Business Roundtable℠

Growing Business Dependence on the Internet

New Risks Require CEO Action

September 2007

Business Roundtable℠

Business Roundtable (www.businessroundtable.org) is an association of chief executive officers of leading U.S. companies with $4.5 trillion in annual revenues and more than 10 million employees. Member companies comprise nearly a third of the total value of the U.S. stock market and represent more than 40 percent of all corporate income taxes paid to the federal government. Collectively, they returned $112 billion in dividends to shareholders and the economy in 2005.

Roundtable companies give more than $7 billion a year in combined charitable contributions, representing nearly 60 percent of total corporate giving. They are technology innovation leaders, with $90 billion in annual research and development (R&D) spending — nearly half of the total private R&D spending in the U.S.

Growing Business Dependence on the Internet

New Risks Require CEO Action

September 2007

Table of Contents

Executive Summary

Companies have entered an era in which their fundamental business operations increasingly rely on the Internet, creating challenges and risks that require a new way of thinking about incident response and business planning.

The threats posed by this increasing reliance on the Internet are urgent and real. It is imperative that they be addressed as an integral part of existing corporate continuity planning that includes both physical and cyber components, as well as units responsible for business operations.

Companies should assess their Internet dependencies from a business perspective to ensure that they are able to get vital operations running as quickly as possible following a major Internet disruption. This is critical for minimizing the potential adverse impact on companies, as well as minimizing the negative effect on our nation's economy and our national security.

Greater Internet Dependence Raises New Business Vulnerabilities

The significant advance of the Internet and other technology improvements give companies new and greater opportunities and help them conduct business operations that reach every corner of the worldwide economy. At the same time, however, continually increasing reliance on the Internet now places technology at the center of many fundamental business operations, making them more vulnerable to significant Internet disruptions.

This new reality means that although the Internet and its infrastructure may be resilient, disruption or corruption of the data running through the Internet could undermine public confidence in the reliability and integrity of that information. Lack of public trust, paired with the loss of confidence among business leaders, would significantly disrupt business operations and cripple the economy.

Increasing Risk of a Costly Internet Disruption

Risks exist in all aspects of the Internet, as well as the business operations that depend on it. These risks include malicious code, disruptions caused by coding error, natural disasters that have major impacts on vital Internet hubs, and attacks by terrorists or other adversaries. The World Economic Forum estimates a 10 to 20 percent probability of a breakdown of the critical information infrastructure in the next 10 years — one of the most likely risks it studied. Additionally, it estimates the global economic cost at approximately $250 billion, one of the largest cost estimates of the risks examined.

Economic ripple effects of a major Internet disruption could lead to a drop in productivity, lower profits, stock market declines, a decline in consumer confidence, reduced spending and a potential liquidity crisis.

Key Findings: Business Is Not Ready to Handle Significant Internet-Related Disruptions

- **Lack of awareness:** Business leaders are not sufficiently aware of their Internet dependencies and the impact of these dependencies on their ability to conduct the "business of the business" — vital business functions central to operations.
- **Planning shortfalls:** Business continuity plans often do not address the comprehensive risk of a significant Internet disruption to their companies or their supply chains.
- **All companies affected:** An Internet disruption will affect nearly every U.S. company directly or indirectly, and the efforts to respond will create stress points that will hinder recovery.
- **Misplaced expectation of government:** Contrary to the belief of many businesses, government does not have the primary role in restoring business operations following a major Internet disruption.
- **Credible and actionable early warning needed:** Business needs reliable information about significant credible threats delivered as quickly as possible, as well as in-depth analysis of a threat or pattern that could grow into a bigger threat.

Recommendations: Leadership Required

- Companies should assess the Internet dependencies of their business operations.
- Businesses should proactively address Internet dependence and interdependence risks in corporate continuity and recovery plans.
- Because of the far-reaching effects of Internet interdependencies on response and recovery, companies should engage with industry partners, government contacts and other senior decisionmakers to strengthen organizational response capacity.
- Companies will need to engage with existing industry-operated information-sharing and analysis centers to share information on Internet threats, vulnerabilities and disruptions.
- Corporate executives should ensure executive-level engagement with government to set and communicate expectations about early warning and threat notifications for business.

Conclusion: Chief Executive Officers (CEOs) Must Ensure Business/Information Technology (IT) Collaboration to Assess Internet Dependencies of Business Operations

A major Internet disruption will affect critical business operations at nearly every U.S. company, with ripple effects throughout the economy, disrupting vital financial and government operations and putting our national security at risk. CEOs must recognize that leadership is needed to ensure that company business and IT leaders are working collaboratively to determine the Internet dependencies of core business operations, associated risks and whether continuity plans properly address those risks.

I. Introduction: Major Changes Needed to Address New Risks Due to Greater Reliance on the Internet for Business Operations

"Make no mistake: Our networks and systems are vulnerable and exposed. Our adversaries are sophisticated, nimble and organized and they will stop at nothing to achieve their motives, which include economic gain or damage, espionage, revenge, publicity."

— **Gregory Garcia,** *Assistant Secretary for Cyber Security and Communications, Department of Homeland Security, RSA® Conference, February 8, 2007*

According to the World Economic Forum, a breakdown of the critical information infrastructure (CII) is probable in the next 10 years.[1] Yet despite such risks, many companies are not aware of the increasing dependence of their critical business functions on the Internet or of the extent of their business operations' vulnerabilities to a prolonged and widespread Internet disruption — whether caused by a terrorist, a widespread computer virus or a natural disaster.

The pervasiveness of the Internet in business functions means that a cyber catastrophe will be exactly that: The effects will be serious and far-reaching, affecting — directly or indirectly — nearly every U.S. public institution, business and citizen.

This Business Roundtable report seeks to raise an alert for business leaders about a developing risk posed to their companies and the U.S. economy. This risk is from increasing reliance on the Internet for business operations combined with an increasingly vulnerable Internet — and addressing this risk requires a new way of thinking.

Much like our national highway system, which we assume will function to support business needs, the Internet is treated as a public infrastructure: From time to time, there may be isolated damage and repairs, but the roads will always be available. Unlike the national highway system, however, the Internet is not well understood, has complex and global vulnerabilities, and is owned and operated in large part by the private sector. Business, therefore, needs a new approach to incident response and business planning that accounts for the novel characteristics of the Internet.

For example, typical disaster response and business continuity plans often assume a single incident that affects physical assets, requiring companies to shift operations or business functions to other locations. A major Internet disruption will pose far different challenges to businesses, as the impacts will be felt in numerous ways through the loss of functionality of multiple systems at nearly all locations within a vast number of companies across various industry sectors.

Moreover, unlike an attack that affects a single physical asset at just one company and then ends, the interdependencies inherent in the Internet mean that a disruption could have cascading, compounding effects as vital business functions are disturbed. In addition, the effect this disruption will have on customers, vendors and suppliers will hinder and frustrate recovery efforts.

This means that a significant Internet disruption will hurt individual companies, affect supply chains and markets, ripple throughout the nation's economy, and disrupt vital government and financial operations — such as the financial markets and the Federal Reserve — that are critical to maintaining public trust and confidence.

A Need for Greater Awareness of the Business Consequences of an Internet Disruption

In 2006, Business Roundtable issued a report, *Essential Steps to Strengthen America's Cyber Terrorism Preparedness,* that identified significant gaps in our nation's preparedness for a cyber catastrophe.

> *"How can you manage risk if you don't have a good handle on what your environment looks like?"*[2]
>
> — **Jerry Dixon**, *Director of the National Cyber Security Division, Department of Homeland Security*

Building on the 2006 report, this Business Roundtable paper argues that business leaders do not fully understand their dependencies on the Internet nor do they understand their interdependencies relative to other industry members and their supply chain partners. There is a pressing need for companies to be more aware of and better understand their dependencies on the Internet for essential business operations.

It is important to understand that the threats posed by the increasing reliance on the Internet for business applications are urgent and real. They must be addressed as an integral part of existing corporate business continuity planning that includes both physical and cyber components, as well as units responsible for operations.

Potential Impact of Disruptions Demands Due Diligence by Companies

The significant advance of the Internet and other technology improvements give companies new and greater opportunities and help them conduct business operations that reach every corner of the worldwide economy. At the same time, however, continually increasing reliance on the Internet now places technology at the center of many fundamental business operations, making them more vulnerable to significant Internet disruptions.

This new reality means that although the Internet and its infrastructure may be resilient, disruption or corruption of the data running through the Internet could undermine public confidence in the reliability and integrity of that information. Lack of public trust, paired with the loss of confidence among business leaders, would significantly disrupt business operations and cripple the economy.

Business Roundtable believes that business leaders must accurately assess the exposure of both their information technology (IT) and business operations to a widespread Internet disruption and ensure that business planning is supported by sound risk assessment.

Simply put, Business Roundtable's goal is to heighten awareness to ensure that companies are able to get the "business of the business" — vital business functions that enable enterprises to operate — running as quickly as possible following a major Internet disruption to minimize the adverse impact on the economy and national security.

