3

Understanding and Managing Crises in an "Online World"

Sarah Kovoor-Misra
and Manavendra Misra

Given the pervasive use of online technology in conducting business today, it is important to understand the threats inherent in the online environment. The academic literature on crisis management has not sufficiently studied online forms of crises and their implications for crisis management. This paper discusses why the online environment creates vulnerabilities for organizations, the various forms of crises that may threaten organizations, strategies for crisis management, and implications for future research.

After the Bhopal and *Challenger* disasters in the 1980s, we have seen increased interest in the academic literature on the subject of crisis management. Crises are events, situations, or trends that can threaten the survival or goals of an organization (Nystrom & Starbuck, 1984). Researchers have provided key insights into the causes of crises and their manifestations, and have prescribed strategies for crisis management (Pearson & Mitroff, 1993).

The last 20 years have also seen radical changes in the business environment, particularly as it pertains to crisis management. The Internet has transformed business communications and operations and new forms of threats have emerged. In February 2000, for instance, a 14-year-old hacker from Montreal, Canada, using the screen name "MafiaBoy," launched denial-of-service attacks on some of the most prominent Web sites. He singlehandedly brought down the Web sites of companies such as Yahoo!, Amazon, eBay, Buy.com, E*Trade, Datek Online, and CNN. It is estimated that the resulting downtime at these companies caused more than $1.7 billion in damages.[1] At approximately the same time, a hacker named "Curador" claimed to have hacked into at least eight e-commerce sites and stole over 23,000 credit card numbers. He then proceeded to post these stolen numbers on his Web site (Borland, 2000).

These new threats are not only relevant for "pure play" online organizations (those that are totally reliant on the online medium for the delivery of their product or service) but also provide an avenue for attacking more traditional companies that may have an online presence (i.e., either a Web site or an online distribution channel). Today, many traditional brick-and-mortar organizations in banking, retailing, and education have established online operations. With the maturing of the Internet as a medium for conducting business, it is important to take stock of and understand the threats inherent in the online environment and how organizations can be better prepared to manage them.

The academic literature on crisis management, however, has not kept abreast with some of these changes. Relatively little attention has been paid to understanding the threats inherent in the online environment, the forms these threats may take, how they fit into existing categorizations of crises, and their implications for crisis management. In this chapter we seek to fill some of these gaps in the literature. The chapter examines why the online environment creates vulnerabilities for organizations. We discuss the various forms of online crises that have emerged and where they fit in existing crisis frameworks, and then suggest strategies for crisis management and directions for future research.

Threats in the Online Environment

Organizations differ in their reliance on the online environment for their business operations. There are "pure play" organizations such as Amazon.com that are totally reliant on the online medium for the delivery of their product or service. Other organizations may be "bricks and clicks" such as banks and stores that have traditional brick-and-mortar outlets but also use the Internet for offering their product or service. However, most organizations use online technology to communicate information and conduct day-to-day operations. In this section, we discuss some of the attributes of the online environment that create crisis vulnerability for organizations.

EASY ACCESSIBILITY, A DOUBLE-EDGED SWORD

The World Wide Web allows users anywhere in the world to have access to a company's Web site 24 hours a day. Geography and time are therefore not significant constraints to reaching customers. However, the same attribute that allows an organization to reach a worldwide audience also allows a malicious attack to be launched from geographically distant points at any time of the day. For example, the Mafiaboy attacks described before originated in Canada but overwhelmed a number of U.S.-based companies. In another case, May Day 2001 saw a number of attacks from Chinese activists against a number of U.S. government sites in order to protest the U.S. handling of the spy-plane-collision crisis. Furthermore, the cross-border nature of these incidents makes it very difficult for authorities in one country to pursue the perpetrators in another. For instance, the creator of the "Love Bug" virus could not be indicted, as there were no laws addressing computer attacks in the Philippines.[2] In contrast, for individuals to shut down all outlets of a large brick-and-mortar company, a significant amount of organization is needed to bring people to each physical location. Thus, geography can be a deterrent to physical threats for brick-and-mortar organizations. Organizations that rely on the online medium lack this deterrent.

CENTRALIZED OPERATIONS

Exacerbating the vulnerability of these organizations is the fact that online operations tend to be centralized. The Web sites run off servers located in one data center, which creates a single point of failure that may be exploited either inadvertently or maliciously. Even those companies that can afford multiple data centers typically have no more than a few. This means that any kind of an outage, whether a systems outage or a malicious attack, has the potential to prevent the company from generating any revenue from its online operations.

