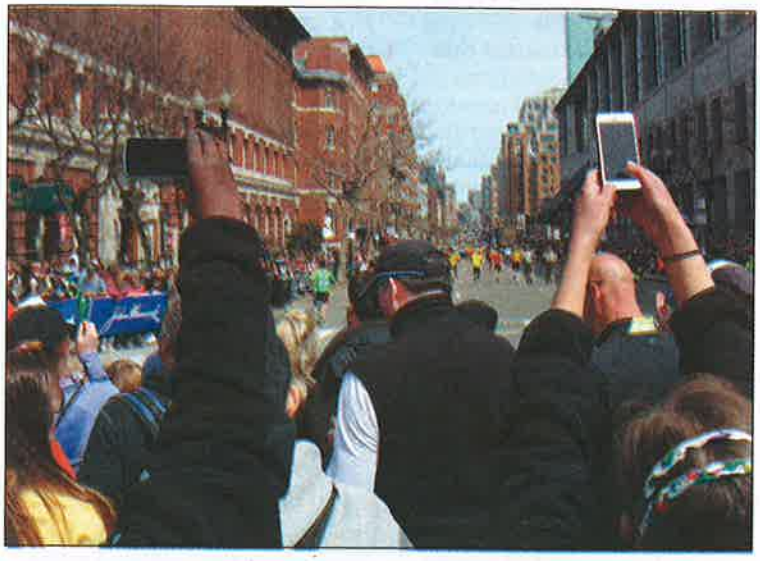
MIKE MCCONNELL

On Cybersecurity, Nation Needs 'Meta-Leadership'

When tragedy struck the Boston Marathon, law enforcement and national security officials sifted through untold amounts of information and identified suspects within three days. Data came from literally everywhere: video from business-owned cameras; individual bystanders' cellphone pictures, information from the media and large amounts of material collected by investigators themselves.

Information was shared from multiple public and private sources, analyzed and acted on instantly. It was a real-time case study, unfolding before the eyes of the world, about the power of information sharing – and it illustrated the critical role information sharing must play to prevent cyberattacks and cyberespionage that could lead to another kind of devastation.

In February, President Barack Obama issued an executive order to set up a structure for information sharing between the public and private sectors, and the House of Representatives just passed another version of cyber legislation to enhance protections when information is shared. But both of these efforts face obstacles in the debates over privacy and the fear of regulation — unless effective leaders step forward.



AP

Spectators take cellphone pictures of the Boston Marathon on April 15, before two bombs exploded at the finish line. Information sharing among police and public played a key role in identifying the bombers, the author writes.

If these efforts fail to achieve their purpose of significantly enhanced information sharing between the government and private sectors, the nation will achieve some limited kind of information sharing, but it will come in response to a major attack, and the plan will be assembled quickly and haphazardly after the fact. The nation will get a solution: a patchwork solution — something we should work now to avoid.

Today, under the president's order, leadership of the effort to collaboratively develop a Cybersecurity Framework with the private sector has been assigned to the National Institute of Standards and Technology, under the Department of Commerce.

NIST is an excellent arbiter of the technical details, but the political skills and the market understanding required for this

See **CYBERSECURITY** on Page 24

Patchwork Strategy Is Not Nearly Enough to Combat Cyberthreats

From **CYBERSECURITY** on Page 23

task represent a significant new challenge to its team.

The National Preparedness Leadership Initiative at Harvard has done extensive research on the characteristics of "meta-leaders" who take an enterprise-wide approach to problems, which is what's called for in the NIST effort. Meta-leaders lead their own agencies, and they lead up, speaking "truth to power" to those more senior; they also lead across all agencies involved in a particular event, and in so doing, they develop situational awareness to create a path forward, often in the face of incomplete information.

For NIST to bring all of the parties together and create meaningful change, I believe that its senior leaders must become directly involved in this effort, bringing to it these enterprise-wide leadership skills, and the engagement of the Department of Commerce, and interagency and business leadership. The commercial finance, energy and other private industry players need to understand that the government can provide unique, sensitive information and help create information sharing standards across industries that are consistent, and the government needs to better understand the needs of the private sector. We won't overcome these challenges without executive branch "meta-leadership."

NIST is planning a series of upcoming discussions with private industry this summer to develop a framework for cybersecurity practices to help critical infrastructure manage risk. These would benefit from hands-on attention now and throughout the process from the Institute's senior leaders, other senior leaders across the government sector and senior leaders from the private sector.

On the legislative side, the House has again passed a bill that would foster information sharing, allowing the government and businesses to share data about cyberattacks, potential threats and other information in a manner that avoids antitrust or classification issues. The bill also would grant legal protections to businesses that have been hacked as long as they met standards for protecting their networks. The question will be "who sets the standards"? In my view, industry should set the standards with a simple "agree or disagree" response by the government until agreed-upon standards are established with a method to evolve.

Currently, the Obama administration and many privacy advocates fear the bill provides too few protections against the improper sharing and use of individuals' private information, and they have raised questions about the ability of private companies to shirk their responsibilities for protecting information under the cloak of immunity privileges.

I believe there is middle ground — some liability protection is important, but the protection standards required of industry must be strong and enforceable. Just as meta-leadership is needed around the parameters of the executive order, meta-leaders must step forward around the congressional effort.

The U.S. Chamber of Commerce, which has been a leading opponent of cyber legislation out of fear of additional regulations on industry, must look beyond its traditional point of view. Leaders in Congress — many of whom have seen in classified reports the scope and depth of the cyberthreat — need to bring the business community and privacy advocates to the table in a more urgent, thoughtful way. The Obama administration must do its part through the NIST effort on the executive front and by engaging with Congress on the issue.

In Saudi Arabia last year, 30,000 computers at the Saudi Aramco oil company were attacked and all data deleted in a cyber-attack. Week after week, U.S. banks are hit with denial-of-service attacks. Billions of dollars of patented intellectual capital — plans for building advanced systems — have been stolen by China and other countries. And our banking system, our electric grids, our transportation systems — the lifeblood of our daily lives — every day operate in cyberattackers' cross hairs with largely inadequate protections.

New kinds of leaders need to step forward and bring their meta-skills to this urgent, enterprisewide problem. We need sensitive information shared by the government to the private sector, cyber-penetration information shared by the private sector to government, agreed-upon standards for protection of the nation and liability protection for industry. And we need all this before our nation is trying to recover from an attack or the continued bleeding of our intellectual capital and asking after the fact, "Why didn't we know it was coming?"

Mike McConnell is the vice chairman of Booz Allen Hamilton and previously served as director of national intelligence under Presidents George W. Bush and Barack Obama. He retired from the U.S. Navy in 1996 as a vice admiral.

Just as meta-leadership is needed around the parameters of the executive order, meta-leaders must step forward around the congressional effort.