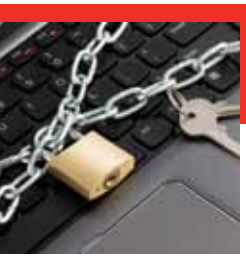
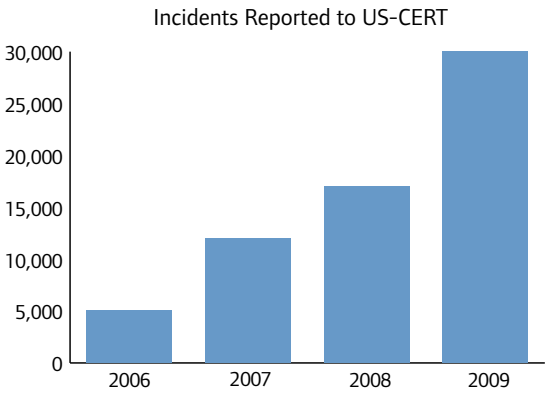


PROTECTING U.S. TECHNOLOGY ASSETS WITH EFFECTIVE CYBERSECURITY

Fast Facts

- The World Economic Forum calls threats to cybersecurity one of the top five global risks to watch, citing "the prevalence of cyber theft and the little understood area of all-out cyber warfare."[1]
- According to a broad investigation of data breaches in 2011, 92 percent of all breaches were caused by "external agents," and organized crime was responsible for 58 percent of those breaches by external agents.[2]
- The Internet Crime Complaint Center, a partnership of the Federal Bureau of Investigation and the National White Collar Crime Center, reports that complaints of online crimes increased by more than 22 percent from 2008 to 2009. Moreover, the costs of these online crimes more than doubled, increasing from $265 million in 2008 to nearly $560 million in 2009.[3]

Cybercrime incidents continue to increase.



Source: GAO analysis of US-CERT data

With the spread of information and telecommunications technologies across the economy, the daily operations and long-term value of most economic enterprises in America now depend on the capabilities and security of their information systems. Moreover, the capacities and security of these systems have become critical elements of U.S. technological and economic leadership. As strategic economic assets, these systems must be protected. The government has a prominent role to play in this security realm. Unfortunately, this role is currently fragmented across many departments and agencies, as well as dozens of congressional committees and subcommittees, all claiming jurisdiction — and often lead status as well.

"Safeguarding America's strategic information systems, *most of which are privately owned and operated, is* **'mission critical' for U.S. business and government."**

— Ajay Banga, President and CEO, MasterCard Worldwide, and Chair, Business Roundtable Information and Technology Committee

In addition, neither the government nor the private sector currently has the necessary information and analytic tools to assess and defeat the most serious threats to the cybersecurity of American companies. Meeting this challenge will require robust, collaborative public-private partnerships, which can respond to a rapidly changing threat environment for privately owned and operated information assets.

Solutions

BRT CEOs are committed to strong private-sector cybersecurity protections, including direct involvement and oversight by CEOs and their boards. They also call on government to do its part, including the following:

- **Coordinate and integrate the far-flung resources of the U.S. government to protect strategic information** in the United States, including the Departments of Defense, Homeland Security, Commerce, Justice and State; appropriate intelligence offices and agencies; and U.S. diplomatic, economic and security assets.
- **Avoid a top-down, prescriptive, check-the-box approach to cybersecurity** that cannot take effective account of the private ownership and operations of information assets and respond decisively to the rapidly changing threat environment.
- **Support the efforts of U.S. businesses to securely and effectively use the tools they need to combat global cybersecurity threats,** including:
    - Formal information-sharing mechanisms with appropriate legal protections;
    - Technical cooperation;
    - Strategic threat assessments; and
    - Strict criminal penalties and sentencing for cyber crimes.

---

1 World Economic Forum. (2011). *Global risks 2011.* (6th ed.). New York, NY. Retrieved from http://riskreport.weforum.org/

2 U.S. Secret Service. (2011). *2011 data breach investigations report.* Washington, DC. Retrieved from www.secretservice.gov/Verizon_Data_Breach_2011.pdf

3 Internet Crime Complaint Center. (2009). *2009 Internet crime report.* Washington, DC. Retrieved from www.ic3.gov/media/annualreport/2009_IC3Report.pdf