Business Roundtable

Essential Steps to Strengthen America's Cyber Terrorism Preparedness

New Priorities and Commitments from Business Roundtable's Security Task Force

June 2006

Business Roundtable

Business Roundtable (www.businessroundtable.org) is an association of chief executive officers of leading U.S. companies with over $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 nearly a third of all corporate income taxes paid to the federal government. Collectively, they returned more than $110 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 $86 billion in annual research and development spending — nearly half of the total private R&D spending in the U.S.

Essential Steps to Strengthen America's Cyber Terrorism Preparedness

New Priorities and Commitments from Business Roundtable's Security Task Force

A White Paper by Business Roundtable | June 2006

Table of Contents

I. Introduction and Background

The Internet and its communications infrastructure serve as the critical backbone of information exchange that is vital to our nation's security and our economy. Yet the United States is not sufficiently prepared for a major attack, software incident or natural disaster that would lead to disruption of large parts of the Internet.

Despite a series of efforts in recent years to address this issue, significant gaps exist in the response plans of the U.S. government and the private sector for reconstituting the Internet in the event of an unprecedented massive Internet disruption.

The uninterrupted use of the Internet is essential to the continuity of our nation's economy. For this reason, Business Roundtable's chief executive officers (CEOs), who represent 160 leading U.S. companies, made fortifying the Internet and the infrastructure that supports Internet health one of the main priorities in 2005.

The CEOs urged an examination of preparedness as well as Internet-restoration capabilities. The Roundtable hosted member and nonmember companies to explore various dimensions of the problem, including a review of government plans in an effort to understand the federal government's commitment, funding and preparation for a major cyber disruption. The Roundtable's review found that there are no well-coordinated processes that would integrate the disparate plans of industry and government to restore Internet functioning.

Progress has been made over the past 10 years on technical issues, such as establishing computer security readiness teams in government and gaining a better understanding of cyber risks across the industry and government, but strategic management and governance issues have yet to be addressed. These include ways to reconstitute the cyber economy and shore up market confidence after a widescale Internet failure. Unaddressed strategic issues also include the types of leadership and management challenges government and industry leaders faced after Hurricane Katrina.

Should a cyber attack or massive Internet failure occur, well-intentioned government officials and industry leaders are not currently in a position to synchronize efforts and deploy coordinated and tested capabilities to restore Internet services.

In addition, the nation's political and business leaders are not prepared to manage public trust issues, such as confidence in the markets, in the event that cyber-restoration efforts are unsuccessful or appear uncoordinated.

Although experts disagree about the likelihood of a wide-scale cyber disaster, they do agree that the risks and potential outcomes are serious enough to mandate careful preparation and planning. The Roundtable believes that business and government must take action — individually and collaboratively — to address this issue.

In Section III, the Roundtable offers business and government leaders specific recommendations designed to:

- Improve the ability to identify and assess strategic threats and provide early warning;
- Better coordinate reconstitution responsibilities of both the public and private sectors; and
- Ensure that necessary commitments and investments are made in the institutions that will play critical roles in reconstituting the Internet infrastructure.

Unlike the nation's response to Hurricane Katrina, which was centered on the government's role, industry must undertake principal responsibility for reconstituting the communications infrastructure, including telephony, Internet and broadcast media. The Roundtable's analysis highlights the need to further explore consolidation of response programs and to negotiate additional mutual aid agreements in the critical infrastructure community.

Developing a private sector/government partnership focusing on an appropriate response program will enhance our nation's cyber-response position. The federal government should take action to redefine roles and responsibilities, fund long-term programs, and treat potential Internet disruptions as a serious national problem.

Without these changes, our nation will continue to use ad hoc and incomplete tools for managing a critical, national risk to the Internet.

The Problem: Our Nation Is Unprepared to Reconstitute the Internet after a Massive, Nationwide Disruption

To date, the United States has not experienced a massive Internet disruption in which government, industry and others that use the Internet for critical purposes are unable to access services for days, weeks or even months. The United States has not experienced a coordinated and well-funded attack, a malicious or accidental introduction of flawed software into key components of the Internet backbone, or a catastrophic natural disaster that exceeds Hurricane Katrina's impact on the Internet. A coordinated physical attack against multiple critical information technology (IT) facilities that support Internet services could also hamper reliable high-speed service.

Currently, government agencies are responsible for various aspects of Internet security, functionality and use, such as early warning communication and coordination within the government during a significant attack. However, agencies have failed to institutionalize the provision of these services to a wider audience, such as through the creation of a formal doctrine on roles and responsibilities. There is no national policy on why, when and how the government would intervene to reconstitute portions of the Internet or to respond to a threat or attack.