II. Growing Dependence by Business on the Internet

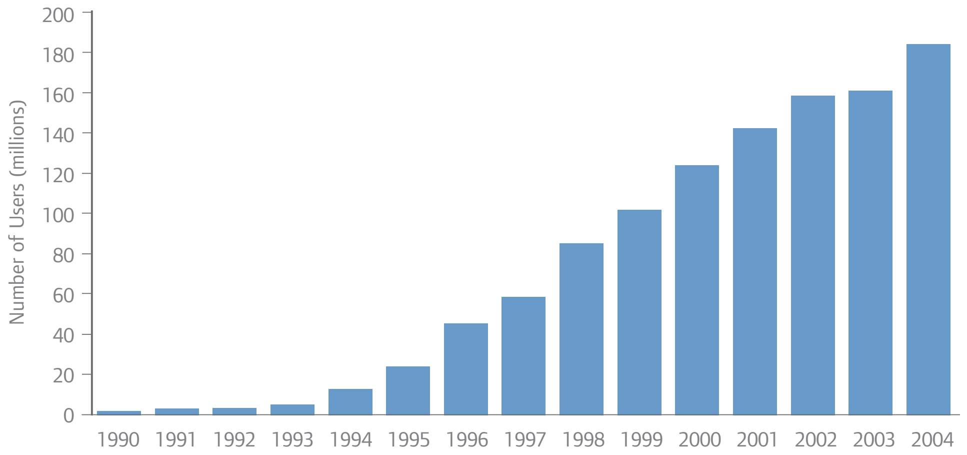
Over the past decade, IT has played an increasingly critical role in generating economic growth and higher productivity across the globe. Yet, though the Internet has been an enormously positive and transformative technology, it also can be a double-edged sword, creating new and unfamiliar vulnerabilities to fundamental business operations.

In 2006, almost one-fourth of all private fixed investment by U.S. businesses was spent on information processing equipment and software, much of which uses, leverages or fully relies on the Internet.[3]

The Internet and Business: Increased Use Results in Greater Productivity and Greater Efficiencies

Internet usage by U.S. businesses and government has grown rapidly in the past decade, and Internet dependence has penetrated every corner of the economy. Between 1994 and 2004, Internet usage in the United States grew from less than 10 million users to more than 180 million users.[4] As of 2002, roughly two-thirds of all American enterprises were using the Internet — a number that has increased in the past five years and is likely to continue to increase. The business community's Internet usage and, by extension, its dependence on the Internet to conduct day-to-day business will increase in the coming years.

A Growing Dependence: U.S. Internet Usage, 1990–2004



Source: *World Development Indicators,* 2007.

By 2010, the Internet is expected to save U.S. businesses approximately $500 billion and result in increased revenues of $1.5 trillion.[5] A significant portion of these savings can be attributed to productivity gains that the Internet confers on businesses; that is, the Internet reduces the time and effort involved in communicating ideas and information, and consequently, workers can accomplish more in a given period of time.

Economic Benefits from Increased Use of the Internet by Business

- Enhanced communications between businesses and between companies and consumers
- Lower search costs that enable businesses to purchase materials at the lowest possible price
- Increased production efficiency
- Lower inventory costs
- Increased competition by making more information readily available
- Reduced customer support costs
- Lower human resource costs
- Lower costs for accounting and finance
- Expanded sales and delivery channels

Core Business Processes Leveraging Internet Efficiencies

Increased reliance on the Internet for critical business and management applications and services as well as communication with customers and vendors has placed the technology at the center of many newly integrated and interdependent core business processes and functions.

These integrated and interdependent functions bring with them new and unfamiliar vulnerabilities in fundamental business operations not experienced in a pre-Internet environment. The convergence of the Internet and telecommunications infrastructure needed to support this integrated functionality is a major component of increased business risk.

This change has been dramatic. In the recent past, typical network infrastructures supported distinct business applications. Private networks handled internal corporate traffic and applications. The Internet supported Web-based and external e-mail services. The switched telephone network supported call centers and corporate voice communications.

Today’s business dependencies create vulnerabilities not only within a company, but also throughout the supply chain. Under the previous configuration, many critical operating systems that support core business functions, such as payment systems, electric power grids, emergency services and telephone communications, relied on infrastructures separate from the Internet.

VoIP is currently used by 20 percent of U.S. businesses. Robust business adoption of VoIP will continue, as In-Stat predicts that two-thirds of U.S. businesses will have some form of VoIP service by 2011.[6]

However, these infrastructures are converging. For example, technical Internet protocols that are the backbone of the Internet increasingly are being used in private networks and in new voice services, such as Voice Over Internet Protocol (VoIP), and corporate management systems and production systems are becoming accessible to external network access. This infrastructure convergence also goes hand in hand with the increased use of outsourced suppliers for such services as call center support, workforce and sales force management, and supply chain management.

These technological changes often are driven by lower costs, greater efficiencies and increased workforce mobility, but the migration of business services from previously secure internal networks to the public Internet requires a new assessment of vulnerabilities and risks.

Greater Dependence Raises New Business Vulnerabilities

This growing trend of dependence means that operations critical for the "business of the business" — once handled in isolated network infrastructures — now rely on the Internet and increasingly are being exposed to its vulnerabilities.

Thus, the exploitation of a growing number of hardware, software and technical vulnerabilities may have even greater consequences to business functions than currently anticipated.

Given the rapid pace of change with which business Internet interdependencies are growing, Business Roundtable believes that many business continuity managers and corporate IT experts are not fully aware of the extent to which global and national business operations rely on Internet services.

Consequently, business leaders must address the risks that these new technology dependencies bring to their business functions. This requires them to partner with IT leaders to understand which functions are vulnerable to a widespread Internet disruption, whether continuity plans address these new risks and whether these plans have been tested.

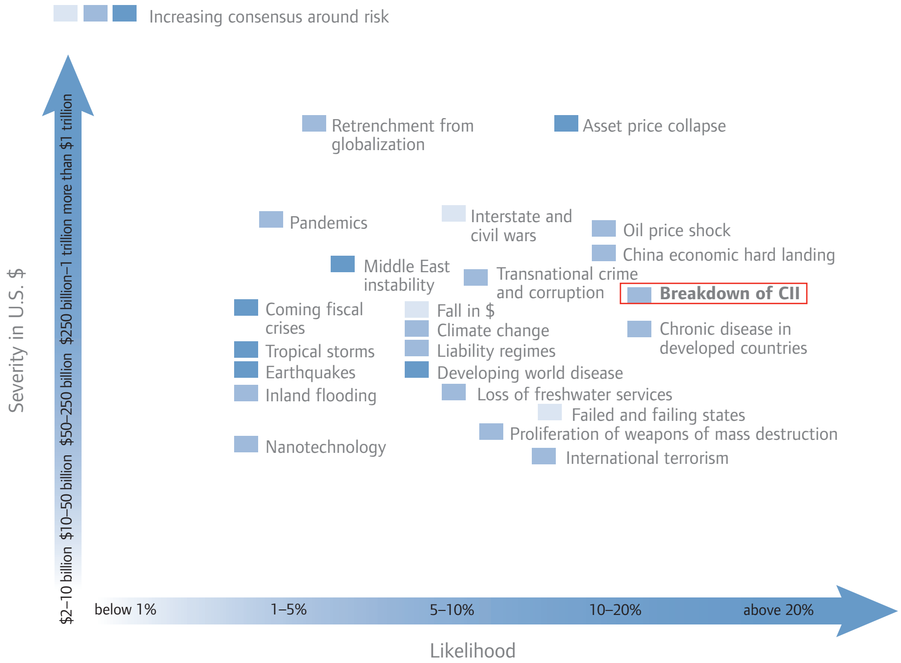
Typical Business Functions That Rely on the Internet

- Remote call center operations
- Travel services
- Points of sale
- Customer contact
- Sales force management
- Payroll administration
- Employee benefits administration
- Securities trading
- Corporate transfer of funds
- Operational control of company electric power grids
- National and international collaboration
- Just-in-time inventory management
- Document backup and storage
- Communications (e.g., voice, data)
- Accounting
- Facilities management

III. Likelihood of a Major Internet Disruption: Threats Posed to Business

According to the World Economic Forum, a breakdown of the CII is one of the core risks facing the international economy. The World Economic Forum estimates that there is a 10 to 20 percent probability of a CII breakdown in the next 10 years, one of the highest likelihood estimates of the 23 global risks it examined in a recent report. The report estimates the global economic cost of the incident at approximately $250 billion, or more costly than two-thirds of the risks.[7]

The 23 Core Global Risks: Likelihood with Severity by Economic Loss



Source: *Global Risks 2007: A Global Risk Report,* prepared by the Global Risk Network, www.weforum.org/en/initiatives/globalrisk/index.htm, and published by the World Economic Forum in collaboration with Citigroup, Marsh & McLennan Companies, Swiss Re and the Wharton School Risk Center. www.weforum.org/pdf/CSI/Global_Risks_2007.pdf

Potential threats to the Internet include malicious code written by individuals, accidental disruptions caused by coding error, natural disasters that have major impacts on vital Internet hubs, and attacks by terrorists or other adversaries. All of these could lead to a significant Internet disruption affecting businesses directly and indirectly due to loss of confidence in Internet usage.

Terrorists and adversaries who wish to harm the financial health of the United States may look to use the Internet as an avenue of attack. A report issued by the research arm of Congress

> *"Our freedom to use cyberspace is threatened by the actions of criminals, terrorists, and nations alike. Each seeks their own form of unique advantage, be it financial, political, or military, but together they threaten our freedom to embrace the opportunity offered by a globally connected and flattened world."* [8]
>
> — **Gen. James E. Cartwright,** *Commander, U.S. Strategic Command*

indicates that attacks on the Internet are increasing in frequency, and the severity of future attacks is expected to escalate.[9]

Several organizations, from nation-states to independent terrorist cells to malicious hackers, possess both the motive and the means to launch a successful attack against the Internet.

