Computer & Communications Industry Association
Tech Advocacy Since 1972

ABSTRACT

CYBERSECURITY **APRIL 2014**

Cybersecurity has increasingly become an area of concern for policymakers. Government agencies and American businesses, including critical infrastructure, are under attack on a daily basis.

Numerous pieces of legislation on cybersecurity have been proposed, ranging from piecemeal approaches to comprehensive legislation packages. Issues addressed include facilitating cyber threat information sharing; requiring baseline cybersecurity practices for critical infrastructure; creating a federal standard for data breach notification; investing in cybersecurity research and development, education, and workforce training; and updating cyber crime statutes.

Cybersecurity policymaking should seek solutions that leverage the expertise of both the private sector and Federal Government and should be results-oriented and technology-neutral.

Background: Over the past several years, cybersecurity has become an increasingly pressing issue for those at the top levels of government and in the private sector. As President Obama has noted, cyber attacks have become "one of the most serious economic and national security threats our nation faces," and in 2011, then CIA Director Leon Panetta warned, "the potential for the next Pearl Harbor could very well be a cybersecurity attack."

The cyber threats America faces range from basic hacking and identity theft; to theft of national security secrets and cyber corporate espionage; to the potential disruption and catastrophic failure of the nation's electric grid, utility plants, and telecommunications and financial networks. The magnitude of the cybersecurity threats America faces is great and it is increasing.

Industry experts estimate that approximately 60,000 new, malicious computer programs and 315,000 new, malicious files are discovered every day. From 2006 to 2012, the number of cybersecurity incidents reported by federal agencies increased from 5,503 to 48,562 – a rise of 782% – and a 2013 McAfee study estimated that global cybercrime losses may total $400 billion. Cyber attacks are a threat to America's national and economic security, as well as to individual privacy, and to the bottom lines, business strategies, and intellectual property of both large and small companies.

The Obama Administration and recent Congresses have raised the profile of cybersecurity. In May 2009, the White House produced a *Cyberspace Policy Review*, and in 2011 it released the President's comprehensive cybersecurity legislative proposal. In February 2014, the Administration launched a Cybersecurity Framework geared toward the critical infrastructure community, following up on an issue that President Obama raised in the 2013 State of the Union

address. The current Congress has put forward numerous proposals on cybersecurity. Of particular note are the recommendations of the House GOP Cybersecurity Task Force, which opts for a piecemeal approach to tackling cybersecurity issues, as well as the comprehensive Cybersecurity Act of 2012 sponsored by Senators Lieberman, Collins, Feinstein and Rockefeller.

In 2012 there were significant efforts by both the House and Senate and by both parties to pass cybersecurity legislation. In April, the House of Representatives passed the Cyber Intelligence Sharing and Protection Act (CISPA), which would enable and promote greater cyber threat information sharing between the private sector and the Federal Government. In the Spring and Summer, the Senate Democrats and Republicans worked to reach a compromise on amendments to the Cybersecurity Act of 2012; however, divisions over whether and how privately-owned critical infrastructure should be required to comply with cybersecurity best practices ultimately derailed the bill's passage.

An amended version of CISPA passed the House in April 2013. The Cybersecurity Enhancement Act of 2013 also passed the House in April 2013. In February 2014 the House Homeland Security Committee voted unanimously to approve the National Cybersecurity and Critical Infrastructure Protection Act, a bill intended to secure the Federal Government and critical infrastructure elements from cyber attacks.

Policy Considerations: Cybersecurity encompasses a wide range of policy areas ranging from the role of the Federal Government in protecting and setting baseline levels of cybersecurity for critical infrastructure; to allowing and encouraging information sharing on cyber threats between and amongst the Federal Government and private entities; to promoting cybersecurity awareness and preparedness through awareness campaigns, education and cybersecurity workforce development.

Information Sharing

Companies already share cyber threat information with both the government and other entities; however, as is common practice, information sharing is too slow and encumbered by over-classification. Information sharing about cyber threats needs to be faster and easier. Sharing should be done in real-time and machine-to-machine, enabling automated processes to address threats as they're discovered. Private entities need assurance that they are not violating laws and regulations by sharing cyber threat information, and individuals need confidence that cyber threat information sharing does not infringe on expectations of privacy. Finally, processes should be established to expedite security clearances so critical infrastructure employees can receive classified government cyber threat information.

Data Breach Notification

Forty-nine states, the District of Columbia, and three territories have data breach notification requirements. The requirements mandate, to varying degrees, that companies inform individuals when they have a data breach involving personally identifiable information. Compliance with the current patchwork of state laws and requirements is both burdensome and expensive for companies – many of which are under attack every day. A federal data breach notification standard that pre-empts the maze of state requirements would be both more effective and less onerous, and would provide companies with clear rules and individuals with plain expectations of privacy for their personal information.

Critical Infrastructure

The vast majority of America's critical infrastructure is owned and operated by the private sector, and there is widespread disagreement on what should be designated as critical infrastructure for cybersecurity purposes. Governments, companies, hospitals, and individuals rely on private companies to provide necessary services, such as electricity, water, and communications. If providers of these services do not protect themselves from cyber threats, economic activity and the delivery of social services will be compromised.

Cybersecurity R&D, Education, Awareness, and Training
The Administration, House, and Senate all agree on the need to invest in and promote increased cybersecurity research and development, education, and workforce development. New technologies and a workforce with the skills to detect and repel sophisticated cyber attacks are the necessary tools to address cyber threats today and in the future. Public awareness campaigns on cyber threats, such as Stop.Think.Connect, can have a profound impact in stopping cyber attacks. It is estimated that 85% of cyber attacks can be stopped with good "cyber hygiene."

Cyber Crime Laws
Criminal laws on cyber crime need to be updated to address the nature and magnitude of today's cyber attacks. However, lawmakers should be cautious to focus on real criminal activity and not criminalize harmless actions such as user violations of terms of service for websites and Internet services.

International Cooperation
Many of the most sophisticated cyber attacks originate outside the United States. Additionally, the United States Government, American companies, and U.S. citizens are not the lone targets of cyber attacks. Policymakers must engage foreign governments, multilateral organizations, and multinational companies to work together to address cybersecurity.

CCIA's Position: CCIA supports efforts to facilitate and streamline information sharing on cyber threats between the private sector and the Federal Government, and amongst private firms. Cyber crime laws should be updated to address today's threats, but must not inadvertently criminalize trivial user behavior. A federal data breach standard should be implemented to reduce compliance costs for businesses and make privacy protections more transparent for consumers. Increased research and development, education, and workforce training will create new tools to address cyber threats and a workforce trained to use them, and will also lead to new cybersecurity products and skilled professionals for the private sector. Finally, policymakers should work with the international community to address cyber threats. New laws relating to cybersecurity should include a sunset period so policymakers can evaluate what policies are effective and which are not. Any standards should be results-, rather than process-oriented, and technology-neutral.