The National Response Plan (NRP) represents a positive effort by the federal government to address several of these important issues. The plan creates a new organization — the National Cyber Response Coordination Group (NCRCG) — and suggests that it is accountable for coordinating a response to Internet emergencies. However, few outside a small group of government officials know much about NCRCG and its authority over coordinating efforts in government and across the business community. The role of the Defense Department is even less clear.[1]

From the private sector's perspective, individual companies may have adequate plans for their own business interests, but the private sector as a whole is unprepared to work together on a wide scale. No single critical infrastructure sector owns, operates and uses the Internet. Even within the communications sector, different organizations manage restoration and reconstitution efforts, and in some cases, there are too many organizations without appropriate levels of accountability and responsibility.

Furthermore, the business community has no overarching governance strategy or program to coordinate efforts to respond to a catastrophic cyber event, to triage the most serious matters or to assign responsibility for specific issues.

In sum, the nation is unprepared to set in motion the kind of coordinated response needed to repair Internet infrastructure in the event of a massive Internet disruption. Ensuring clear leadership and management necessary to reconstitute the Internet will require the attention of the nation's senior leadership in the public and private sectors. Since Y2K, both government and industry have worked to resolve Internet-reconstitution challenges. However, in light of the lack of capabilities and clarity of purpose, efforts to become better prepared appear inadequate.

Stakes Are High for Economic Security and Preparedness

Our nation's critical infrastructure and economic engine depend increasingly upon reliable, survivable and available Internet services. Companies that supply financial services, transportation, health care, and other essential products and services have become dependent on access to the Internet. As the integration of voice and data onto a common IP-based backbone increases, a significant disruption would impair voice services as well as the Internet and data messaging.

Our nation's ability to support the public's safety, health and welfare is also at risk from a nationally significant Internet disruption. The public health response is heavily dependent on the Internet in ways not predicted by the government's response plans. First responders use the IT infrastructure heavily to coordinate for and manage catastrophic events — whether to dispatch emergency personnel; communicate with law enforcement, health and fire professionals; or even track essential supplies and goods via a Global Positioning System (GPS).

Public trust and confidence in the markets are also at risk from a major cyber event. A long-term Internet disruption would undermine the public's trust and confidence in both the government and industry. Citizens obtain crisis information from many sources, including TV, radio and the Internet. An inability to reconstitute the Internet would block citizen access to data from the Internet. In addition, the government might not be able to gather facts for alerts and warnings, commu-

nicate such data across government agencies, and disseminate warnings and alerts to citizens. The news media might also be unable to obtain and disseminate information through the Internet.

Roundtable Role: Identify Gaps and Recommend Solutions

Business Roundtable's Security Task Force identified Internet reconstitution as a priority and launched a cyber-reconstitution initiative. Throughout 2005, the Roundtable convened a series of meetings and conference-call discussions with key players in the industry, including Roundtable member and nonmember communications providers, IT companies, and end users.

In addressing fortifying and reconstituting the Internet, the Roundtable's goal is not to outline all of the details that must occur or to represent the business community in reconstituting the Internet in the event of an attack or significant disruption. Rather, the Roundtable's sole purpose is to identify gaps in our nation's ability to effectively manage a reconstitution effort following a catastrophe and offer strategic recommendations for filling those gaps.

II. Significant Cyber Gaps

The Roundtable's review of Internet-response programs highlights three significant gaps in our nation's ability to reconstitute the Internet following a major disruption.

Gap Number 1: Lack of Formal "Trip Wires" to Indicate an Attack Is Under Way

Our nation lacks a mechanism to identify potential Internet emergencies prior to an attack or disruption. These so-called trip wires, when invoked, should precipitate agreed-upon protocols and thresholds that indicate an attack is under way or a disruption is imminent. Such trip wires are an essential ingredient in preparedness and reconstitution given the velocity of Internet attacks — far less than the 24 to 72 hours provided in advance of a hurricane — and for clarifying who is expected to do what, when and where.

Our nation relies extensively on long-standing programs to provide advance warnings for certain types of natural disasters. These warnings are government sanctioned and widely supported, as broadcast radio and TV stations recognize the validity of the alerts. In August 2005, the National Weather Service (NWS), for example, issued several alerts to the citizens of Florida and the Gulf Coast states well in advance of Hurricane Katrina. Advance alerts in September 2005 provided time for residents and vacationers in the Florida Keys to evacuate in a timely and calm manner in response to Hurricane Rita. These alerts allow citizens and businesses to undertake preventive measures and to set in motion response and reconstitution programs.