In particular, several nation-states could become significant threats to the U.S. Internet infrastructure. As an example, reports indicate that countries are devoting assets to cyber warfare,[10] or are believed to be developing cyber warfare capabilities[11] that could create extensive Internet disruptions and have the ability both to conduct cyber attacks on the U.S. Internet infrastructure and to sponsor cyber terrorists to conceal their identity.[12] Rogue hackers and terrorists also are a threat to the Internet infrastructure.[13] In addition, in June 2007, a top Defense Department official warned the House Armed Services Committee that other nations are pursuing technological advances that could enhance their abilities to launch cyber attacks against U.S. military systems.[14]

In the future, experts believe, attacks from both state and nonstate enemies could be focused equally on harming the nation's economy.[15]

There already are examples of cyber attacks aimed not at military targets but at economic ones. For instance, a massive Internet-based attack in April 2007 on Estonian critical infrastructure exemplifies how the vulnerabilities of an economy built on Internet infrastructure can be exploited — and the resulting business consequences. Estonia, a highly connected nation, sustained a two-week attack on various elements of its Internet infrastructure. The attack not only crashed government Web sites, but also disrupted Internet service providers and forced banks to suspend online service.

IV. Economic Consequences of a Major Internet Disruption

The growing dependence on the Internet for business functions — in conjunction with the risk of terrorist attacks on the Internet infrastructure, as well as the consequences of natural disasters — raises well-founded concerns about the business impact and the costs to businesses, the economy and national security.

Additional research conducted for Business Roundtable by Keybridge Associates suggests that the economic costs to the United States of a month-long Internet disruption could be more than $200 billion, a finding similar to that of the World Economic Forum.[16]

Several other studies have attempted to quantify the economic costs of a catastrophic cyber security attack and a prolonged Internet disruption. This research includes a study of 66 security breaches between 1996 and 2001 by the Congressional Research Service (CRS), which showed a 2.1 percent decline in stock value for affected firms once they released the information about the breach, with a larger 2.8 percent reduction in value for those companies highly dependent on the Internet.[17] The CRS study also found that the impact is much greater if an Internet failure lasts longer than a day or two, with a reduction in stock price of 2.7 percent relative to the rest of the market on the day after the attack, but a 4.5 percent drop three days later.[18] For perspective, a 4.5 percent drop in the Dow Jones would result in a reduction of 600 points. Although data breaches represent an imperfect analogue to a major Internet disruption, market impacts of this magnitude and greater can reasonably be expected.

Furthermore, a study by Dartmouth's Glassmeyer/McNamee Center for Digital Strategies and University of Virginia's School of Engineering and Applied Science looked at the economic costs of an Internet disruption to three industries. This study estimated that the costs of a 10-day event would be $22.6 million on the electrical parts sector, $54.15 million on the automobile parts sector and $404.76 million on the oil refining sector's Supervisory Control and Data Acquisition (SCADA) safety network.[19]

It also is likely that a widespread and sustained Internet disruption will ripple through the economy in several ways that will have a notable significance to business. These include:

- **Drop in productivity.** An instantaneous drop in productivity will be accompanied by a fall in economic output as processes become less efficient and the workforce is destabilized. A typical Business Roundtable company could experience degraded productivity of as much as $1 million per day.[20]
- **Congestion costs.** Because businesses will no longer have the option of using the Internet for business applications and services, they will replace these services with the next-best options, when available, which will likely be more time consuming and costly. This could lead to new and unexpected "congestion costs" on the economy.

- **Lower profits and stock market declines.** A fall in productivity and subsequent reduction in expected profits will affect the stock market, as stock values will decline to reflect higher costs and lower profits. The reaction of the stock market could be greater if investor confidence is shaken, which would likely be the case in the event of a terrorist attack.
- **Reduced consumer spending.** A decrease in the value of stocks is likely to have a "wealth effect" as consumers will be inclined to reduce their consumption because they feel less wealthy — further depressing demand and output in the economy.
- **Potential liquidity crisis.** Cash could be in short supply if automated payment systems are interfered with due to the Internet disruption, leading to a potential liquidity crisis. This new demand for cash could be exacerbated if more vendors require cash payment because of greater difficulties in determining whether a customer has available credit. If fewer credit sales are authorized, the increasing challenges for cash-constrained households will have a further depressing effect on the U.S. economy.

The costs associated with lost productivity and the wealth effect will be significant. But it is important to note that the costs of congestion and potential large-scale infrastructure failures could be even larger due to the cascading effects of a widespread and sustained Internet disruption across the economy.

Scenario: Impact of a Widespread Internet Disruption on an Average Business Roundtable Company

A widespread, prolonged Internet disruption will affect the financial performance of a typical large company through a variety of channels, including lost productivity, lost revenue, lost customers, potential liability costs and reconstitution costs. Although companies should determine their specific impact, here are two examples:

Degraded Productivity — $27.9 million in one month

The deployment and use of Internet technology can substantially raise the productivity — either directly or indirectly — of employees in today's large, sophisticated businesses. The average Business Roundtable company has 62,500 employees, and if Internet downtime results in an average productivity loss of 10 percent, a one-month Internet disruption will result in an estimated $27.9 million of lost productivity for such a company, based on average hourly wages of $18.62.

Lost Revenue — $63.7 million in irreplaceable Internet sales in one month

Many companies derive a significant portion of their revenues from online transactions, and a widespread Internet disruption corrupting data could have a substantial impact on sales by Internet-dependent businesses. For example, consider that the average Business Roundtable company has annual revenues of $31 billion. Assuming this typical company derives 10 percent of its revenues from Internet transactions and assuming that 25 percent of these revenues are permanently lost and not replaced with a sale when the disruption has been resolved, the company's lost sales for one month will be estimated at $63.7 million.

V. Key Findings: Business Is Not Ready to Handle Significant Internet-Related Disruptions

Over the past year, Business Roundtable and a number of its member companies have researched, reviewed and analyzed cyber security preparedness from a business operations perspective. The Roundtable believes that this effort offers a fresh look because cyber security generally is analyzed from a purely IT-centric perspective. The Roundtable's research included input and feedback from cyber security experts and leading officials from government agencies as well as information collected from confidential surveys and in-depth interviews of a diverse number of Roundtable member companies.[21]

Following are the key findings of this work.

Finding: Business leaders are not sufficiently aware of their Internet dependencies and the impact of these dependencies on their ability to conduct the "business of the business."

The Internet infrastructure is complex and unfamiliar to business executives, presenting several challenges for business leaders who are responsible for delivering sound business decisions and assessing strategic risks. Many business operations leaders within companies have not assessed the impact of a significant cyber event in terms of business dependence on the Internet. Furthermore, the work of the IT team within companies most often focuses on internal and technical issues and not business functions that depend on the Internet.

In addition, business leaders are not sufficiently aware of the interdependencies affected by a long-duration Internet disruption. A particular challenge for firms is determining the Internet dependencies of their supply chain and infrastructure support for daily internal operations. These challenges have the capacity to hinder, and even halt, essential corporate activity as core business functions increasingly rely on systems that, once infected or disrupted, can jeopardize the processes that are the backbone of daily business operations.

> *Nearly three-quarters [of the executives surveyed by The McKinsey Quarterly] say that their companies plan to maintain or increase their investments in Web 2.0 technologies in coming years.*[22]

Finding: Business continuity plans often do not address the comprehensive risk of a significant Internet disruption to their companies or their supply chains.

Many company disaster response and business continuity plans are focused on such scenerios as a major incident that affects physical assets at one location, requiring companies to shift operations or business functions to other locations. Any attempt to treat a widespread Internet disruption like a well-known disaster (e.g., natural disaster), even in sophisticated companies, will inadequately address the unique risks associated with a widespread Internet incident.

A major Internet disruption is different from a traditional attack or incident at a physical structure, with the impacts of a cyber incident more widespread and compounded, creating a cascading effect as operations and supply chains are affected.

Unlike an incident that affects a single physical asset, a significant and long-lasting Internet disruption will result in the loss of network functionality that will affect a range of business operations at many locations. Such a major loss also will disrupt business continuity plans which themselves are Internet dependent (such as backup hosting sites using the Internet for communications).

The growing interdependencies of network communications compound the impact of an attack. Also, when a network or system becomes disrupted, IT and business professionals could have difficulty determining the duration of the incident and, therefore, options for remediation. Finally, IT and business managers may have difficulty assessing the business impact of a disruption.

In addition, business continuity plans often do not contemplate a scenario in which the Internet — though not completely down — is disrupted or unreliable for a long period of time. This could result in a lack of confidence by consumers and business leaders and force companies to find alternatives. Business continuity plans can be a positive tool for addressing business disruption as a result of reduced confidence in the Internet.

Currently, many business continuity plans seem to emphasize the challenges that arise when an individual company is affected, without due consideration for the challenges that arise when all companies are faced with the same challenges and simultaneously increase demand for the same services.

Finding: An Internet disruption will affect nearly every U.S. company directly or indirectly, and the efforts to respond will create stress points that will hinder recovery.

In a situation in which the Internet is down or found to be unreliable for an extended period, companies are likely to turn to conventional methods of communication and processing until Internet service can be restored. Where such backup capabilities are possible, their use will put enormous stress on the telecommunications, mail, delivery and office supply industries.

Success at mitigating the economic impact of a disruption will largely depend on the ability of these industries to successfully manage a surge in demand and sufficiently scale up operations using spare capacity, temporary labor and/or creative work-arounds.

For example, most companies taking part in the Business Roundtable research project indicated that, in the event of a disruption, they will replace Internet communications with mail services and express shipment providers, complicating recovery efforts. This will lead to dramatically increased volume and stress on all express shipping and postal providers.

