Business Roundtable

Strengthening America's Cyber Preparedness: Essential Steps for the Public Sector and the Private Sector

Before the Senate Homeland Security and Governmental Affairs Subcommittee on Federal Financial Management, Government Information, and International Security

July 28, 2006

Karl Brondell
State Farm Insurance Companies
on Behalf of Business Roundtable

Testimony and Comments for the Record

Business Roundtable
1717 Rhode Island Avenue, Suite 800
Washington, D.C. 20036
Telephone: (202) 872-1260

Introduction

Thank you for this opportunity to testify today on Internet recovery on behalf of State Farm Insurance Companies and 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. Our 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.

Following the 9/11 attacks on the World Trade Center and the Pentagon, Roundtable CEOs formed the Security Task Force to address ways that the private sector can improve the security of employees, facilities, communities and our nation. The Roundtable believes that the business community must be a partner with government in disaster preparedness and response because more that 85 percent of the nation's critical infrastructure - power grid, financial services, information services, railroads, airlines and others - is owned and operated by the private sector.

The Roundtable commends the Subcommittee and its members for their interest in improving procedures and preparedness to ensure recovery of the Internet following a major disruption. Hardening the Internet and strengthening cyber security is one of the priorities of the Security Task Force, which is chaired by Frederick W. Smith, Chairman, President & CEO, FedEx Corporation. The working group focusing on cyber security issues is led by State Farm's Chairman and CEO, Edward B. Rust, Jr.

Preparing for Internet Recovery

More than a year ago, the Roundtable began work on an initiative to assess the public sector and the private sector plans and procedures for Internet recovery following a cyber catastrophe. We have just produced a report, *Essential Steps to Strengthen America's Cyber Terrorism Preparedness*, which identifies significant gaps in our nation's preparedness. The Roundtable has provided copies of our report to the Subcommittee, others in Congress and to the Department of Homeland Security.

The Roundtable's analysis finds that the United States is ill-prepared for a cyber catastrophe, with significant ambiguities in public and private sector responses that would be needed to restore and recover the Internet following a disaster.

As the Subcommittee knows, the uninterrupted use of the Internet is a crucial issue for our national and homeland security. The Internet and cyber infrastructure serve as a critical backbone for the exchange of information vital to our economic security. But our analysis has exposed significant weaknesses that could paralyze the economy following massive disruption – regardless of whether this is caused by a terrorist attack or a natural disaster.

Progress has been made over the past decade on technical issues. The Department of Homeland Security, for example, has established a computer security readiness team and is fostering a more sophisticated understanding of cyber risks that could adversely affect the nation's security. However, other issues have not been addressed in government or industry, such as strategic management and governance issues around reconstituting the economy and shoring up market confidence after a wide-scale Internet failure..

Three Gaps in Plans for Restoring the Internet

The Roundtable's report identifies three significant gaps in our nation's response plans to restore the Internet:

- **Inadequate Early Warning System** – First, we found that the U.S. lacks an early warning system to identify potential Internet attacks or determine if the disruptions are spreading rapidly across critical systems.

- **Unclear and Overlapping Responsibilities** – Second, public and private organizations that would oversee restoration and recovery of the Internet have unclear or overlapping responsibilities, resulting in too many institutions with too little interaction and coordination.

- **Insufficient Resources** – Finally, existing organizations and institutions charged with Internet recovery have insufficient resources and support. For example, only a small percentage of the National Cyber Security Division (NCSD)'s funding is targeted for support of cyber recovery.

Collectively, these gaps mean that the U.S. is not sufficiently prepared for a major attack, software incident or natural disaster that would lead to disruption of large parts of the Internet – and our economy. If our nation is hit by a cyber catastrophe that wipes out large parts of the Internet, there is no coordinated, public-private plan in place to restart and restore it. A cyber disaster could have immediate and nationwide consequences to our nation's security and economy, and we need to be better prepared.

Let me make one other point. Although there is no agreement among experts about the likelihood of a wide-scale cyber disaster, they do agree that the risks and potential outcomes are serious enough to mandate careful planning and preparation.