Similar advance-warning mechanisms do not exist for the Internet. Those who maintain the IT infrastructure need global trip wires to ensure the well-being of the Internet should a massive disruption or cyber attack come from overseas. Without adequate trip wires, the government, businesses and citizens lack the ability to anticipate when coordinated mitigation strategies are needed or understand if or how government might intervene.

Gap Number 2: Lack of Accountability and Clarity on Which Institutions Provide Reconstitution Support

The Roundtable's analysis found that there are too many institutions, both public and private, with unclear or overlapping responsibilities chartered to manage aspects of Internet reconstitution. This proliferation of security institutions has, ironically, undermined our nation's ability to restore Internet services.

In other areas of security and preparedness, our nation has designated a single institution that provides certain services. As an example, in addition to the NWS, which provides advance warning of major weather-related threats, the Centers for Disease Control (CDC) coordinates across 50 states in managing outbreaks of the most infectious diseases. In the event of a pandemic flu outbreak, public and private entities across all 50 states know that the CDC will integrate reports on the avian flu and undertake full responsibility for sharing relevant information.

However, the roles are less clear and less defined for reconstituting the Internet, as both government and industry offer similar solutions. The industry-based Information Sharing and Analysis Centers (ISACs), for example, have charters to monitor threats, vulnerabilities and incidents. In addition, the Internet industry typically responds to Internet threats at the technical level by working together through the North American Network Operators' Group. Critical infrastructure companies are often split on which institution to join, how best to collect data on cyber-based risks and where to obtain a trusted source of data without taxing limited resources. The National Communications System (NCS), under the Department of Homeland Security (DHS), and the National Cyber Security Division (NCSD), which includes the U.S. Computer Emergency Readiness Team (US-CERT), have overlapping and conflicting responsibilities while making artificial distinctions between communications, IT and the Internet. The NCS also manages the Alerting and Coordination Network (ACN), while NCSD oversees portions of the Homeland Security Information Network (HSIN).

The Roundtable's gap analysis identifies serious problems stemming from the lack of consolidation, including the fact that these organizations are not accountable for their actions. Many of the organizations that are serving the critical

infrastructure are steeped in voluntary activities, relying on "trust models" rather than formal management arrangements with clearly defined accountability. Whether they share data, provide restoration support or coordinate with other groups is not typically written into contract or recognized by law.[2]

Gap Number 3: Lack of Resources for Institutions that Must Reconstitute Internet Infrastructure

The Roundtable believes it is important to explore whether sufficient resources and support exist for institutions that provide Internet-reconstitution services, such as the NCSD and US-CERT, which is identified in the NRP as the key point of contact for cyber reconstitution. Congress funds US-CERT at approximately $70 million annually, which is less than 0.2 percent of DHS funding. In addition, almost none of the NCSD's funding is targeted for cyber-reconstitution support.

Private sector entities responsible for Internet reconstitution must contend with resource limitations, as well. For example, telecom carriers and Internet service providers (ISPs) that must restore services rely heavily on access to diesel fuel. However, the government has not developed a diesel prioritization. There are other similar resource issues, including out-of-band communications, addressed further in Roundtable Recommendations.[3]

III. Roundtable Recommendations

To address these gaps identified by the analysis, Business Roundtable recommends the actions covered below.

The private sector must undertake most of the responsibility for fixing weaknesses in key Internet assets. Business executives are dependent on a patchwork of public- and private-response programs to restore Internet infrastructure services. In many cases, these programs are not fully coordinated via a central organization. Immediate- and long-term commitments to change the current reality should include the following steps:

- **Establish a single point of contact and responsibility for government interaction.** Executives must appoint a single management professional (or corporate office) to coordinate Internet restoration in the company and with responsible government officials. In many cases, government decisionmakers must navigate across various corporate offices, undermining efficient restoration activities. This appointee should be responsible for quickly learning existing government protocols and programs. CEOs must clearly define expectations, roles and responsibilities in the event of a widespread Internet disruption. Companies must also provide ample resources so that managers can coordinate within the company, across the private sector and with the government.

- **Set strategic needs and direction.** In addition to creating a single manager responsible for coordinating Internet restoration within the company, corporate executives must also develop a strategic plan that accounts for the movement of goods and services, corporatewide priorities for Internet services, and restoration of corporate communications.

- **Consolidate early warning and response organizations.** The private sector has created institutions to respond to communications disruptions. However, the gap analysis for this initiative concludes that there is confusion about multiple organizations with overlapping responsibilities. In addition, some of these organizations are founded on trust models, where actions during emergencies are not required or part of an industrywide

agreement. The private sector must change this by limiting the number of authorized institutions, shoring up membership of resulting institutions, and crafting agreements so that response activities can occur in a predictable and disciplined manner.