Other stress points from a widespread Internet disruption could include:

- **Demand for cash.** Financial institutions will face a demand for cash if Internet-based delivery channels are perceived as vulnerable or unreliable, potentially creating a need to replace electronic communications with manual, paper-based methods.
- **Temporary workers.** Temporary workers will be in high demand as companies use less-efficient paper systems. Such provisional systems and workers will be unable to sustain the corporate knowledge that central, automated processes have provided.
- **Gasoline and other fuels.** Energy company distribution systems could be hampered by an Internet disruption. At the same time, demand for gasoline could increase vehicle traffic because workers who telecommuted must now go into the office to access private networks. Fuel hoarding also could occur. Transportation fuel providers may need to enforce rationing and/or physical security measures at fuel stations depending on the nature of the crises and the public response.
- **Unavailability of alternative technology.** Efforts to return to telephone-based communications and faxes to restore company operations will place new demands on equipment that often was being phased out or replaced. Moreover, this equipment may be Internet-dependent in some cases.
- **Paper and other office supplies.** Office supply companies will experience a surge in demand for paper-based methods of communication, and their own supply and distribution operations may be compromised by the disruption.
- **Greater demand on existing phone systems.** Sales and other transactions currently done on the Internet will be replaced by telephones.
- **Congested transportation systems.** Transportation networks are likely to become more congested as delivery services and in-person meetings increase and as work-at-home employees are forced to go into local offices to access private networks.

Potential Stress to the U.S. Postal Service

A major Internet disruption may occur at a time when the U.S. Postal Service is reducing staff and increasing its dependence on technology. A 2003 report by the President's Commission on the United States Postal Service notes that the Postal Service has cut more than 40,000 workers since 2002 because of a continuing decline in mail due to electronic bill payment and other Internet communications. In addition, the 2003 report notes that the Postal Service is using the Internet more in its operations as well, creating possible vulnerabilities and disruptions that businesses may not be aware of in their contingency planning.

In addition, vendor dependencies and prioritization conflicts are likely to affect businesses. As a widespread disruption will crosscut sectors and industries, many organizations will rely on their vendors for resources and support. The interdependencies and prioritization processes of these vendors are generally unknown to organizations. These procedures may run into conflict with service level agreements and resource allocations.

Finding: Business has a misplaced expectation of government. Government does not have the primary role in restoring business operations following a major Internet disruption.

The Business Roundtable research involving a sample of member companies found that most companies expect government to play a critical role during the disruption. These companies expected government to assume a variety of responsibilities, including setting and communicating national priorities, coordinating efforts among industries, providing stability and security, spearheading the restoration process, and maintaining public confidence in markets.

Furthermore, a majority of companies participating in the Business Roundtable research also indicated that they would expect federal, state and local governments to provide relief, safe harbor and/or grace periods for satisfying mandatory reporting requirements.

However, government systems for responding to a major Internet disruption likely will not provide the level of response that companies are anticipating. This is particularly true given that Internet functionality is essentially made possible via an integration of private-sector companies in a complex and interdependent system. Additionally, it is unclear that government has established adequate and tested protocols for setting priorities and avoiding conflicting directives from different agencies during an extended disruption.

It is likely that companies will receive directives and guidance from a variety of government agencies or authorities, with a real possibility of conflicting directions from different agencies.[23] Discussions with various government agencies suggest that there is no single government entity with authority to grant waivers or grace periods regarding the myriad regulations and requirements that affect business.

There also remains a lack of clarity in the operational relationship between private-sector and government responsibilities in addressing a major Internet disruption. Although many planning policy documents exist, such as the National Infrastructure Protection Plan (NIPP) and the National Response Plan, they are heavily focused on physical incidents and not Internet disruptions and consequence management.

These gaps between business expectations of government and the government's response capabilities in the event of a major Internet disruption could significantly hinder recovery and lead to a greater economic impact.

With the objective of adversaries being to impede the national economy by disrupting the ability of companies to conduct business, it is business, not government, that understands the needs and has the primary responsibility to mitigate and restore its operations following an Internet disruption. As a consequence, business cannot wait for the government to address all Internet disruption issues.

Finding: Business needs reliable information about significant credible threats delivered as quickly as possible, as well as in-depth analysis of a threat or pattern that could grow into a bigger threat.

Credible and actionable communication about threats or attacks, response coordination, and stress-point management are critical for businesses as part of a responsible Internet security and risk management plan. Businesses will benefit from timely and actionable information about a threat or attack and from clear and coordinated information from government on actions to take following a major disruption.

Government has special obligations with respect to threats against the Internet. Early warning about a major threat or growing attack against the Internet might allow companies to be ready to take preventative action or minimize the potential damage to their IT systems and to business operations that are dependent on the Internet.

This capability is a component of "information sharing," a trusted and regularized means for exchanging information about threats, vulnerabilities, exploits and response to disruptive incidents affecting the Internet. Although improvements have been made, gaps remain in information sharing. For example, private-sector companies have invested in establishing and operating around-the-clock Information Sharing and Analysis Centers (ISACs) in many critical infrastructure sectors. However, businesses representing large segments of the U.S. economy are not part of any ISAC, and some sectors have not yet invested in ISAC capabilities.

Business Roundtable acknowledges that cyber attacks or disruptions can occur without warning but notes that the current information-sharing structures and their linkages to government "watch and warning" systems do not enjoy a single government point of contact. Such a point of contact would enable the sharing of timely information about threats and pending attacks so that companies could take appropriate steps to strengthen defenses or manage risks. Although this is an area of much discussion in government and private-sector planning arenas (represented in meetings and such forums as Sector Coordinating Councils), the current operational environment is inadequate.

Furthermore, given the lack of understanding of the extent to which company business systems rely on the Internet, it is likely that in many companies, threat information that is received by companies is kept in the IT part of the company and not disseminated to business leaders whose applications and operations could be affected.

In all cases, before a crisis occurs, it is important for companies to establish operational relationships with their appropriate ISACs (which are organized by industries) or, for companies for which an ISAC appropriate for their business sector has not yet been established, with the appropriate government agencies. Building relationships now is a sound business continuity practice and can be of tremendous help when there is a need to contact a government agency, other companies or other industry response organizations during a crisis.

At the same time, companies also have an obligation to establish internal processes and systems for receiving, managing and acting on threat and other shared information. At a time of seemingly endless amounts of information, companies must be able to pinpoint trusted information and ensure that trusted information about Internet-related threats or disruptions is provided in a timely way to business unit leaders whose business functions may be affected by Internet disruption.

Government must play a key role in providing information as part of a coordinated response following a significant Internet disruption. This might include measures to maintain order, establishment of priority lists, or other steps necessary to avert or mitigate extreme — and costly — outcomes. Government also needs to provide a means of using intelligence information more widely among its own agencies and businesses. At the same time, companies need to have structured their internal business continuity planning to properly interface with government and external industry efforts.

VI. Recommendations: Leadership Required

1. Recommendation: Companies should assess the Internet dependencies of their business operations.

Companies should undertake a robust examination of how their essential business activities rely on the Internet. An assessment of the company's reliance on Internet services is not a simple undertaking, but chief executive officers (CEOs) must set and direct the tone regarding the importance of this effort and direct business and IT managers to work collaboratively to dive deeply into this examination.

A range of best practice options is available to CEOs to support a risk management approach. For example, companies that responded to Business Roundtable questions regarding the effect on their business of a month-long Internet disruption scenario took a variety of approaches.[24] One consistent finding is that the most detailed responses involve formal meetings and discussions encompassing representation across the corporate community. This suggests that a mapping of critical Internet connections will not track organizational charts, so gathering the right perspectives across internal organizational boundaries is critical.

Company responses also reinforce the importance of involving senior business operations managers, who understand how essential business functions support delivery to customers and the market. The best-prepared companies seek to look deeply into dependencies, supply and value chains, and contingency plans by mapping each of these key activities to the Internet. Understanding unique stress points can follow only from a sophisticated understanding of how business delivers goods and services.

In this environment, CEO involvement — directing and setting the tone from the top — almost certainly is a condition of success. Business Roundtable questionnaire responses uniformly underscore the need for — and the complexity of — gathering together senior professionals and managers from such diverse corporate environments. For example, IT managers may understand reliance on the Internet, but lack information regarding the "business of the business." In addition, company responses to the Roundtable questionnaire suggest that senior business leaders may rely on faulty assumptions about uses of the Internet. Lack of resources and priority business goals, the research suggests, also could undermine efforts to clarify

Questions That CEOs Can Ask

- If Internet services were no longer available, how would our business be affected? What are the potential economic costs to the company? On what basis are we drawing our conclusions?
- What degree of consumer confidence in our data, services or products may be affected by a disruption of the Internet or corruption of data and services that are dependent on the Internet?
- To what extent have we initiated a formal process to map and assess our dependencies on the Internet? If we have, did the process involve senior business managers as well as IT and communications managers?
- Have we identified a position that will take responsibility for resolving risks associated with Internet reliance for the "business of the business"? Do I need to provide authorization for a person to work across the corporate community to ensure we prioritize an assessment?
- Have we considered the dependence of our vendors and supply chain on the Internet?

Internet use and risk management alternatives absent CEO involvement. This cannot be delegated to the IT professionals within companies — it must be integrated into business leader deliberations.

2. Recommendation: Businesses should proactively address Internet dependence and interdependence risks in corporate continuity and recovery plans.

Corporate leaders must ensure that business continuity and disaster recovery plans account for lessons gathered from the Internet assessment process. This is especially critical where the assessment reveals a relationship between Internet services and critical business activities.

