

2/18/2016

Global Forum to Advance Cyber Resilience organized by the Global Institute for Cybersecurity + Research and hosted at American University

News that a California hospital was forced to pay ransom to regain control of their own computer system is just the latest example of the constant cyber threat faced daily by governments, businesses and individuals worldwide. Coordinating and managing a swift and effective response to cyber attacks is one of the biggest challenges in today's complex and interconnected world. An even more vexing problem is how to build a coordinated fortress for cyber resilience, bringing together the public and private sector entities who need to work together to better fend off and respond to attacks.

This week at American University in Washington, DC, the Kogod School of Business Cybersecurity Governance Center hosted the first meeting of the Global Forum to Advance Cyber Resilience. Organized through the leadership of the Global Institute for Cybersecurity + Research (GICSR - headquartered at NASA's Center for Space Education at the Kennedy Space Center), today's meeting initiated an ongoing forum for public and private sector leaders to collaborate.

"The Kogod Cybersecurity Governance Center (CGC) is focused on assisting corporate executives and board members with the critical action plans they need to have in place to prevent and respond to cyber attacks," said Executive Director William DeLone, one of the nation's leading IT experts. "Our Advisory Committee at the Kogod CGC is made up of public and private sector leaders who know and understand the overwhelming challenges businesses and government organizations of any size face in mitigating and minimizing the enterprise risks associated with cyber attacks. The new Global Forum to Advance Cyber Resilience provides a unique opportunity to bring together top experts to work together finding solutions. We see this forum as a marketplace of ideas and potential partnerships and will be using these resources to further our own work. We are in a race to educate as many leaders as we can in the private sector about how they can carry out their cybersecurity governance responsibilities. It's a race our country can't afford to lose."

Other participants in the Global Forum include leaders from academia and U.S. and global companies working to address cyber challenges, including AxonCyber, UK-based Axelos, AIG, Pepco, Symantec, Lockheed Martin, PSCU (Public Service Credit Union), Fifth Third Bank, Well Florida and Discovery Communications. Public sector participants include leaders from the US Department of Defense, DISA, US Department of Commerce, NIST and US Department of Homeland Security.

Deborah Kobza, the CEO of the Global Institute, said "We have a historic opportunity to leverage increasingly connected globally trusted public and private sector organizations, while breaking down long standing barriers and silos that have slowed joining action".

Thursday's inaugural meeting of the new Forum focused on creating a structure for sustainable collaboration and ongoing development of best practices for mission driven cyber resilient services.

"Collaboration between public and private sector leaders is an imperative in today's challenging and constantly shifting cyber environment," said John Honeycutt, CTO of Discovery Communications and a member of the Kogod Cybersecurity Governance Center Advisory Committee. "The Global Forum to Advance Cyber Resilience is important to advancing a shared dialogue and providing an ongoing forum for idea sharing and planning - for companies and government organizations already well versed in best practices, as well as those just beginning their journey to more advanced cybersecurity preparation and governance."

"Almost every business and government in the world now realizes it's not a matter of whether you will be hit by a cyber attack, but a matter of how often and how hard," said Richard Schroth, co-Executive Director of the Kogod Cybersecurity Governance Center and a frequent adviser to Fortune 100 companies. "Now the challenge is convincing business and government leaders that responsibility for combatting those threats rests with leaders at the top of every organization and not simply your IT department."