Ultimately, networking early warning and response efforts must also occur in a seamless manner. Thus, even if industry leaders choose to rely on more than one organization for early warning and response services, we must find ways to fabricate a single, consolidated reconstitution process. This process must account for a wide range of strategic needs (e.g., roles and responsibilities in the event of a national outage) and operational challenges (e.g., how to communicate with the right people at the right time). Dependability and clarity can occur across different industry centers through business rules, finely honed memoranda of agreement or mutual aid agreements.

Irrespective of the format, our industry-populated centers must undertake full and transparent responsibility for fulfilling national goals for reconstituting the Internet.

- **Agree on an information-sharing mechanism.** Industry must consolidate into a single information-sharing framework for early detection, response and reconstitution of the Internet. Currently, there are information-sharing programs for different ISACs, for the HSIN tool deployed by the federal government and for other ad hoc organizations that are based in academia or the not-for-profit community. Industry leaders, individually or via entities such as the NCC-Communications ISAC, must work to consolidate these protocols and present a formalized process to the government for formal recognition.

The federal government should complete response plans by defining key terms and responsible parties. Clearly, the federal government must continue to prioritize threats from weapons of mass destruction, such as biological or nuclear weapons, as well as catastrophic natural disasters. However, the government's policies should fully and completely address reconstitution of the Internet given the catastrophic damage that could result from an

Internet attack. Establishing clarity, responsibility and accountability would not undermine other priority programs. Specifically, the federal government's strategy should incorporate the following:

- **Communicate the government's policy for reconstitution of the Internet.** The gap analysis suggests that the federal government has no clearly defined policy for reconstituting the Internet in the event of a massive disruption. Such a policy should:
  - Determine the role and responsibility of DHS in supporting reconstitution activities.
  - Detail as much as possible the role and responsibility for US-CERT as the office in DHS responsible for cyber security.
  - Ensure that US-CERT has statutory and regulatory authority to implement its responsibilities, as well as sufficient funding.
  - Specify how DHS principals will use the Homeland Security Operations Center, if at all, to coordinate complex cyber-reconstitution actions — even where restoration is occurring as the result of a natural disaster or accident and not an attack.
  - Explain the role of regulators, such as the Federal Communications Commission (FCC) or sector-specific agencies (such as those in the financial services sector). In particular, the administration needs to explain how the FCC will operate once a critical warning occurs and in the aftermath of an event, and how the FCC coordinates with DHS and other entities. Since Hurricane Katrina, the FCC has created the Public Safety and Homeland Security Bureau, which is charged with helping to manage a massive Internet disruption. There is no guidance, however, on how the FCC's evolving responsibilities duplicates DHS' mission and operations.
  - Explain the role and responsibility of the Federal Emergency Management Agency (FEMA) and how it will operate during a cyber event of national significance. If a disaster declaration is approved, there is no clarity about how the emergency support functions (ESFs) — other than the communications ESF — operate to support reconsti-

tution following a cyber event. Similarly, DHS should clarify the roles and responsibilities for the White House prior to and in the aftermath of a disruption. For example, if a disruption is global, how will roles and responsibilities differ for the Homeland Security Council and National Security Council? DHS should explain the roles and responsibilities of other entities, including the State Department, Department of Defense and others with global responsibilities to manage global incidents.

- **Fix the NRP's Cyber Annex.** The administration should review the NRP and immediately make changes that reflect the administration's policy. At a minimum, the administration should define key assumptions and statements directly in the NRP, which includes the Cyber Annex. For example, the administration states that it has the authority to declare a cyber emergency and will consult with industry leaders. The administration should set forth the factors for declaring such an emergency and the details of what aspect of the industry DHS will consult. It should define the roles and responsibilities of various government entities — such as the NCSD, NCS, FCC and the White House's Office of Science and Technology Policy (OSTP).

- **Develop a national economic recovery system.** The gap analysis suggests that the sole use of the NRP for cyber events might not be the most prudent course of action. The NRP has worked successfully at times for natural disasters and terrorist attacks. However, more than any other critical infrastructure, Internet disruptions can raise serious market concerns, undermine the delivery of critical business services and harm the economy. The Roundtable recommends developing a separate planning mechanism that allows final decisionmakers to balance the priorities of first responders with those of more sophisticated market issues.