Continuity planning should include plans for an extended Internet disruption and its impact on business functions of the company. This updated plan should address issues such as fall-back business processes, employee communications plans, media plans, customer outreach and corporate finance requirements, all with the understanding that the Internet may not be available to execute the plan. Internet dependencies of key suppliers also should be assessed and addressed.

Business Roundtable’s research suggests that a failure to understand how the “business of the business” relies on the Internet could undermine continuity response plans. Roundtable survey responses repeatedly underscore the importance of understanding Internet connectivity and dependencies. This is especially the case where planning assumptions are tied to the availability of the Internet and corporate stress points, including the availability of cash and corporate communications (e.g., fax).

There are additional strategic considerations. Many companies assume, for example, that geographic separation will permit the “business of the business” to restore and recover in the event of a disaster, such as loss of Internet service on the East Coast. However, if an Internet catastrophe occurs, there could be degradation of service on both coasts and internationally. In this circumstance, the assumption that Internet service disruptions will be localized may not be accurate.

Questions That CEOs Can Ask

- To what extent do our business continuity and disaster recovery plans account for Internet availability, and have we tested them?
- If Internet service were disrupted for two, five, 10, 20 or 30 days, what would the impact be on our critical business activities? How have we decided to mitigate Internet availability risks in our plans with regard to the “business of the business”?
- In developing our plans, what conclusions did we draw about the ability of our key suppliers and other corporate partners (such as vendors, contractors, and upstream and downstream partners) to provide essential business services? Since they too rely on the Internet, how have we accounted for their resilience if the Internet is not functioning?
- To what extent do we account for services associated with our people, such as payroll, benefits and employee communications? In a similar manner, how do our plans account for customer and supplier communications?
- Do our plans include participation in existing industry-government response exercises?

3. Recommendation: Because of the far-reaching effects of Internet interdependencies on response and recovery, companies will need to engage with industry partners, government contacts and other CEOs.

Because an Internet-related disruption has impacts that extend well beyond any single company, alerts as well as response and recovery also will require pre-established working relationships, communication, collaboration and coordination among companies, IT and communications sector information-sharing organizations and with government.

Business Roundtable's research and meetings leading up to this report suggest that both public and private sectors are in the early stages of understanding Internet reliance; research also suggests that the lack of robust response plans in government and industry could hamper restoration of essential government services as well as the "business of the business."

In light of these findings, the lack of maturity in response efforts also could undermine public-private collaboration in the event of a prolonged Internet outage, especially if Internet reliance is far more widespread than anticipated.

Companies should review measures available for alerts, response and recovery from an Internet disruption. This review should include identification of ways to ensure strong internal and external communications with industry partners and government contacts.

For example, in the event of a crisis or attack, CEO discussions with government — and each other — can be facilitated by Business Roundtable's CEO COM LINK^{SM}. CEO COM LINK is a secure telephone communications system established by the Roundtable to enable the nation's top CEOs to enhance the protection of America's employees, communities and infrastructure by communicating with leading government officials and each other regarding a terrorist threat, crisis or natural disaster. The CEO COM LINK system does not rely on the Internet.

It is important for companies to identify what other tools are available to them to facilitate emergency communications and enable collaboration.

Questions That CEOs Can Ask

- Do we have a strategy for collaboration with the government in the event of a major Internet disruption?
- Given our company's Internet assessment and findings associated with restoring the "business of the business," have we identified the key government officials (federal and state or local), including our regulators, that we must engage to manage the disruption of business services?
- Have we outlined a game plan for working with other private-sector institutions to gain an understanding of the scope of the disruption and its impact on the nation?

4. Recommendation: Companies should engage with existing industry-operated ISACs to share information on Internet disruptions.

In the current environment, it is important for companies to establish relationships with information-sharing organizations appropriate for their business interests or, where they are not yet in place, with government information-sharing mechanisms before a crisis occurs. Building operational relationships now is a best practice that will pay off in an Internet crisis.

There are several organizations and programs currently in place to facilitate information sharing and early warning with regard to Internet security alerts.

In addition to ISACs, private-sector companies have internal staffs as well as "managed services" contracts in place through third-party vendors to specifically monitor corporate networks, protect against unauthorized intrusion and provide information needed to patch vulnerable systems or make network changes in response to attacks. External organizations include:

- **ISACs —** Many critical information sectors have established these centers, specifically designated to facilitate information sharing across sectors. ISACs are a potential source of early warning information for each sector, although not all Business Roundtable member companies are in sectors covered by an ISAC. Contact information for each of the ISACs can be found in Appendix C.
- **US-CERT —** The Department of Homeland Security (DHS) has opened its U.S. Computer Emergency Readiness Team (US-CERT) portal to the private sector. This team and its US-CERT portal provide insight into cyber events occurring across the nation and can be a good source of information when a cyber attack has potential regional or national impact. More information can be found at www.us-cert.gov.

Companies should encourage the National Cyber Security Division and US-CERT to include Internet disruption matters in sanctioned exercise scenarios. For example, future Cyber Storm exercises conducted by DHS should

Examples of Sources of Internet Alerts and Warnings about Threats in Today's Environment

Information Sharing and Analysis Centers

- Industry sector driven

National and International Computer Emergency Readiness Teams (CERTS)

- U.S. Computer Emergency Readiness Team (US-CERT)
- CERT® Coordination Center (CERT®)
- Forum of Incident Response and Security Teams (FIRST)

Alerts Service Providers and Vendors

- For-fee/contractual/private companies

Hardware and Software Suppliers

- Developers and providers of software/hardware

Industry Forums — Ad Hoc Volunteers

- Trade associations/academic

Government to Business

- Regulatory/Department of Defense/Department of Finance/Federal Emergency Management Agency

Private-Sector Industry Internal Security Capabilities

- Company-to-company

Public Sources

- Nonprofits

Media

- News outlets
- IT periodicals

include scenarios that address getting the "business of the business" functioning. The perspective has traditionally focused on business from an IT angle — there is an urgent need to approach business recovery from a business perspective.

Business Roundtable encourages companies — as part of an evaluation of information-sharing needs — to consider the benefits of becoming an active member of an appropriate sector ISAC and of registering with US-CERT.

Companies also should become familiar with the NIPP, which outlines a comprehensive risk management framework that defines critical infrastructure protection roles and responsibilities for all levels of government and private industry, and participate in the development of government and private-sector plans through membership in the sector coordinating councils, which work in partnership with DHS and other federal agencies.

Questions That CEOs Can Ask

- Are we a member of an ISAC relevant to our sector or industry? Should we be?
- Do we have an operational relationship with US-CERT?
- Do we have the right businesspeople with appropriate security clearances to enable effective partnership with government?
- Do our venders and suppliers have alternative avenues for receiving early warning information, and are we aware of those relationships? Are they members of their ISACs? Do they have a relationship with US-CERT?

In May 2007, the department announced completion of 17 sector-specific plans (SSPs) in support of this infrastructure protection effort. The 17 critical infrastructure and key resource sectors, identified by DHS Presidential Directive 7, require protective actions to prepare for, or mitigate against, a terrorist attack or other hazards. The SSPs define roles and responsibilities, catalog existing security authorities, institutionalize already existing security partnerships, and establish the strategic objectives required to achieve a level of risk reduction appropriate to each individual sector. Nonsensitive SSPs and executive summaries are available at www.dhs.gov/nipp.

5. Recommendation: Corporate executives should ensure executive-level engagement with government to set and communicate expectations regarding the future state of early warning and threat notifications for business.

Though avenues of improving early warning notifications exist, the current state of threat notification is not fully sufficient for businesses to guard against significant widespread Internet disruptions. Specifically, the private sector does not have a consistent, reliable source of early warning information for organized threats, which is vital for maintaining situational awareness for business. To better prepare for Internet disruptions, the private sector needs the following:

- Knowledge of active and strategic threats;
- Awareness of significant threats that can exploit specific vulnerabilities;
- Credible, actionable alerts;

- Active warnings delivered to ISACs and to industry;
- Timely information enabling companies to be able to prepare, defend, respond and reconstitute as soon as the government has credible intelligence; and
- Analysis of vulnerabilities and recommended actions to mitigate.

There are several challenges to achieving this desired future state. First, the government is reluctant to share sensitive information with business leaders who do not possess security clearances. The cost of security clearances and the sheer number of private-sector managers that will request such clearances present barriers to information sharing. Second, government organizations that possess early warning data are institutionally structured to withhold intelligence. Generally speaking, government agencies prioritize the protection of information over the dissemination of information.

In light of the difficulties above, companies should take steps to set expectations and achieve the desired future state of early warning notifications. These include:

- Corporate executives should ensure that business and IT decisionmakers work together to set strategy for achieving the future end state.
- CEOs should communicate, periodically and when appropriate, with high-ranking officials in the intelligence and security communities. This interaction is essential to reinforce the criticality of sharing early warning information with America's business community.
- To improve collaboration, business should better explain to government the kind of information that is valuable and necessary about significant Internet threats so that government officials can structure appropriate information-sharing arrangements.
- Business leaders should strengthen the ISACs and leverage ISAC members as part of the effort to develop a more robust future state of warning.
- Finally, corporate executives should clearly convey, both to internal employees and to external partners, that a well-prepared business and nation require vast improvement in early warning capabilities.

Questions That CEOs Can Ask

- Have we clearly identified the kinds of early warning information essential for protecting our critical business activity?
- Have we communicated this sensitive information to government officials responsible for collecting and sharing early warning information? If we are choosing not to share this information because of security concerns, what are options for managing risks associated with communicating such information?
- Have we set in motion a strategy for attaining early warning information to better protect our customers and corporate assets as well as our suppliers and partners?

