wiley

NEWSLETTER

FCC Chairman Addresses Cybersecurity - Momentum Builds

March 2012

In a speech given on February 22, 2012, at the Bipartisan Policy Center, Federal Communications Commission (FCC) Chairman Julius Genachowski announced the cybersecurity recommendations of the Communications Security Reliability and Interoperability Council (CSRIC). CSRIC is a multi-stakeholder working group whose mission is to provide recommendations to the FCC to ensure, among other things, optimal security and reliability of communications systems, including telecommunications, media and public safety. In March 2011, Chairman Genachowski asked CSRIC to recommend how to best address private sector Internet security vulnerability. He announced those recommendations in his remarks.

CSRIC recommends that Internet Service Providers (ISPs) take three steps to increase cybersecurity: (1) develop and adopt an industry-wide code of conduct to combat the botnet threat and protect the public; (2) adopt secure routing standards to stop internet route hijacking; and (3) implement the Internet Engineering Task Force's Domain Name System Security Extensions (DNSSEC) to prevent domain name fraud.

These recommendations focus on what the private sector can do to advance the nation's preparedness for cyber attacks. It will further discussions in Congress and in the Administration about how best to respond to increasing cybersecurity threats. Momentum is building for some solution, whether targeted or comprehensive, and a way to create incentives for free information sharing across and among the private and public sectors.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

First, CSRIC recommends ISPs help consumers protect their private computers from botnets. A botnet is a robot network created by cyber criminals to distribute malware. A PC or server can become infected with malware when a user unwittingly opens an bad email, link or file, which then installs malicious software on the machine so that it can be controlled remotely. These "zombie PCs" are then used to launch cyber attacks. To prevent botnet attacks, CSRIC recommends that ISPs engage in consumer education. ISPs can play a significant role in preventing these types of attacks by increasing consumer awareness of signs that computers are being used as bots, detecting infections, notifying users about infections and offering remediation support in a way that does not compromise consumers' privacy. Chairman Genachowski called on ISPs to develop and adopt an industry-wide code of conduct to combat the botnet threat and protect the public.

Second, CSRIC recommends that ISPs do more to prevent Internet route hijacking. Connectivity between networks serves as the basis of the Internet's architecture. The method by which individual networks are connected, known as border-gateway protocol, does not include mechanisms to protect against cyber attacks. Cyber criminals can misdirect Internet traffic meant for one destination onto a bad network, and then that network can steal or change the data as it passes through the bad network. CSRIC recommends that network operators adopt secure routing standards to stop Internet route hijacking. Chairman Genachowski urged ISPs to support the development of these secure routing standards. He suggested that they could minimize the cost of implementing these standards through advanced planning and implementation during the course of regularly scheduled maintenance.

Third, CSRIC recommends that ISPs do more to prevent domain name fraud. The domain name system (DNS) is the digital phonebook for the web. DNS has vulnerabilities that can allow identifying information to be changed, letting cyber criminals direct unknowing users to fraudulent websites. Users often are unaware they are not dealing with a legitimate site and provide operators with financial and personal information. The Internet Engineering Task Force has developed a series of security extensions to DNS called DNSSEC, which can prevent domain name fraud. CSRIC believes that DNSSEC can be implemented in a way that protects privacy and the openness of the Internet. It recommends that ISPs implement DNSSEC because doing so will provide tangible benefit to the businesses and users who rely on DNS.

Momentum is building in Congress and in the Administration for action on cybersecurity. A flurry of proposed legislation has hit Congress in the last few weeks and hearings are being held. There is not yet consensus on what legislation will look like-comprehensive or targeted-and there are many moving parts and industries that could be affected.