensky, 1991). Generational differences are especially noteworthy in crisis and risk communication: A 2006 study showed that 20% of Americans overall relied on the Internet as their primary source of news and information about science. But, for adults ages 18–30, who also had broadband access at home, that figure was 44%—more than double (Horrigan, 2006).

Although lingering generational differences can be expected to conflate in coming years as the population ages, inconsistent patterns of use pose important implications for new technologies and for the communicators that reply upon them. Research suggests that while dependence on new media has increased, and considerable variation remains in the adoption and commitment to new media across user groups (Horrigan, 2007). For this reason, new media are not panaceas to all crisis and communications challenges—and cannot be examined out of context of a more integrated approach that also incorporates traditional media (see Neuwirth, chapter 20, this volume).

Experts agree that crisis and risk communicators must use both traditional and cyber media in order to be effective in creating the most effective messages and targeting and reaching key audiences most efficiently (Coombs, 2007, pp. 102, 171–172; Hallahan, 1994; Looker, Rockland & Taylor, 2007). Although using new technology is fashionable and organizations confront rising expectations about their technological prowess (Kazoleas & Teigan, 2006), evidence from a study of 2,847 global companies suggests that organizations are guarded in their investment in Web 2.0 technologies (McKinsey, 2007; see also Business crawls, 2007). Indeed for some entities, it might be appropriate to forego social pressures (Fianagin, 2000, White, Lublin & Kesmodel, 2007) to engage in the wholesale adoption of new technologies and to deploy these new tools selectively.

This discussion has focused on the implications of communications for crises and risk that might exist in the real world. Yet, as online experiences become a part of our everyday experiences,
it is not inconceivable to expect the emergence of virtual crisis and risk specialists whose roles will be to cope with incidents that take place entirely within the realm of cyberspace.

Consider the emergence of Second Life—the fantasy Web world where users create and act out life through avatars, or customized cartoon-like characters. More than 80 major brands have created (and paid for) a virtual presence in Second Life in order to reach the site’s more than 13 million visitors. Yet, the netizens of Second Life have crashed planes into the Nissan building, murdered customers going into the American Apparel retail store, plastered the NBC Universal logo on a S&M sex parlor, and vandalized the headquarters of then U.S. presidential candidate John Edwards. Such misdeeds are called “griefing” in Second Life parlance (Fass, 2007; Semuels, 2007). Nevertheless these incidents represent potential crises and risks that might need to be addressed by future virtual crisis and risk managers who undoubtedly will soon inhabit this virtual world.

REFERENCES


specialists whose roles will rspace.
re users create and act out major brands have created more than 13 million visi-
t building, murdered cus-

77, from http://www.econo-
SA Today. Retrieved August
aker, more prevalent. USA
or forums. USA Today. Re-
trieved February 13, 2007,
media agenda setting and to International Communi-
E-resistance in the case 3–145. 
porate press rooms in
Week. Retrieved March 22,
trieved February 20, 2006,
aging media work at Hur-
of cyber security risks re-
rial, 26(4), 907–923.
hington, DC: Pew Internet
et, 30(27), 14.
- McGraw-Hill.
ution, Communication &
ev23 April 23, 2007, from


Farrell, G. (2000, April 7). From sour grapes to online white. USA Today, pp. 1B–2B.


Holz, S. (1999). Public relations on the net. Winning strategies to inform and influence the media, the investment community, the government, the public and more. New York: AMACOM.
Holtz, S. (2002). *Public relations on the net. Winning strategies to inform and influence the media, the investment community, the government, the public and more* (2nd ed.). New York: AMACOM.


Now, a gadget can bite 24 hours a day (2000, January 24). Business Week, no. 3665, p. 150.
Now, a gadget can bite 24 hours a day (2000, January 24). Business Week, no. 3665, p. 150.
Palser, B. (2002, November). Not so bad: the performance of online news sites on September 11 was better than most reviews suggest. American Journalism Review, 24(9), 26–27.


This just in…. (1997, August/September). *Communication World*, 14(8), 62.