VII. Conclusion

It is critical for CEOs to recognize that it will be the responsibility of senior executives to assess and mitigate the effects of Internet dependence on crucial business operations. As part of these efforts, CEOs should ensure that business and IT leaders collaborate and take steps to prepare for, respond to and recover from prolonged Internet disruptions.

Business leaders must recognize the growing dependence of their business functions on the Internet as well as the corresponding greater vulnerability of these operations to an attack on the Internet.

A prolonged and widespread Internet disruption will affect critical business operations at nearly every U.S. company, with ripple effects that will extend throughout the economy, disrupting vital financial and government operations. To address this new reality, businesses must assess their vulnerabilities and develop robust incident response and continuity plans.

The recommendations in this report offer Business Roundtable's approach to addressing these new challenges. By doing so, Roundtable members will protect employees, customers and corporate assets. Furthermore, strong and immediate action by CEOs will minimize the impact of Internet disruptions on the conduct of business, reduce the negative impact on the economy and subsequently protect national security.

Appendix A

Summary of CEO Questions to Ask

Business dependencies on the Internet:

1. If Internet services were no longer available, how would our business be affected? What are the potential economic costs to the company? On what basis are we drawing our conclusions?

2. What degree of consumer confidence in our data, services or products may be affected by a disruption of the Internet or corruption of data and services that are dependent on the Internet?

3. To what extent have we initiated a formal process to map and assess our dependencies on the Internet? If we have, did the process involve senior business managers as well as IT and communications managers?

4. Have we identified a position that will take responsibility for resolving risks associated with Internet reliance for the "business of the business"? Do I need to provide authorization for a person to work across the corporate community to ensure we prioritize an assessment?

5. Have we considered the dependence of our vendors and supply chain on the Internet?

Continuity plans:

1. To what extent do our business continuity and disaster recovery plans account for Internet availability, and have we tested them?

2. If Internet service were disrupted for two, five, 10, 20 or 30 days, what would the impact be on our critical business activities? How have we decided to mitigate Internet availability risks in our plans with regard to the "business of the business"?

3. In developing our plans, what conclusions did we draw about the ability of our key suppliers and other corporate partners (such as vendors, contractors, and upstream and downstream partners) to provide essential business services? Since they too rely on the Internet, how have we accounted for their resilience if the Internet is not functioning?

4. To what extent do we account for services associated with our people, such as payroll, benefits and employee communications? In a similar manner, how do our plans account for customer and supplier communications?

5. Do our plans include participation in existing industry-government response exercises?

Communication with industry partners and government:

1. Do we have a strategy for collaboration with the government in the event of a major Internet disruption?

2. Given our company's Internet assessment and findings associated with restoring the "business of the business," have we identified key government officials (federal and state or local), including our regulators, that we must engage to manage the disruption of business services?

3. Have we outlined a game plan for working with other private-sector institutions to gain an understanding of the scope of the disruption and its impact on the nation?

Membership with industry-operated information-sharing organizations:

1. Are we a member of an ISAC relevant to our sector or industry? Should we be?

2. Do we have an operational relationship with US-CERT?

3. Do we have the right businesspeople with appropriate security clearances to enable effective partnership with government?

4. Do our venders and suppliers have alternative avenues for receiving early warning information, and are we aware of those relationships? Are they members of their ISACs? Do they have a relationship with US-CERT?

Future state of early warning notifications:

1. Have we clearly identified the kinds of early warning information essential for protecting our critical business activity?

2. Have we communicated this sensitive information to government officials responsible for collecting and sharing early warning information? If we are choosing not to share this information because of security concerns, what are options for managing risks associated with communicating such information?

3. Have we set in motion a strategy for attaining early warning information to better protect our customers and corporate assets as well as our suppliers and partners?

Appendix B

Findings and Analysis of Business Roundtable Company Research Project on Business Impact of a Widespread and Prolonged Internet Disruption

April 21, 2007

Memorandum for Business Roundtable Cyber Security Working Group

From: Keybridge Research LLC
Re: Cyber Security Working Group Survey Assessment & Insights

In September 2006, the Business Roundtable Cyber Security Working Group was charged with examining the risks associated with a prolonged, pervasive Internet outage and the potential impact on American businesses and the U.S. economy as a whole. With this goal in mind, the Working Group surveyed a subset of Roundtable members to better understand businesses' unique Internet dependencies, level of preparedness and likely actions. To ensure that survey responses would remain confidential, the Working Group commissioned an independent third-party investigator (Keybridge) to review the survey responses in detail and prepare an analysis for the larger Roundtable membership. The following report presents the key findings and conclusions from this analysis.

I. Context

In an attempt to get an economy-wide perspective of the scenario, the Working Group constructed a small sample of companies representing a diverse set of industries and economic sectors. The goal was to ensure that the survey responses provided a "360 assessment" of the situation and adequately reflected the varied perspectives and interests of Business Roundtable membership and the business community as a whole. Companies were asked to anticipate the challenges they would face in response to a carefully crafted scenario. Respondents were then presented with a series of questions designed to solicit information about a business's preparedness, likely response and perceived conflicts. Recognizing that each company's dependency on the Internet is unique to the character and structure of its business, the Working Group decided to utilize an open-ended questionnaire format. Respondents were presented with broad "issue questions" and were encouraged to provide answers as detailed as seemed appropriate. This approach resulted in a wealth of qualitative information but limited quantitative data. Consequently, the analysis is primarily the product of the collective perception and interpretation of the analysts, rather than a statistical analysis.

The analysis approaches the problem through four different organizing frameworks or analytical lenses. Section II presents summary statistics and other indicators about the overall number, nature and quality of the survey responders. Section III describes a likely response scenario based on the collective actions of all companies, with particular emphasis placed on those industries or services that are likely to become “stress points” in the economy during such an event. Section IV identifies specific actions companies have taken or plan to take in response to the event before classifying them as mitigating, adaptation or resolution strategies. Finally, Section V presents the key themes that emerged from the collective responses and offers recommendations with the goal of assisting companies in managing the risks associated with a catastrophic Internet failure. Key findings and insights are presented throughout the document where appropriate.

II. Summary Statistics

(1) Industries Responding

- Includes leading companies with operations and expertise that will be critical to the successful resolution/response of a widespread Internet outage and the general economic stability of the nation, such as telecommunications, mail/delivery services, information technology (IT) services, software, office supplies, financial services and energy.

(2) “Solution” versus “Non-Solution” Companies

- Of those responding, 33 percent of companies were assessed as “solution” companies — that is, companies providing services that will be critical and directly related to the successful resolution and/or critical to the economy’s ability to adapt to the crisis.
- The remaining 66 percent of companies were assessed as “non-solution” companies — that is, companies providing services that will not be critical or directly related to the successful resolution and/or adaptation to the crisis. However, several of these companies might be considered “secondary solution” companies that provide services critical to the underlying stability of the economy and might be heavily relied upon, depending on the severity and extent of the crisis (utilities, transportation fuel providers, security services).

(3) Key Findings

- The survey sample includes a broad range of businesses and, collectively, the responses represent a fairly complete assessment of critical industries and provide a “360 perspective” on likely impacts, interdependences and responses. Survey responses from a financial institution or large retailer would have strengthened the analysis.
- There appeared to be no correlation between the quality of a company’s response and its status as a “solution” or “non-solution” company — suggesting that a company’s “proximity to the problem” had no influence on its efforts (or lack thereof).[25]

III. A Collective Response Scenario

The extent to which a company will be affected by a widespread Internet outage and its subsequent response to the event is likely to be particular to the nature and structure of the individual business. Thus, the value of any one survey response is limited by the uniqueness of the company and the environment that it operates in on a daily basis. However, the collective response of a diverse set of companies representing a large cross section of the economy has the potential to paint a clear and compelling picture of what a widespread Internet outage might mean for the American businesses community and the functioning of the economy as a whole.

To capture this "wisdom of the crowd," responses were aggregated and linked according to the services or sectors that businesses expect to rely upon heavily during the scenario. Sectors characterized as vital to conducting business in a "pre-Internet" world were identified as potential stress points within the economy.

3.1 Potential Stress Points

- Telecommunication service providers will experience a surge in demand for services as most companies expect to revert back to pre-Internet technology (voice, fax, mail) for business operations and communication that would have otherwise taken place over the Internet.

- Financial institutions will need to go to manual, paper-based methods. The demand for liquidity may increase significantly, especially if there is a general panic, and the Fed may need to respond accordingly. With increased demand for cash, there may also be additional demands on physical security services.

- Telephone/fax equipment suppliers will be called upon to provide new equipment as companies revert back to pre-Internet technology.

- Transportation fuel providers may need to enforce rationing and/or physical security measures at fuel stations depending on the nature of the crises and the public response (i.e., if there is a panic and stockpiling of essential goods).

- Internet service providers may be overwhelmed in the near-term as consumers demand service and information about the severity, extent and duration of the crisis. Restoration of service is likely to take place in stages and Internet service providers (ISPs) will need to prioritize customers.

- Network/IT service providers will be in high demand as companies look to technology experts to provide guidance on developing non-Internet-based workarounds and temporary solutions. IT security concerns may arise if companies feel obliged to give customers/suppliers access to their private networks.

- Software developers/distributors will need to rapidly develop and deploy software patches and other tools necessary to support daily operations and support the restoration process.