The private sector and the government should cooperate to create joint public and private programs and institutions. The Roundtable's gap analysis identified strategic gaps that require joint collaboration across the critical infrastructure sectors, with government and partners in academia. These coordinated efforts would seek to accomplish the following:

- **Improve the ability to warn globally about Internet attacks.** Government, industry and academia must come to terms with the lack of clarity surrounding early warning mechanisms and services. The Roundtable recommends that the administration direct appropriate entities to prepare documentation to clarify roles and responsibilities for early warning systems. The Roundtable also recommends that DHS' chief financial officer and business office commit to funding US-CERT (or some other entity) to provide these and other services. At this time, neither DHS nor US-CERT has set forth, in clear and unmistakable language, how the federal government will identify trip wires and share such findings with appropriate industry stakeholders. Nor are such services amply funded within DHS.

- **Increase the ability to respond quickly.** The initial 24 hours after a major cyber disruption is identified may determine the success of protective actions as well as reconstitution. As the nation consolidates and authorizes institutions to manage reconstitution, efforts must immediately focus on how best to coordinate the initial actions once a threat is identified. Also, the Roundtable recommends that the stakeholders immediately clarify who is responsible, whether in industry or government.

- **Create a panel of subject matter experts.** The Roundtable recommends that Congress, the administration, industry and academia immediately resolve the lack of formally recognized subject matter experts that can help restore Internet services in the event of a massive disruption. Both public and private sectors point to available expertise to serve as subject matter experts, such as the National Infrastructure Coordinating Center (NICC) in DHS. Other groups, such as the NCC-Communications ISAC and IT-ISAC, also offer expertise. However, there is no single, agreed-upon center of such support, with business rules and relevant agreements on how experts will be called on to provide support. Congress must also authorize and appropriate funds for support — whether in the form of NET Guard or some other format.[4]

- **Exercise, train and develop processes from lessons learned.** The Roundtable recommends that DHS and industry institutions create formal processes to exercise and train for Internet-reconstitution emergencies. At

this time, there are no formal programs; DHS is in the process of creating a large-scale cyber exercise, but we will need several exercises that focus on various goals and objectives. Lessons learned for each is required as is a governance process to ensure that lessons are integrated into formal programs and procedures, whether in government or industry.

- **Develop a joint program to shore up market confidence.** The public and private sectors must have a single plan for shoring up the financial markets and public trust and confidence following an event. Lessons learned from Hurricane Katrina suggest that political and business leaders must consider, in advance, how they intend to respond prior to and in the aftermath of a major cyber disruption.

- **Provide effective oversight and strategic direction.** To date, Congress has not outlined its oversight role with regard to Internet reconstitution. The Roundtable recommends that Congress work more closely with the administration and industry to develop a strategic agenda. The Roundtable also believes that there are long-term funding needs that must be met. In many cases, the funding required is not substantial. For example, funding for communications capabilities, such as the ACN, HSIN and the Critical Infrastructure Warning Information Network (CWIN) should be consolidated into a single, reliable capability essential to meet cyber-reconstitution goals. However, these programs overlap, have had to fight for resources internally at DHS and are not receiving the attention required given the importance of the Internet. Congress must carve out an oversight and legislative agenda to meet these short-term needs as well as other long-term challenges.

IV. Conclusion

The lack of a national policy on Internet reconstitution could undermine the economy and the security of the nation. The gaps identified from this analysis, as well as the possible solutions, do not require extensive funding. In addition, implementation of these recommendations does not require massive reorganization of the government.

Instead, both the public and private sectors must commit to focus their efforts and funding on specific capabilities to have strategies and plans in place to reconstitute the Internet following a significant disruption. A coordinated response will help our nation and our economy recover more quickly following a cyber attack.

Endnotes

1. The government completed a large-scale exercise in February 2006 known as Cyber Storm. Cyber Storm was the first, full-scale government-led cyber security exercise to examine response, coordination and recovery mechanisms to a simulated cyber event — including an Internet disruption. The war simulation included international, federal, state and local governments, in conjunction with the private sector. In total, 115 public, private, and international agencies, organizations, and companies were involved in the planning and implementation of Cyber Storm.

2. The Roundtable's gap analysis uncovered important exceptions to this observation, such as the Telecom ISAC, which is recognized, responsible and accountable for specific restoration actions.

3. The administration's CWIN was created as a stopgap measure to provide out-of-band communications support among owners of critical IT infrastructure. A lack of funding and congressional support for the program will undermine access to such communications tools in the long run.

4. The DHS was authorized by the Homeland Security Act of 2002 to establish the National Emergency Technology Guard (NET Guard). NET Guard is designed to keep reserves of local volunteers with science and technology expertise who can repair communications networks in their local communities during a disaster.

Business Roundtable

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

Telephone 202.872.1260
Facsimile 202.466.3509
Website businessroundtable.org