111TH CONGRESS
1ST SESSION

H. CON. RES. 193

Expressing the sense of Congress regarding the need to pass meaningful legislation to protect commercial and Government data from data breaches.

IN THE HOUSE OF REPRESENTATIVES

OCTOBER 1, 2009

Mr. BURGESS (for himself and Mr. GONZALEZ) submitted the following concurrent resolution; which was referred to the Committee on Science and Technology, and in addition to the Committee on Oversight and Government Reform, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

CONCURRENT RESOLUTION

Expressing the sense of Congress regarding the need to pass meaningful legislation to protect commercial and Government data from data breaches.

Whereas over 261 million records have been subject to a data breach in the United States since January 2005;

Whereas almost 10 million adults in the United States were victims of identity fraud in 2008;

Whereas 64 percent of breaches can be attributed to hackers;

Whereas data breaches occur in a wide rage of institutions, including Government, military, education, health care companies, banking, and credit and financial services;

Whereas in 2007, the number of data security breaches at colleges and universities increased over 67 percent from 2006, and the number of educational institutions affected increased over 72 percent;

Whereas the Department of the Interior, the Nuclear Regulatory Commission, the Department of Treasury, the Department of Veterans Affairs, and the Department of Agriculture all scored an ''F'' on the May 2008 Federal Security Report Card;

Whereas the 2006 Department of Veterans Affairs data breach put 28.6 million veterans' names, addresses, and social security numbers at risk;

Whereas in 2008, medical data of over 3,000 patients at the National Institutes of Health was stolen from an unencrypted Government laptop;

Whereas in 2009, CheckFree Corp. and some of the banks that use its electronic bill payment service said that criminals took control of several of the company's Internet domains and redirected customer traffic to a malicious Web site hosted in the Ukraine;

Whereas the company believes that about 160,000 consumers were exposed to the Ukrainian attack site, however, because the company lost control of its Web domains, it doesn't know exactly who was hit so it must warn a much larger number of customer;

Whereas this breach was reported back on December 3, 2008;

Whereas since 2001, the Department of Commerce previously reported to the House Committee on Government Reform that a total of 1,137 department laptops have been stolen, lost, or reported missing;

Whereas the Government Accountability Office found in 2008 that significant control weaknesses continue to threaten the confidentiality, integrity, and availability of the Securities and Exchange Commission's financial and sensitive information and information systems, and the S.E.C. has not consistently implemented effective controls to prevent, limit, or detect unauthorized access to computing resources;

Whereas the President's Budget proposal for fiscal year 2009 calls for information technology security of $7,200,000,000, an increase of $600,000,000 over the fiscal year 2008 budget that has yet to be enacted;

Whereas a 2009 report found that more electronic records were breached in 2008 than the previous 4 years combined and the financial services sector accounted for 93 percent of all compromised records and 90 percent of these records involved groups engaged in organized crime;

Whereas in 2006, hackers broke into the Congressional Budget Office's (CBO) mailing list and sent a phishing e-mail that appeared to come from the CBO;

Whereas a 2009 report found that data breaches are caused by a variety of sources, including 74 percent from external sources, 20 percent caused by insiders, 32 percent by business partners, and 39 percent where multiple parties are involved;

Whereas a 2009 report found that data breaches occur in a variety of ways, including 67 percent attributed to significant error, 64 percent resulted from hacking and intrusions, 38 percent incorporated malicious code, 22 percent

exploited a vulnerability, and 9 percent were due to physical attacks;

Whereas cyber crime is a growing international business that presents a fundamental threat to the Internet;

Whereas 44 States, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information;

Whereas the total cost of the data security crisis to business and consumers is approaching $50,000,000 annually, with the average breach costing a consumer $1,200 and a business $5,000,000;

Whereas a 2009 report indicated that the average cost of a data breach has risen to $202 from last year's $197 per customer record breached;

Whereas 62 percent of consumers have been notified that their confidential data was lost or stolen and 84 percent of these consumers expressed increased concern or anxiety due to the data lost;

Whereas 87 percent of breaches are considered avoidable if reasonable controls had been in place; and

Whereas solutions to these threats exist in the marketplace for relatively low cost: Now, therefore, be it

Resolved by the House of Representatives (the Senate concurring), That it is the sense of Congress that Congress should—

(1) enact into law a meaningful national standard to protect commercial and Government data, which includes a robust definition of encryption tied

to National Institute of Standards and requires leadership at the top levels of an organization to take an active role in ensuring that their systems are secure;

(2) adopt legislation that requires that sensitive data be protected through meaningful encryption technology and require Federal Government subcontractors that have access to sensitive and personally identifiable information to comply with the same standards as Federal agencies and departments; and

(3) encourage leaders of Government agencies and private enterprises to actively manage and rigorously protect the data collected and stored within their institution by making data security a priority within the institution.

○