THE ARCHITECTURE OF THE INTERNET

In addition to centralized operations, many organizations with an online presence are vulnerable because of the architecture of the Internet itself. Since the Internet was designed as a research collaboration tool, it lacks significant security mechanisms built into it. Unlike the telephone network, where it is extremely difficult for an end-user to get access to the control components of the network, the Internet has both the transport and the control on a single network. All the control devices, such as routers and switches, are accessible by the same Internet Protocol (IP) addressing mechanism that a user uses to access Web servers. This means that a hacker could access devices on the Internet infrastructure and cause them to crash, in turn preventing a number of Web sites from being accessed.

HIGH VOLUMES OF CUSTOMER DATA

Unlike a brick-and-mortar retail store, where a customer can come in and anonymously buy products, the very nature of e-commerce results in Internet-based companies collecting a large volume of data on customers such as names, credit card numbers, and addresses. A large database of personal information that is also accessible to potential saboteurs anywhere in the world creates a vulnerability to crises. In January 2000, a hacker calling himself "Maxus" claimed to have stolen 350,000 credit card numbers from online store CD Universe and demanded $100,000 from the company in return for these numbers (Borland, 2000). Loss of sensitive customer data makes these organizations vulnerable to economic losses, a negative image, and potential legal liability.

24/7 OPERATION

Further compounding these problems is the fact that Internet-based organizations have little down time to solve problems that may occur in their systems. They are open to their customers 24 hours a day, 7 days a week. As a result, problem-solving becomes difficult as it is most often done while being operational. Brick-and-mortar companies, on the other hand, often have the luxury of addressing problems during off-hours.

HIGH VISIBILITY

Exacerbating all of these issues is the fact that operational problems in online organizations are also highly visible. If a site is down, for instance, that information is available to anyone tracking the site. In addition, the hype that has surrounded the Internet has resulted in inordinate media coverage of the "dot-coms." This has made it more attractive for hackers that are seeking attention or notoriety to make such companies targets of their attacks. The high visibility also affects how the investment community perceives the company. A major crisis can cause a severe drop in market capitalization for these organizations. For example, a June 1999 outage at eBay caused its stock price to drop by 20%.[3]

QUICK DISSEMINATION OF INFORMATION AND A WELL-CONNECTED CLIENTELE

The Internet medium also allows for the quick dissemination of information and the spread of rumors. Through mass mailings, chat groups, and fraudulent Web sites, rumors can be spread quickly and persist.

Caribou Coffee, for example, had to dispel a two-year-old rumor that it was linked to Islamic terrorists. This rumor cost them sales in the Jewish community. Procter and Gamble has also had to battle rumors that it is linked to Satan, as some individuals believed they saw the number 666 in the company's logo. Procter and Gamble subsequently changed its logo (Schmeltzer, 2004).

Furthermore, Internet organizations need to be vigilant as their consumers tend to be highly connected through e-mail as well as discussion and chat groups and dissatisfaction can spread quickly between them. To organize a grassroots boycott campaign against a major brick-and-mortar chain requires significant organizing capability and considerable time and resources. The connectedness of consumers in online organizations enables dissatisfied consumers to quickly put pressure on the organization to respond. In 1999, for instance, a lawsuit was filed by eToys against a group of artists who owned the etoy.com domain name. These artists, lacking the resources of the larger organization, launched a counterattack through the Internet called Toywar. Using e-mail, discussion groups, and Web sites, the small organization was able to mobilize thousands of activists from many countries in a concerted boycott and public-relations campaign against eToys. Finally, eToys was forced to drop the lawsuit.[4] The Toywar was a successful campaign because eToys was able to recruit numerous activists over the online medium.

HIGHLY MOTIVATED HACKER COMMUNITY

Unlike other industries, the online sector has associated with it a hacker community that is technologically savvy and motivated to identify flaws in the technology of these firms. These hackers are often driven by the need to gain attention or notoriety, or simply by the challenge of beating a well-designed technology system. Easy accessibility enables these individuals to demonstrate their technological expertise by bringing down a site. Unlike the brick-and-mortar world, where an organized group is often needed to do any harm, these hackers can single-handedly cause major damage. Most physical retail stores budget for a small amount of petty theft in the form of shoplifting, or "shrinkage" of inventory, but the damage here is akin to having shoplifters who can shut down the whole company on their own! The examples of Mafiaboy, Curador, and Maxus described above highlight these dangers.

To summarize, easy accessibility, centralized operations, insufficient built-in security in the Internet architecture, being open 24 hours a day and 7 days a week, high visibility, the quick dissemination of rumors, a connected Internet community, and motivated hackers all contribute to the crisis vulnerability of online organizations. In the next section, we examine various forms of crises that organizations with an online presence may experience, and we discuss those that are specific to online organizations and those that are shared with traditional organizations.