- Mail/Delivery/Shipment providers will be heavily relied upon as data and documents otherwise sent via Internet will need to be sent via courier, package delivery service or USPS. Capacity constraints could cause significant lags in delivery times.

- Printing service providers will need to meet an increased demand for invoices, forms and other paper-based documents that would otherwise be completed online.

- Office supply companies will experience a surge in demand as companies turn to paper-based methods of communication. Office supplies are likely to be in short supply in a prolonged outage.

- Data tape/disk suppliers will need to meet an increased demand for transferring and storing large amounts of data.

- Transportation networks are likely to become more congested as delivery services pick up, in-person meetings increase and work-at-home employees are forced to come into local offices to access private networks.

- Temporary workers will be in high demand as companies turn to relatively more "live" or "manual" measures for communication, processing and logistics. Companies will need to dramatically increase customer support representatives, sales associates, order processing assistants and mail service personnel. The competition for temporary labor will be fierce and processing errors will increase.

3.2 Key Findings

- The mass migration toward non-Internet methods of communications is likely to increase congestion and significantly impact all businesses, regardless of their direct level of dependency on the Internet.

- Maintaining continuity and minimizing economic losses will largely depend on the ability of key service providers to rapidly scale up operations and effectively satisfy a surge in demand. Should any one of these stress points fail, the economic losses will be greatly amplified.

- In particular, the continued functioning of the telecommunications and delivery services will be critical. Virtually all respondents cited increased reliance on conventional communication methods (voice, fax, mail), hinting at issues such as capacity constraints management, rapid resource deployment, quick scale-up of operations, and potential instability or system failure. As one respondent stated, "instability in the telecommunications sector following an Internet outage will severely disrupt all mitigating business continuity strategies, and perhaps result in anarchy."

- The likelihood of an "extreme scenario" will significantly depend on the extent of interdependencies between stress points, as well as the perceived source and intent of the "attack." For example, stockpiling and hoarding of fuels (including gasoline for cars and diesel for generators) could constrain operations in the transportation sector (including mail and delivery services) and limit the nation's ability to adapt to the crisis.

- Many survey responders indicated that government's role in providing clear communication, coordination and managing stress points will be paramount. This might include measures to maintain order, establish priority lists, "commandeer" certain sectors of the economy, or other measures necessary to avert or mitigate extreme outcomes.

IV. Types of Responses & Strategies

One possible framework for analyzing the wealth of information in the surveys is to examine companies' responses across three dimensions: mitigation, adaptation and resolution.

4.1 Mitigating Strategies: Proactive Measures Taken Before the Outage

- Maintaining satellite phones in headquarters and key offices to insure a minimal level of communication and reduce reliance on conventional telecommunication networks.

- Maintaining an up-to-date global contact directory, including cell phone numbers, which will be accessible offline.

- Developing a crisis management plan with clearly defined protocols and dedicated staff.[26]

4.2 Adaptation Strategies: Reactive Measures Taken in Response to an Outage

- Relying on the availability of conventional communication methods such as voice, fax and mail.

- Switching to paper-based methods of communication and processing.

- Hiring additional workers to handle increased manual processing and live customer support.

- Relying on the government (local, state and federal) and trade associations for support and guidance.

4.3. Resolution Strategies: Measures Taken to Directly Resolve the Outage

- Working with government agencies and other coordinating organizations to identify the problem and develop a restoration plan.

- Establishing restoration priority protocols.

- Developing and deploying new software and patches.

V. Key Themes

5.1 Dependencies

Companies will rely heavily on conventional methods of communication and processing until Internet service can be restored. This will put enormous stress on the telecommunications, mail/delivery and office supplies industries. Success at mitigating the economic impact of the outage will largely depend on the ability of these industries to successfully manage a surge in demand and sufficiently scale up operations using temporary labor and/or creative workarounds.

Recommendations: Companies should assess their direct and indirect level of dependency on the Internet to conduct various business operations and tasks, including potential dependencies that may be embedded in the operations of key suppliers and customers. Wherever possible, non-Internet based continuity and reconstitution plans should be developed and evaluated within the context of the "collective response scenario" presented above.

5.2 Expectations for Government

Companies expect government to play a critical role during the outage and assume a variety of responsibilities, including communication, coordination, security, management of priorities for scarce resources and the restoration process. Government also would be expected to provide relief, safe harbor and/or a grace period for satisfying mandatory reporting requirements.

Recommendations: To the greatest extent possible, federal and state government should communicate their priorities and expectations before a pervasive Internet outage occurs. Clearly established points of contact for both critical industries and the business community as a whole may minimize confusion and facilitate the rapid dissemination of credible information. Furthermore, the business community should engage government before a pervasive Internet outage occurs to understand how businesses might help authorities effectively respond to challenges within a particular area of expertise.

5.3 Customer Expectations

Companies have a diverse view of what customers will expect from them during the event. Some suggested that customers will expect a "business-as-usual" level of service, while others indicated that customers are likely to be more understanding.

Recommendations: Companies should examine their various customer bases and determine the likely needs of each segment during such an event. Those companies that can help business customers solve problems, including those not directly related to contracted services, will gain an edge over the competition. In particular, Business Roundtable members should be mindful of their leadership roles within their respective industries. As one respondent noted, small companies often look to big companies in times of crisis.

5.4 Conflicts & Inconsistencies

Companies cited a wide range of potential conflicts. Conflicting reporting requirements for the federal government were frequently mentioned, though most seem to expect that relief, safe harbor or grace periods will be instituted without controversy. Otherwise, most responses about conflicts were rooted in the fundamental observation that conflicts are likely to arise with increased resource scarcity — especially when speaking of key stress points such as telecommunications and delivery services.

Recommendations: Companies should identify likely conflicts in the event of a pervasive Internet outage and understand how those conflicts are likely to be resolved. Understanding where a company is likely to rank on supplier priority lists will be critical to developing flexible and realistic crises response strategies. Companies should also develop criteria and procedures for resolving conflicting interests among customers, with consideration for both short-term crisis management objectives and long-term business implications.

5.5. Source of Information

Companies intend to tap into a broad range of information sources. The government was frequently cited as a key and highly trusted source, although at least one company that would provide critical services during an outage suggested that government sources may fail to disseminate information in a timely manner. Others indicated that they would rely on their technology providers or telecommunication providers for credible information. At least one company's respondents admitted that they were unsure of how to plug into the reconstitution effort.

Recommendations: Companies should develop protocols for collecting, filtering and disseminating information during a major communication network disruption, including an Internet outage. Companies that both gather and disseminate credible information will satisfy an important need for suppliers, customers and employees. Companies within similar industries should establish protocols for sharing information with each other, as well as leverage industry knowledge to provide governments with technical expertise, advice and the business community's perspective where appropriate.

Scenario and Questions Sent to Selected Business Roundtable Companies

Scenario

A catastrophic Internet failure has occurred, and it is so large and widespread that no one company or industry sector can restore its operations to full capabilities without inter-industry and government collaboration. The event that caused the failure could be from either a cyber or physical incident or from a combination of the two. These incidents could result from intentional events such as a terrorist attack, unintentional events such as a catastrophic natural disaster, or software corruption. However, the incident also could be a combination of one or more interdependent catastrophic events that would compound the effects of an initial disaster.

The event is a worst-case scenario and would occur at the worst possible time for an organization or industry sector. As a result, many organizations would be unable to comply with contractual obligations, regulatory requirements or other external dependencies that rely heavily on the Internet. The period of complete disruption is expected to last at least four weeks — however, Internet functionality would be plagued with sustained technical disruptions for at least eight weeks and most likely longer.

Questions

1. What external assistance does your company want or need to restore and resume business operations? What will you need? Who can provide it? Assuming that the Internet is down but that your telecommunications system is operational, how would you get this assistance? And, if your company is likely to be part of the solution to a cyber outage, what will your customers and others expect from you, and how will you get it to them?

2. What demands, mandates or filings might be made on your organization from external organizations — public, private or regulatory — during this kind of a catastrophic Internet disruption? What will your customers expect from you?

3. Building on Question 2, what are possible conflicts or inconsistencies in the anticipated mandates or direction given to your organization?

4. How will your company plug into the government or non-governmental command-and-control structure during a major Internet outage? Who do you contact for assistance?

5. Building on Question 4, do you anticipate confusion surrounding critical sources of timely and actionable information, such as information from government agencies? How would you resolve and prioritize among multiple and uncoordinated sources of information that might undermine business operations? Is there one particular source that you weigh more heavily, and if so, please identify that source.

Appendix C

Contact Information for Information-Sharing Organizations

Following are links and contacts to facilitate information sharing and foster relationships across the private sectors and with the government.

US-Computer Emergency Readiness Team (US-CERT)
www.us-cert.gov

Information Sharing and Analysis Centers (ISACs)

- Chemical Sector ISAC
  Housed in the Department of Homeland Security's secure Homeland Security Information Network

- Communications ISAC
  www.ncs.gov/services.html

- Electricity Sector ISAC
  www.esisac.com

- Emergency Management and Response ISAC
  www.usfa.dhs.gov/fireservice/subjects/emr-isac/index.shtm

- Financial Services ISAC
  www.fsisac.com

- Highway Watch ISAC
  www.highwayisac.org

- Information Technology ISAC
  www.it-isac.org

- Multi-State ISAC
  www.msisac.org

- Research and Education Networking ISAC
  www.ren-isac.net

- Supply Chain ISAC
  https://secure.sc-investigate.net/SC-ISAC

- Surface/Public Transportation ISAC
  www.surfacetransportationisac.org

- Water ISAC
  www.waterisac.org

Government Programs

The following information is intended to provide a reference for some of the various government organizations and programs engaged in joint intelligence analysis and communication. More information on these programs/organizations can be found at www.dhs.gov.

