Cyberthreats must require governments and businesses to be 'cyberrisk intelligent'

May 2 2013, by Jeff Falk

(Phys.org) —In an age where cybersecurity is of foremost interest for governments and businesses, public and private organizations must deploy risk-intelligence governance to secure their digital communications and resources from eavesdropping, theft or attack, according to a new paper from Rice University's Baker Institute for Public Policy.

The paper, "Risk-Intelligent Governance in the Age of Cyberthreats," was authored by Christopher Bronk, a fellow in information technology policy at the Baker Institute. Against the backdrop of technology experts and policymakers' elusive battle to find a remedy for the myriad cyberthreats and vulnerabilities, the paper proposes the concept of "cyberrisk intelligence," a general framework for understanding the varied phenomena that impact an organization's capacity to secure it cyberinfrastructure.

"In the geopolitical context of cyberincidents and conflict, perhaps the most important questions revolve around 'Why?'" Bronk said. "In cyberdefense activities, the typical mindset has been one in which risks are identified and mitigated based on known vulnerabilities and threats. Where organizations often fall short is in pulling together all the different inputs in understanding their vulnerabilities."

Bronk proposes a holistic identification and mitigation model that considers cybersecurity in the broader scope of an organization. "Considering what bad outcomes might occur in the cyberarena needs inputs not just from the IT space but the broader space of operation," he said. "We suggest three general flows of information in determining an organizational frame for cyberrisk intelligence: one that encompasses the awareness of the IT enterprise and its apparent health; a second that brings internal business activities into view; and a third that encompasses broader geopolitical and economic forces. These three areas can be combined into a common operating picture for cyberrisk awareness."

For organizations to become cyberrisk intelligent, Bronk said, they must move beyond seeing cybersecurity as province of organizational IT. They must also understand and evaluate how they are exposed to competition or harm and join industrywide efforts that identify key security concerns and meet them with a collaborative response.

Bronk draws comparisons to more visible security threats in making the case for the importance of cyberrisk intelligence. "Since the Sept. 11, 2001, attacks, two air travelers have tried to blow up airplanes and been thwarted by fellow passengers and flight crew because there is a clear understanding of what is at stake," he said. "People aboard airliners now understand that successful hijacking may mean death. Threats in cyberspace are not so clear and so great, in terms of life and limb. The case is clear that the world's organizations depend on IT to function. The question for preserving cyberspace is how those organizations pool their attentions and resources to preserve a vibrant and functioning cyberspace that may be used to enhance human endeavor. Without adequately studying new and even unorthodox approaches to security, we may eventually lament the loss of the cyberconnected world we once enjoyed."

More information: "Risk-Intelligent Governance in the Age of Cyberthreats," paper: www.bakerinstitute.org/publica … overnance-042613.pdf.

Provided by Rice University

Citation: Cyberthreats must require governments and businesses to be 'cyberrisk intelligent' (2013, May 2) retrieved 30 June 2024 from https://phys.org/news/2013-05-cyberthreats-require-businesses-cyberrisk-intelligent.html