Forms of Online Crises

Crises may be caused by a combination of individual and organizational failures or by changes in an organization's environment that put pressure on the organization to respond (Hambrick & D'Aveni, 1988; Kovoor-Misra, Clair, & Bettenhausen, 2001; Pauchant & Mitroff, 1992; Shrivastava, 1987; Turner, 1976). For example, crises such as denial-of-service attacks can be attributed to insufficient security in the current technology of online organizations to differentiate between spurious and legitimate customer requests and individuals with malicious intent interested in attacking the organization. As another example, the deaths of many dot-coms, such as mvp.com, garden.com, and WebVan.com, can be attributed to their inability to compete in an increasingly resource-scarce environment.

Crises also tend to be multidimensional, with multiple crises present in the same situation, often with one crisis triggering others (Kovoor-Misra, 1995; Pearson & Mitroff, 1993). In the Napster crisis, for example, where the organization was being sued by the recording industry, the economic survival of the company was at stake, the organization's reputation was threatened, and the organization had to deal with the ensuing legal issues. When hackers attack an organization, it has to protect its technology and its reputation and minimize economic losses that could ensue. Thus, an organization is very often confronted with multiple crises that require attention.

Crises may take various forms. Researchers in crisis management have categorized the forms of crises that threaten traditional companies (Fink, 1986; Pearson & Mitroff, 1993). For example, crises may be classified based on whether they are technical-economic or human and social on one axis, and severe versus normal on another (Pearson & Mitroff, 1993). Another way of classifying crises is to categorize them by the dimension of the organization where their triggering causes originate or the dimension that they primarily impact (Kovoor-Misra, 1995). Thus, an organization may face technical, economic, human and social, legal, and political crises.

This same categorization scheme can be used to classify online crises. However, the examples of crises within each category may be different from those experienced by traditional organizations. Table 3.1 uses this scheme to highlight some general crises that online organizations share with traditional companies, and crises that are specific to them.

Below, we describe five of these crises: Web site failures, denial-of-service attacks, virtual blackmail and sabotage, virtual boycotts, and copyright and privacy issues that we believe are currently most salient to online

Table 3.1 Some Types of Crises for Online Organizations

Category	*General Crises (shared with traditional organizations)*	*Online Crises (specific to online organizations)*
1. Technical Crises (Caused by failures in the technology core or may impact it)	Loss of database	Web site failure
2. Human and Social Crises (Caused by people-related dysfunctions or may have serious consequences for individuals' psychological or physical health)	Workplace violence Strikes Bomb threats	Denial-of-service attacks Virtual blackmail
3. Public Relations Crises (Adversely affects the organizational reputation and relationship with external stakeholders)	Negative publicity	Negative publicity associated with online-specific crises
4. Legal Crises (Caused by perceived violation of the law)	Violations of relevant laws	Copyright and privacy violations (not specific to online organizations but currently salient)

organizations. We also describe how these crises trigger other crises. The extent to which any of these situations would rise to crisis potential would depend on their scope and impact. Crises, as we have indicated, are those situations that could threaten the survival or goals of an organization; hence, if these situations have serious economic, human, and social or reputational costs to the organization, they would be considered a crisis.

WEB SITE FAILURES

Web site failures are technical crises as failures occur in the technical core of online organizations. These failures may be due to a number of reasons, such as glitches in software or a poor system architectural design. Web sites in Internet-based organizations are also vulnerable to high volumes of traffic and problems with their external networks. Web traffic to the sites of online organizations tends to be highly cyclical and often unpredictable. There are cycles with well-defined peaks during the day, as well as cycles during the year. Since a number of e-commerce companies serve the gift market, they have significant peaks around gift-giving occasions. Toy sites, for instance, see tenfold jumps in traffic during the 6 weeks preceding Christmas. In 1999, almost every major e-commerce site had problems because they under-estimated the volume of traffic that they would receive. Toysrus.com, for instance, was overwhelmed by traffic generated by the mailing of their “big-book” of coupons that promised discounts to shoppers on the Web site. Most companies had to throttle traffic coming to their sites, resulting in large numbers of customers either not being able to access their site or seeing extremely slow page download times.[5] This resulted in the maturing of an industry niche in 2000. Service companies such as Mercury Interactive developed technologies to provide realistic load-testing of sites so that e-commerce sites could better prepare themselves for the upcoming peak season.

In addition, Web site problems for online organizations may also be precipitated because of problems in external networks that prevent customers from getting to their sites. In March 2001, for instance, the Yahoo! advanced services (Instant Messaging, Mail, MyYahoo) were unavailable for a day to a large section of the population because of a problem with a global-crossing router in Denver.

