

PressRelease

For Immediate Release: October 7, 2009



THE OFFICE OF
ENTERPRISE TECHNOLOGY
STATE OF MINNESOTA

CONTACT:

Cathy de Moll, Director of Communications
651-556-8002
Cathy.de.moll@state.mn.us

658 Cedar Street
Saint Paul, MN 55105
www.oet.state.mn.us

**State Officials, National Cyber Security Experts
Converge at Cyber Security Awareness Briefing**
Gathering "Key to solving important problems" CEO of Information Security Forum says

St Paul, MN (Oct. 5, 2009) – National Cyber Security thought leaders led a discussion of current and future tactics for best securing government information during the State of Minnesota's Fourth Annual Cyber Security Executive Briefing on Oct. 5 at Metro State University.

On the heels of Gov. Tim Pawlenty's proclamation of October as Cyber Security Awareness Month in Minnesota, the Fourth Annual Cyber Security Executive Briefing helped kick off a month of activities that will include statewide events, including a day-long event at the University of Minnesota.

"It is vital that we sit down with our state colleagues and leaders to discuss the many issues surrounding cyber security and our collaborative efforts to protect citizen data," said State Chief Information Officer Gopal Khanna, in his opening remarks at the event. "It is also key that we invite nation-leading thinkers to validate our approaches and share with us the best practices that can be incorporated into the Minnesota model. This helps us continually improve the state's security posture."

A group of about 100 Minnesota legislators, agency leaders and information technology department heads met with Professor Howard Schmidt and Dr. Ron Ross to discuss strategies for securing citizens' information on the federal, state, and local levels.

"This was the kind of meeting that could be key to solving important problems that governments face," Schmidt said. "It was a good opportunity for real stakeholders to hear a consistent perspective, interact and communicate with each other. "

Schmidt, former White House cyber security advisor and former Chief Security Officer for Microsoft, is currently the President and CEO of the Information Security Forum Ltd. He spoke with the audience about global risks to information security, focusing on challenges to information security, and risk avoidance.

His message for the audience was forward-thinking. "As we build out the next generation of great information technology," Schmidt said, "we also need to take into account the likelihood that someone will want to do harm, and build security from the beginning, rather than having to go back in and try to fix problems later."

Minnesota's Chief Information Security Officer Chris Buse gave the Information Security State of the State and walked through the State of Minnesota's Enterprise Security Tactical Plan, one of the most comprehensive in the nation. It's a two-year plan with the goals of improved situational awareness, proactive risk management and

PRESS RELEASE

Continued



robust crisis and security incident management. According to Buse, “the State of Minnesota has made incredible progress towards improving its cyber security risk posture since the inception of the Enterprise Security Program, three years ago. However, government leaders must understand that more needs to be done to position our state for success in the digital future. This conference and the Enterprise Security Tactical Plan will help leaders understand that we have a clear vision that we are prepared to execute.”

The plan was applauded by Ron Ross, who leads the Federal Information Security Management Act (FISMA) Implementation Project for the National Institute of Standards and Technology (NIST). A senior computer scientist and information security researcher at NIST, he is the principal architect of the NIST Risk Management Framework.

“The State of Minnesota's information security program is only three years old but shows a breadth and depth consistent with programs that have been in operation for a much greater length of time,” Ross said. “The collaborative initiatives underway across the state set an outstanding example for other organizations to follow. We look forward to continuing our relationship with the State of Minnesota as together, we attempt to find more effective and efficient ways to manage the ever-increasing risks to organizational IT operations and assets at the federal, state, and local levels of government.”

Ross gave an overview of new, unconventional threats to security, and warned that the cyber battle is being fought at every government workstation. He said that an enterprise-wide, risk-based information security program is the best defense against sophisticated cyber threats targeting critical public and private sector information systems.

Ross also noted that “senior leadership involvement in developing and implementing a comprehensive risk management and information security strategy is critical to the mission and business success of organizations today.”

Giving balance to the national perspective, Scott County Chief Information Officer Marilyn McCarter spoke about the challenges of smaller organizations facing security issues. McCarter also emphasized the value of thorough training, the accountability of county leaders for security breaches, and the importance of following regulations and standards that come from the national and state levels.

McCarter opened up a discussion, later taken up by Legislative Auditor Jim Nobles, on enterprise standards, and how much control is too much. The day ended with a discussion among the IT leaders and state officials present on how far standard-setting should go.

Photos of the event and speakers are available upon request and will be posted on Minnesota’s Cyber Security Awareness Month website at oet.state.mn.us.