DPCC
DEMOCRATIC POLICY & COMMUNICATIONS CENTER | 202.224.2939 | DPCC.SENATE.GOV
CHAIRMAN SENATOR CHARLES SCHUMER | VICE-CHAIRWOMAN SENATOR DEBBIE STABENOW

The Cybersecurity Act: Recent Notable Cyberattacks

Oak Ridge National Laboratory was the target of cyberattacks. In 2007, a coordinated cyberattack "allowed personal information about thousands of laboratory visitors to be stolen," including "Social Security numbers and birth dates of every laboratory visitor from 1990 to 2004." The Lab was hacked again in 2011, and '"a few megabytes' of data were extracted before the Lab was able to cut its internet connection." [The New York Times, 12/7/07; CSIS]

Computer spies hacked into the Pentagon's F-35 Joint Strike Fighter project, stealing terabytes of the aircraft's design and electronic related schematics. It is believed that attack originated in China. "Six current and former officials familiar with the matter confirmed that the fighter program had been repeatedly broken into…. the scope of the damage to the U.S. defense program, either in financial or security terms [is still unknown]…. Computer systems involved with the program appear to have been infiltrated at least as far back as 2007…. The intruders appear to have been interested in data about the design of the plane, its performance statistics and its electronic systems, former officials said." [The Wall Street Journal, 4/21/09]

The NASDAQ stock exchange was hacked in 2011. Hackers broke into a NASDAQ service for corporate officers to share confidential documents, and planted malware. At the time of the attack, NASDAQ accounted for 19 percent of U.S. stock trading. An unrelated "flash crash" of the Dow Jones Industrial Average demonstrated the potential damage a successful cyberattack could inflict, resulting in a rapid loss of nearly 1,000 points and $1 trillion in market value. [The Atlantic, 2/7/11; Wired, 3/30/11; CNN Money, 10/1/10]

Leading computer security company RSA was hacked and proprietary information was compromised. In March 2011, it was revealed that RSA Security, one of the world's top computer security companies, had been hacked. This attack put at risk RSA's SecureID products, which are used by more than 40 million businesses to protect their own networks. Using a "phishing" email designed to entice an email recipient to open an infected email, the hackers were able to download malware onto the user's computer and ultimately gain access to the machine and steal several of the employee's passwords, enabling the hacker to access other users account information and sensitive data within RSA's system. Eventually, the hacker was able to steal RSA files, and later infiltrate defense contractor Lockheed Martin through RSA's SecureID tokens. [CSIS, 8/3/11; The New York Times, 6/7/11; The New York Times, 6/6/11]

NASA's computer systems were infiltrated, compromised, and remotely controlled. According to a report issued by NASA's inspector general, "Hackers with IP addresses originating in China took control of computers in NASA's Jet Propulsion Laboratory" in November 2011. "The attack let intruders gaining access to 150 NASA employee credentials….

- In fiscal year 2011, NASA reported it was subject to 47 hacking incidents – 13 of which successfully compromised the agencies computers. In total, 5,408 computer security incidents 'that resulted in that installation of malicious software on or unauthorized access to its systems' were reported by NASA in 2010 and 2011.... These intrusions 'have affected thousands of NASA computers, causes significant disruption to mission operations, and resulted in the theft of export-controlled and otherwise sensitive data, with an estimated cost to NASA of more than $7 million.'" [CNN Security Clearance, 3/2/12]

Hackers successfully penetrated and stole from defense contractors and internet security companies. "For a decade, hackers accessed the corporate computer network of Nortel, whose digital switches power much of the Web; defense contractor Lockheed Martin suffered a break-in when the SecureID system that provides encrypted authentication was breached; the U.S. Chamber of Commerce had all its systems accessed…; five large oil companies lost information about their operations, including bidding strategies; and hackers accessed details of the Pentagon's costliest weapons program – the $300 billion Joint Strike Fighter project – including aircraft design and electronics." [The Wall Street Journal, 2/27/12]

Malicious cyber actors carried out significant intellectual property thefts against US companies, including:

- In 2009, "an employee of Valspar Corporation [one of the world's biggest coatings manufacturers] unlawfully downloaded proprietary paint formulas valued at $20 million, which he intended to take to a new job in China.... This theft represented about one-eighth of Valspar's reported profits in 2009, the year the employee was arrested." [NCIX report to Congress, 10/11]

- A cyber incident originating from a Chinese IP address targeted U.S. companies in an effort "to obtain information on sensitive competitive proprietary operations and on financing of oil and gas field bids and operations." [NCIX report to Congress, 10/11]

- Google's networks were penetrated by sophisticated attacks in 2010 perpetrated by China. Google uncovered "a 'phishing' campaign aimed at stealing passwords of hundreds of Google email account holders, including senior U.S. government officials, Chinese activists and journalists." [CSIS; *Reuters*, 6/3/11]

For a comprehensive list of significant cyber incidents since 2006, please review the Center for Strategic and International Studies' (CSIS) report, which is updated regularly.