Web site outages for the prominent Internet-based organizations result in tremendous media scrutiny. Thus, the organization also must deal with the related public-relations issues and maintain customer confidence. In addition, inability to access Web sites also results in a loss of revenue and in some cases can significantly hurt the market valuation of a public company, as experienced by eBay and discussed earlier in the chapter.

DENIAL-OF-SERVICE ATTACKS

A denial-of-service attack is an example of a crisis in the human and social category. These crises are caused by individuals with malicious intent who bring down a company’s Web site. As we have noted, the accessibility of online organizations makes it relatively easy to attack a company’s Web servers from multiple machines that all generate spurious requests for Web pages. It is hard for the Web site to distinguish real requests from spurious requests. Real customers, therefore, start seeing slow response times, and eventually the servers crash. Companies with a single point of failure in any piece of their systems architecture are particularly susceptible to accidental or maliciously caused shutdowns at this “Achilles’ heel.”

In June 2004, Akamai, whose servers provide content distribution for the Web sites of Microsoft Corp., Google Inc., and Yahoo! Inc., experienced a denial-of-service attack that slowed down the Web sites of these companies (Associated Press, 2004). Denial-of-service attacks trigger Web site failures and public-relations issues as an organization’s technical vulnerabilities are exposed. Also, there may be a loss of revenue if customers are unable to access the Web site. The organization in these cases also has to work with law-enforcement agencies such as the FBI to track down these hackers.

VIRTUAL BLACKMAIL AND SABOTAGE BY HACKERS

This is another example of a human and social crisis where saboteurs may steal information from a company's databases by locating security holes in their software. In 2001, the FBI informed e-commerce companies about an extortion racket wherein hackers claim to break into the credit-card databases of e-commerce companies. They then contact the management and demand large sums of money to not misuse these numbers or reveal the break-in.[6]

Another crisis situation involves hackers breaking in and stealing customer information. In December 2000, for instance, hackers penetrated Egghead.com's customer databases and had access to information about their 3.7 million customers. A similar attack in September 2000 allowed a hacker to steal approximately 15,700 credit card numbers from the Western Union site. The FBI also indicted a Russian thief who stole more than 300,000 credit card numbers from CD Universe, an online music seller (Lemos & Charny, 2000; Musil, 2000).

Such incidents bring negative publicity to the organization and erode customer confidence in trusting these organizations to maintain their confidential information. There is the threat that customers may leave and opt for sites that they perceive to be more secure.

VIRTUAL BOYCOTTS OF PRODUCTS OR SERVICES

This is an example of a public-relations crisis that Internet-based organizations may experience. These crises bring negative publicity to the focal organization. Online organizations are vulnerable to these crises, as their highly connected, activist community can quickly initiate and spread the word of a boycott and shut down a site. The eToys example described earlier highlights the vulnerability of online organizations to such activities. Although there have been no well-publicized events so far, it is likely that the online presence of click-and-mortar companies will be the target of activists who want to campaign against the larger companies. Once again, easy accessibility and high visibility will make these companies desirable targets. Another variation of this kind of crisis is when the online medium is used as the means to organize boycotts and protests against companies. Large companies whose policies or business practices are seen as controversial by some groups are often the target of such mobilization. For instance, Web sites abound that help provide a forum for discussion and organization against Wal-Mart (see http://www.walmartwatch.com) and

Microsoft (the Microsoft Boycott Campaign, http://www.msboycott.com, lists over 160 anti-Microsoft sites and discussion forums). Some of the anti-Wal-Mart sites have been used effectively to oppose new Wal-Mart superstores in communities such as Inglewood, California. Such boycotts bring negative publicity to the company, and if not quickly contained can have serious negative economic consequences for the organization.

COPYRIGHT AND PRIVACY ISSUES

Online organizations are also vulnerable to particular legal crises. The Napster case highlights some of the copyright issues that the online medium has precipitated. Napster provided its consumers free access to music through a peer-to-peer online medium. The recording industry, however, felt that Napster was infringing on its copyright and that it was losing revenue. It sued Napster, which was subsequently forced to stop providing this free service. Despite the demise of Napster, a number of other peer-to-peer networks have persisted and a variety of copyrighted material is distributed through these networks. In August 2004, the federal government cracked down on some of these networks in an effort to reduce the sharing of copyrighted material.[7] Educational institutions offering classes online are also forced to grapple with copyright issues. A number of universities are looking at online learning as a new way of educating students while providing a new revenue source for the university. Typically, faculty members retain copyright of the material they develop in order to teach a course. They can therefore use that material to teach at other universities as well. The copyright ownership is less clear for a course that a university puts online.