- **Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)** — HITRAC develops products to help inform infrastructure owners and operators of any threats they may potentially face, as well as to better inform their security planning and investment decisions.
- **US-CERT Einstein Program (EINSTEIN)** — The US-CERT Einstein Program is an initiative that builds cyber-related situational awareness across the federal government. The program monitors government agencies' networks to facilitate the identification and response to cyber threats and attacks, improve network security, increase the resiliency of critical electronically delivered government services, and enhance the survivability of the Internet. Enhanced data sharing across federal government agencies and US-CERT provides an advanced cyber view and analysis of the federal government's critical cyber networks.
- **National Operations Center (NOC)** — The NOC is an around-the-clock all-hazards fusion center that collects and fuses information from more than 35 federal, state, territorial, tribal, local and private-sector agencies.
- **National Coordinating Center (NCC)** — The NCC's primary mission is to assist in the initiation, coordination, restoration and reconstitution of national security and emergency preparedness communications services under all conditions. During regular operations, industry and government representatives work together to produce and execute emergency response plans and procedures, and as part of its ISAC function, members regularly share information about threats and vulnerabilities.
- **National Cyber Response Coordination Group (NCRCG)** — Established in partnership with the Department of Defense and the Department of Justice in the National Response Plan's (NRP) Cyber Annex, the NCRCG serves as the federal government's principal interagency mechanism for coordinating the federal effort to respond to and recover from cyber incidents of national significance and includes 19 federal agencies, including the intelligence community. The Department of Homeland Security's National Cyber Security Division (NCSD) is working with industry to establish a private-sector counterpart to the NCRCG, which will communicate and collaborate with the federal government NCRCG during times of crisis.
- **National Cyber Alert System (NCAS)** — NCAS is America's first coordinated national cyber security system for identifying, analyzing and prioritizing emerging vulnerabilities and threats. Managed by US-CERT, a partnership between NCSD and the private sector, NCAS provides the first infrastructure for relaying graded computer security update and warning information to all users.

Appendix D

Assessing Internet Dependence — One Company's Approach

One of the biggest findings of Business Roundtable's research on businesses and their preparedness in the event of a cyber attack was that businesses were not always aware of their dependencies or vulnerabilities regarding the Internet. One of the participating companies identified a resource for helping their organization determine its dependencies and vulnerabilities. Below are the steps taken to complete the Internet Dependence Impact Analysis Matrix, which the company used to evaluate dependencies and vulnerabilities.

Using the Internet Dependence Impact Analysis Matrix

- The company recognized a need to investigate probable Internet vulnerabilities.
- All departments were encouraged to participate in a loss-of-service exercise based on an Internet disruption. Participation in this activity identified many applications and gaps.
- Further analyses of the financial impacts were completed for applications identified with regulatory or financial impacts. For shared applications, the analysis included costs for all departments.
- A set of requirements (or criteria) were developed to determine which gaps should be closed. Once the requirements were determined, a priority was determined for closing the gaps.
- All departments reviewed on an annual basis their business applications that relied on the Internet and made changes. This review was a joint effort between the business side of the operations and the technical side.
- The Internet Dependence Impact Analysis Matrix (see page 43) was used to evaluate the severity of the affected business and technical operations, and common findings were consolidated.
- Trends were identified and recommendations were made for further measures.

Defining Columns in the Internet Dependence Impact Analysis Matrix

- Business Application(s) Impacted — The application(s) that will be affected by the scenario (this could be the name of the vendor or provider of the application/data).
- Business Function(s) — If the application/data from/to this vendor is not available, what will be the technical impact to the systems that support the business area? Will the impact be high (H), medium (M) or low (L)?

- Customer Impact — What will be the impact to the customers of the business area? Who are the customers (policyholders, internal customers)? Will the impact be high (H), medium (M) or low (L)?
- Business Impact — What will be the impact to the internal operation of business area? Will the impact be high (H), medium (M) or low (L)?
- Regulatory Impact — What will be the impact on any regulatory issues (fines, etc.) on the business area? Will the impact be high (H), medium (M) or low (L)?
- Financial Impact — Will there be a financial impact on the business area? What is the cost estimate for that application outage (if possible to determine)?
- BCP Plan — Do you have a Business Continuity Plan (BCP) for this application disruption (i.e., have you thought about how you will handle that disruption)?
- BCP Plans Documented — Do you have the BCP written down (i.e., do you have a written document that outlines what you will do in the event of the disruption)?
- BCP Plans Tested — Have you tested the BCP?
- Notes — Enter any extra information in this column that you think would be helpful to note.

Internet Dependence Impact Analysis Matrix

Business Application(s) Impacted	Business Function(s) (H, M, L) H=High M=Medium L=Low	Customer Impact (H, M, L)	Business Impact (H, M, L)	Regulatory Impact (H, M, L)	Financial Impact (Y/N; Estimated Amount)	BCP Plan (Y/N)	BCP Plans Documented (Y/N)	BCP Plans Tested (Y/N)	Notes

Endnotes

1. Definition — "CIIs are communications or information services with the availability, reliability and resilience of which are essential for the functioning of the modern economy and of governments. CIIs also support other critical infrastructures, from power distribution and water supply to transportation, emergency services and finance." *World Economic Forum Global Risk Report 2006.*

2. Armed Forces Communications and Electronics Association, Homeland Security Conference, "Intelligence and Information Fusion ... Beyond Sharing," February 28-March 1, 2007.

3. U.S. Department of Commerce's Bureau of Economic Analysis, National Income and Product Accounts.

4. The World Bank, *World Development Indicators 2007,* www.worldbank.org/data/wdi.

5. Hal Varian, et al., *The Net Impact Study: The Projected Economic Benefits of the Internet in the United States, United Kingdom, France and Germany,* January 2002.

6. IT Facts, VoIP, www.itfacts.biz/index.php?id=P8340, April 27, 2007.

7. World Economic Forum, *Global Risks 2007: A Global Risk Report,* in collaboration with Citigroup, Marsh & McLennan Companies, Swiss Re and the Wharton School Risk Center, January 2007.

8. Refer to "Statement of General James E. Cartwright, Commander, United States Strategic Command Before the Strategic Forces Subcommittee, Senate Armed Services Committee on United States Strategic Command," on March 28, 2007, pp. 4-5; 11-12. General Cartwright compares nation-state cyber attacks to "pirates and train robbers of the past," but on a national and global scale.

9. Brian Cashell, et al., CRS Report for Congress, *The Economic Impact of Cyber-Attacks,* April 1, 2004, p. 2.

10. For example, Charles Billo and Welton Chang, Institute for Security Technology Studies at Dartmouth College, *Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States,* November 2004.

11. Clay Wilson, CRS Report for Congress, *Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress,* October 17, 2003, pp. 13-14.

12. Institute for Security Technology Studies, *Cyber Warfare,* p. 120.

13. Institute for Security Technology Studies at Dartmouth College, *Cyber Attacks During the War on Terrorism: A Predictive Analysis,* September 22, 2001, pp. 12-14.

14. Institute for Security Technology Studies, *Cyber Warfare.*

15. Refer to "Statement of General James E. Cartwright, Commander, United States Strategic Command Before the Strategic Forces Subcommittee, Senate Armed Services Committee on United States Strategic Command," on March 28, 2007, pp. 4-5; 11-12. General Cartwright compares nation-state cyber attacks to "pirates and train robbers of the past," but on a national and global scale.

16. Robert F. Wescott, Sandy MacFarlan and Mark W. McNulty, *The Potential Economic Impact of a Prolonged Internet Outage: An Analysis Prepared for the Business Roundtable Cyber Security Working Group,* May 2007.

17. Cashell, et al., *The Economic Impact of Cyber-Attacks.*

18. *Ibid.*

19. Scott Dynes, Eva Andrijcic and M. Eric Johnson, Dartmouth College's Tuck School of Business and University of Virginia's School of Engineering, *Costs to the U.S. Economy of Information Infrastructure Failures: Estimates from Field Studies and Economic Data.*

20. Extrapolated from the "Scenario" box on page 14 of this report.

21. See Appendix A.

22. The McKinsey Quarterly, *How Businesses Are Using Web 2.0: A McKinsey Global Survey,* 2007, p. 1.

23. For example, during Hurricane Katrina, state and local officials were frustrated by the federal command structure. There were multiple Federal Coordinating Officers with varying levels of authority, resulting in confusion around whose commands or directions should be followed. Homeland Security Council, *The Federal Response to Hurricane Katrina: Lessons Learned,* February 2006, p. 42.

24. See Appendix B.

25. The term "correlation" is not used here in a statistical sense, as the nature of the survey and sample size precludes any meaningful quantitative analysis. Rather, it is used to indicate a subjective assessment of a trend's presence.

26. Based on survey responses, these crisis management plans appear to be primarily tailored to security events and natural disasters (e.g., 9/11 or Hurricane Katrina). However, the challenges that arise from a widespread Internet outage are likely to be significantly different than those that arise from "conventional crises." With this in mind, companies may consider conducting an analysis that identifies the key characteristics of conventional crises and contrasts them with those of a widespread Internet outage. This process might lead to the identification of important issues particular to an Internet outage scenario and that companies might account for in their crisis management planning.

Business Roundtable℠

1717 Rhode Island Avenue, NW
Suite 800
Washington, DC 20036-3023

Telephone 202.872.1260
Facsimile 202.466.3509
Website businessroundtable.org