Recommendations for Government and Business

In my remaining time, let me talk briefly about our recommendations for government and business to improve identification and assessment of cyber disruptions, to coordinate responsibilities for Internet reconstitution, and to make needed investments in institutions with critical roles in Internet recovery.

We believe it is important to understand that response and recovery to a cyber disaster will be different from natural disasters, when the federal government has the leading role. Industry must undertake principal responsibility following an incident for reconstituting the communications infrastructure, including telephone, Internet and broadcast.

We believe that business and government must take action – individually and collectively – to address these issues. Let's start with government. The Roundtable calls on the federal government to establish clearer roles and responsibilities, fund long-term programs, and ensure that national response plans treat major Internet disruptions as serious national problems. For example, while the Administration says that it has authority to declare a cyber emergency in the National Response Plan -- and will consult with business leaders as part of the declaration, it is not clear how this consultation will occur or what the factors are for declaring an emergency. Nor has Congress clearly authorized the US-Computer Emergency Readiness Team in the Department of Homeland Security to engage in these activities.

Regarding the private sector, our report urges companies to designate a point person for cyber recovery, update their strategic plans to prepare for a widespread Internet outage and the impact on movement of goods and services, and set priorities for restoring Internet service and corporate communications.

But when it comes to protecting our nation – our employees, customers, facilities and communities – the federal government cannot do it alone, and neither can business. The best security solutions will come from a public-private partnership that identifies and acts on ways to improve collaboration. Let me discuss just a few of our recommendations:

- First, since the first 24 hours after a major cyber disruption often determine the overall success of recovery efforts, we must focus more attention on coordinating initial efforts to identify when an Internet attack or disruption is occurring.

- Second, we recommend the creation of a federally-funded panel of experts – from business, government and academia – who would assist in developing plans for restoring Internet services in the event of a massive disruption.

- Finally, we believe that the Department of Homeland Security, together with business, should conduct large-scale cyber emergency exercises, with lessons learned integrated into programs and procedures. These exercises should include senior government and business executives who are fully authorized to act during a cyber emergency and are accountable either to shareholders and boards of directors or, for government, senior political leadership.

Without these changes, our nation will continue to use ad hoc and incomplete tools for managing a critical risk to the Internet – and to our nation's economy and its security.

Future Business Roundtable Plans

Up to this point I have outlined for the Subcommittee the basis of our observations and our recommendations for government and business to consider. Now I want to spend just a moment telling you about the Business Roundtable's plans to find solutions to the gaps that we identified.

As an extension of our previous work, the Roundtable will examine coordination processes, protocols and practices across the private sector before, during and after a disruptive event. First, let me say that we are confident that our member companies are able to manage through most disruptions that affect regional, national and global Internet operations. For this reason, the Roundtable will focus its efforts on those large-scale events that no single company is positioned to manage absent widespread cross-industry collaboration in areas such as information sharing and technical support from subject matter experts. We will assess protocols on which institutions respond, but also will look at how early warnings are established as well as how companies access information and service critical disruptions in emergency situations.

As I noted a moment ago, the Roundtable's review found that there are multiple institutions formally charged with public-private collaboration – with overlapping roles and responsibilities. The Roundtable expects to conduct a rigorous analysis which will depict areas that require consolidation, refinement or creation of new public-private collaboration. We believe this will provide a foundation for meaningful improvements in our nation's ability to protect and restore the necessary Internet infrastructure as well as clarify specific, meaningful and actionable decisions that will lead to well-coordinated response and reconstitution processes.

Conclusion

In conclusion, let me again thank the Chairman and the Subcommittee for the opportunity to present Business Roundtable's report on cyber preparedness and to discuss our recommendations for improvements.

Roundtable CEOs believe strongly that we need a national response to this challenge, not separate business and government responses – and that means better collaboration. Most important, we must start immediately. Because of the widespread consequences of a massive cyber disruption, our nation cannot wait until an incident occurs to start planning the response.

And I assure you that America's CEOs and our companies are committed to do our part.