Copyright issues as illustrated by the Napster crisis can seriously threaten the survival of an organization. The organization also finds itself in the media spotlight and has to fight to justify its legitimacy and reputation. The economic costs of these efforts itself can weaken the viability of the organization.

The privacy of customer information has also become a major concern. Legal issues related to companies selling this information have been highlighted in the media. Another situation that is getting media and legal attention is what happens to customer data when a company shuts down or is acquired. When Toysmart.com shut down, Disney paid $50,000 to have the customer data destroyed after initial attempts to sell this information created a huge controversy (Sandoval, 2001). Attorneys general of a number of states also made sure that the eToys customer data could not be sold directly as part of bankruptcy proceedings.

Public-relations crises ensue when a company has deliberately or unknowingly violated privacy laws by sending customer data to other companies. Such incidents also have serious economic and legal implications for organizations.

In April 2001, for instance, Alexa, an online subsidiary of Amazon.com, paid $1.9 million to its customers as settlement of a class-action lawsuit. The suit claimed Alexa had sent confidential customer information to Amazon.com in violation of its privacy policy. Alexa, however, did not admit to any wrongdoing as part of the settlement.[8]

Strategies for Crisis Management

Researchers have categorized the phases of effective crisis management as

1. crisis prevention,
2. preparedness,
3. containment,
4. recovery,
5. learning (Kovoor-Misra, Zammuto, & Mitroff, 2000; Pearson & Mitroff, 1993).

Thus, organizations must be able to prevent crises if possible, but they must also have the preparedness capability to contain, recover, and learn from them if they do occur. However, most online organizations are still developing their capabilities in the area of crisis management. As new forms of crises emerge, organizations are making incremental strides in learning from and avoiding them. The occurrence of various online crises has generated awareness among these organizations and has resulted in business opportunities for infrastructure and service companies. For instance, after the inability of a number of e-tailers to adequately prepare for the holiday traffic surge in 1999, a number of companies such as Mercury Interactive now offer services that will test e-commerce sites with artificially generated traffic. Also, a number of security companies have emerged that either provide products or services to help online companies identify vulnerabilities through security audits or help monitor their systems on an ongoing basis.

Online organizations could benefit from the crisis-management literature, where a plethora of strategies are prescribed for organizations in general (Barton, 1993; Fink, 1986; Kovoor-Misra, 1995; Pauchant & Mitroff, 1992; Pearson & Mitroff, 1993). For example, strategies such as having in place crisis plans and teams, instituting a control room, the use of a learning audit, and managing the psychological stress of employees are all valuable crisis-management strategies for online organizations.

In this paper, we suggest seven strategies that we believe are particularly important for leaders of Internet-based organizations to better manage crises. Table 3.2 maps these strategies across the phases of crisis management.

Table 3.2 Crisis Management Strategies for Online Organizations by Phases

	Phase of Crisis Management				
Recommended Strategy	*Preparedness*	*Prevention*	*Containment*	*Recovery*	*Learning*
Monitor technology and chat groups		▨	▨		
Identify key online stakeholders		▨	▨		
Develop online crisis portfolio	▨	▨	▨	▨	▨
Institute secondary data centers	▨		▨	▨	
Address nontechnical aspects of online crises			▨	▨	
Customer relationship management			▨	▨	
Share crisis learning across online organizations					▨

NOTE: Shaded cells indicate phases that each strategy addresses.

MONITOR TECHNOLOGY AND CHAT GROUPS

Top managers must detect threats from external stakeholders, primarily hackers, by monitoring signals in technology and chat groups. One of the most severe threats to an Internet-based organization is to its Web site. Organizations need to be able to differentiate between denial-of-service attacks and increased volume of legitimate customers. They also need to have the necessary security systems in place that will inform them of attacks to their customer data. While there is work underway to create intrusion detection systems that provide early-warning signals to an organization, the technology is still in its infancy. The fact that the nature of these attacks keeps changing also complicates the problem of developing a foolproof security system. External monitoring services such as Keynote and Mercury Interactive are examples of organizations that provide an early-warning system for potential problems on the Web site.

Chat groups that allow consumers to connect with each other are also accessible to members of the focal organization. Chat groups relevant to the organization can be continuously monitored to determine the focus and tone of discussions. Security specialists are often able to gain valuable insights by monitoring hacker chat rooms and notice boards. Financial sites like Yahoo! Finance and Quicken also provide discussion boards that can provide useful information. The Computer Emergency Response Team (CERT) also maintains a database of known vulnerabilities and attacks and should be monitored regularly by the information-technology staff.

IDENTIFY KEY STAKEHOLDERS IN AN ONLINE ENVIRONMENT

A second strategy that can be used to prevent and contain crises is a stakeholder audit that identifies stakeholders who play a critical role in an online environment. Stakeholders are those individuals or groups who can affect or be affected by an organization (Freeman, 1984). Other than the traditional stakeholders of an organization, such as customers, employees, investors, competitors, suppliers, and the media, other stakeholders must be considered, such as the hacking community, online service providers, data center operators, or the Computer Emergency Response Team (CERT).

Stakeholder audits can also be used to determine stakeholder attitudes—whether they are antagonistic or cooperative, and whether they are allies, enemies, or neutral toward the organization. Their power in terms of their ability to harm the organization should also be assessed (Savage, Nix, Whitehead, & Blair, 1991). The organization may find that they have both antagonistic and cooperative stakeholders with high power over the organization. These two groups may indicate who the salient stakeholders are and which groups would be allies versus which would be threats. For example, an organization may have antagonistic investors if it is slow to show a return on the investors' investment. It may also find that it is the target of particular hackers. On the positive side, its employees may be loyal and supportive or the local media may be inclined to give it positive press, as it is the dominant online firm in the community. Efforts need to be made to defuse antagonistic stakeholders and strengthen relationships with cooperative stakeholders. Stakeholder audits prior to a crisis could shed light on and defuse a situation that has the potential to escalate to a crisis. During a crisis, the results of an audit could help an organization plan its crisis-containment strategies.

DEVELOP A CRISIS PORTFOLIO FOR ONLINE CRISES

Crisis-management researchers have suggested the importance of preparing for a portfolio of crises. It is assumed that if organizations prepare for a particular type of crisis, the capability to respond to that crisis can be translated to other similar crises (Pearson & Mitroff, 1993). In this chapter we have described various crises that Internet-based organizations could experience. Thus, we suggest that they prepare for the possibility of Web site failures (technical), sabotage and blackmail (human and social), virtual boycotts (public relations), and copyright and privacy issues (legal).

Threats in the online world are also characterized by constant evolution. After Microsoft reacted to a denial-of-service attack on its DNS servers by distributing its DNS servers across Akamai's content-distribution network, hackers then targeted Akamai's network with a similar attack. It is therefore a challenge to try and stay one step ahead and anticipate the nature of potential attacks. Some security companies have started offering an "ethical hacking" service that attempts to attack a company's network and computers the same way malicious hackers may attack. This often helps identify potential vulnerabilities and new types of attacks that emerge. Similarly, security companies offer intrusion-detection services that detect network intrusions and automatically keep up-to-date with the latest types of intrusions being practiced by hackers. It is important to realize that the nature and form of online crises changes rapidly, and it is critical for an organization to keep updating its crisis preparedness to be prepared for new kinds of online crises.

INSTITUTE SECONDARY DATA CENTERS

Since Internet-based organizations are highly dependent on their Web sites for revenue, it is critical that they build redundancy into their systems architecture in order to be able to recover if there is a fire or a malicious hacker attack against them. While building full redundancy with automatic failover is an expensive proposition, the goal of the technology team should be to eliminate all single points of failure in the system. Even if the organization cannot afford a full secondary data center, it should have crisis-response plans in place that allow the site to be up and running in a matter of hours out of a secondary facility should the primary data center have a catastrophic failure. The company should also carry an adequate insurance policy to ensure that it can survive a temporary outage. Such preparedness enables the organization to minimize losses and quickly recover from a crisis.

ADDRESS THE NONTECHNICAL ASPECTS OF THE ONLINE CRISIS

Internet organizations have a strong technology core. Therefore, there may be a tendency to focus on the technical aspects of a crisis and ignore some of the nontechnical aspects such as the negative media attention, customer relationships, or the psychological burnout of their employees. For example, even though not an Internet crisis, the response from Intel to the floating-point unit bug in the Pentium processor exemplifies this problem. Once the technical problem in its processor was highlighted in the press, Intel focused on arguing the technical issues such as the low impact of the bug in most day-to-day operations. It was slow to recognize and address the public-relations aspects of this problem. This caused a backlash, and Intel was finally forced to recall the processor at an economic cost and with damage to its reputation.

It is important for online organizations to realize that the nontechnical aspects of the crisis often have a significant impact as well. For instance, after a denial-of-service attack, in addition to the technical issue of bringing the Web site back, executives must pay attention to repairing customer relationships (we discuss this further below). They must also project the company's point of view in the media, and address employee burnout once the crisis is past. It is therefore critical that the organization assign high-level executives to manage these nontechnical issues.

CUSTOMER RELATIONSHIP MANAGEMENT

We focus attention on the issue of customer relationship management (CRM) here as many organizations with an online presence are still building their brand and loyalty with their customers. Thus, loss of trust because of an unreliable Web site or an inability to deliver products or services can severely damage the possibility of a longer-term relationship with consumers, and impede an organization's recovery from a crisis.

For online retailers, it is extremely important that the three bases on which customer loyalty is built—a fast and stable Web site, fast and reliable order fulfillment, and excellent customer service—are given the highest priority. Special attention needs to be given to customer-relationship management so that the organization can understand its customers and meet their needs effectively. Efforts need to be made to demonstrate that these relationships are important. For example, after toysrus.com was unable to deliver all orders in time for Christmas during the 1999 season, it attempted to repair the damage by sending customers $100 gift certificates.[9] In addition, evidence that the organization has learned from the crisis and made changes goes a long way in rebuilding trust with stakeholders.

SHARE CRISIS LEARNING ACROSS ONLINE ORGANIZATIONS

Crises are important sources of learning as they highlight organizational strengths and weaknesses, and challenge existing assumptions. Organizations may learn from direct experience or vicariously if they perceive the crisis of another organization as having a high probability of happening to them (Kovoor-Misra, 1996). To effectively learn from a crisis, researchers suggest that top managers create a positive learning climate, conduct a learning audit, use multifunctional learning teams, reward learning behaviors, and follow through with the necessary changes (Kovoor-Misra & Nathan, 2000). We believe these strategies are all relevant for online organizations as well. We suggest, however, that there is a need to share learning across online organizations. We see such shared learning in more mature industries, such as the chemical and airline industries. Given the threat to the industry as a whole, when one organization has a crisis such as a gas leak or airline crash, they make it possible for other members of the industry to learn from each other. For online organizations, crises such as denial-of-service attacks, virtual boycotts, blackmail, and sabotage can severely erode consumer confidence in all online organizations. Thus, we suggest that organizations focus not only on their own learning but share information to build capability in the industry as a whole as well.

Future Directions for Crisis-Management Research

The onset of online crises also has implications for academic research on crisis management. First, additional dimensions need to be added to existing models of crisis typologies. Current models categorize crises by variables such as crisis severity, the source of the primary cause of the crisis, or the area of its impact. Online forms of crises highlight other dimensions, such as geographical scope and speed of escalation, that must be considered in crisis classification schemes.

Online forms of crises often transcend national boundaries. Crises such as fires and explosions may have a local boundary, whereas online crises such as virtual boycotts or sabotage may have international boundaries. Similarly, stakeholders in these online crises may be located in other countries. In some of the examples we discussed, hackers were based in China, the Philippines, and Canada. The geographical scope of a crisis is an important variable to be considered because of its implications on the scope and reach of crisis planning and management activities.

The speed of escalation after a crisis has manifested itself is another dimension that needs to be added to crisis typologies. Crises vary in their speed of escalation. For instance, crises such as virtual boycotts may escalate more quickly than other forms of boycotts because the online medium provides accessibility and visibility of information on the Internet. The faster the escalation, the greater the urgency to minimize the crisis. Thus, models of types of crises should include this variable to classify crises.

Second, the accessibility of organizations to threats and the visibility of a crisis are other variables that must be considered in estimating crisis vulnerability. These factors make online organizations more prone to crises. Typically, models of crisis causation have focused on organizational variables such as structure, culture, technology, and lack of processes such as plans and procedures. The online medium provides greater access to organizations. Organizational Web sites and databases can become targets of malicious individuals at any time of the day or night, from individuals anywhere in the world. In addition, when a Web site fails or a denial-of-service attack is in progress, it becomes visible to other interested observers based anywhere in the world and creates awareness that an organization is in trouble. Accessibility and visibility are important factors and should be considered in estimating the vulnerability of an organization to crisis.

Finally, brick-and-mortar organizations that move to online operations are a rich context for studying how top managers adapt to changes in their crisis environments and prepare for crises. Online divisions typically have different cultures than more established companies by virtue of their environment and the kinds of individuals they attract as employees and as attackers such as hackers. There is often a difference in values and language. The extent to which top managers are able to transcend their more traditional cultures, be open to these new forms of crises, and create greater crisis preparedness provides us with deeper insights as to how top managers respond to potential threats and the crisis-preparation process.

To conclude, the Internet as a medium of conducting business is here to stay. As we become more and more dependent on this medium, it is important to understand the threats inherent in the Internet and the kinds of crises that may ensue. This chapter has sought to shed light on these issues, suggest strategies for top managers to better manage them, and extend academic research to capture some of the complexities of crises that exist in an "online world."

Notes

1. MafiaBoy pleads guilty in hacker case, http://news.cnet.com/news/0-1005-200-4523277.html.

2. Global hacker agreement could affect bug hunters, http://news.cnet.com/news/0-1005-200-3314003.html.

3. Outages plague eBay again, http://news.cnet.com/news/0-1007-200-344247.html.

4. See www.toywar.com and eToys settles net name dispute with etoy, http://news.cnet.com/news/0-1007-200-1531854.html.

5. See Toysrus.com's net congestion continues, http://news.cnet.com/news/0-1006-200-1435578.html.

6. See FBI probes extortion case at CD store, http://news.cnet.com/news/0-1007-200-1519088.html; Borland, op. cit.

7. http://www.cnn.com/2004/TECH/08/26/cybercrime.probe.

8. Amazon unit settles privacy lawsuit, http://news.cnet.com/news/0-1007-200-5754965.html.

9. See Toys "R" Us falling short on Christmas deliveries, http://news.cnet.com/news/0-1007-200-1503101.html.

Bibliography

Akamai says Internet attack disrupted major Web sites. (June 15, 2004). Associated Press.

Barton, L. (1993). *Crisis in organizations: Managing and communicating in the heat of chaos.* Cincinnati, OH: South-Western Publishing.

Borland, J. (2000, March 2). Hacker attack latest in string of online credit card thefts. Retrieved December 29, 2006, from http://news.com.com/2100-1017-237553.html

Fink, S. L. (1986). *Crisis management: Planning for the inevitable.* New York: AMACOM.

Freeman, R. E. (1984). *Strategic management: A stakeholder approach.* Englewood Cliffs, NJ: Prentice Hall.

Hambrick, D. C., & D'Aveni, R. A. (1988). Large corporate failures as downward spirals. *Administrative Science Quarterly, 33*, 1–23.

Kovoor-Misra, S. (1995). A multi-dimensional approach to crisis preparation for technical organizations: Some critical factors. *Technological Forecasting and Social Change, 48,* 143–160.

Kovoor-Misra, S. (1996). Moving towards crisis preparedness: Factors that motivate organizations. *Technological Forecasting and Social Change, 53*, 69–183.

Kovoor-Misra, S., Clair, J. A., & Bettenhausen, K. L. (2001). Clarifying the attributes of organizational crises. *Technological Forecasting and Social Change, 67*, 77–91.

Kovoor-Misra, S., & Nathan, M. (1999). Crisis causation re-framed. *Central Business Review, 18*(2), 29–35.

Kovoor-Misra, S., & Nathan, M. L. (2000). Timing is everything: The optimal time to learn from crises. *Review of Business, 21*(3), 31–36.

Kovoor-Misra, S., Zammuto, R. F., & Mitroff, I. I. (2000). Crisis preparation in organizations: Prescription versus reality. *Technological Forecasting and Social Change, 63*, 43–62.

Lemos, R., & Charny, B. (2000, December 22). Hackers crack Egghead.com. Retrieved December 29, 2006, from http://news.com.com/2009-1017-250262.html

Musil, S. (2000, September 10). Western Union Web site hacked. Retrieved December 29, 2006, from http://news.com.com/2100-1023-245525.html

Nystrom, P. C., & Starbuck, W. H. (1984). To avoid organizational crises, unlearn. *Organizational Dynamics, 12*(4), 53–65.

Pauchant, T. C., & Mitroff, I. I. (1992). *Transforming the crisis-prone organization.* San Francisco: Jossey-Bass.

Pearson, C. M., & Clair, J. A. (1998). Crisis management re-framed. *Academy of Management Review, 23*, 59–78.

Pearson, C. M., & Mitroff, I. I. (1993). From crisis prone to crisis prepared: A framework for crisis management. *The Academy of Management Executive, 7*(1), 48–59.

Sandoval, G. (2001, January 31). Judge OKs destruction of Toysmart list. CNET News.Com. Retrieved December 29, 2006, from http://news.com.com/2104-1017_3-251893.html

Savage, G. T., Nix, T. W., Whitehead, C. J., & Blair, J.D. (1991). Strategies for assessing and managing organizational stakeholders. *Academy of Management Executive, 5*(2), 61–75.

Schmeltzer, J. (2004, May 20). Caribou grinds away at rumor. Chicago Tribune.com. Retrieved December 29, 2006, from http://www.kellogg.northwestern.edu/news/hits/040520ct.htm

Shrivastava, P. (1987). *Bhopal: Anatomy of a crisis.* Cambridge, MA: Ballinger.

Turner, B. A. (1976). The organizational and interorganizational development of disasters. *Administrative Science Quarterly, 21*, 378–397.

Part II

New Crises,
New Meaning