IT Management: Security

Wednesday 19 November 2003

IT leaders question US security mandates

US companies need to work together to improve their cybersecurity before a major cyberattack forces hasty legislation, the chairman of a cybersecurity-focused subcommittee has told IT industry leaders.

Earlier this month, representative Adam Putnam, chairman of the House Committee on Government Reform's Subcommittee on Technology, Information Policy Intergovernmental Relations and the Census, decided not to introduce a bill that would require public companies to report their cybersecurity initiatives to the US Securities and Exchange Commission.

"A hell of a lot of negative feedback" over the proposed bill forced Putnam to reconsider the legislation. IT security experts objected to the proposal during a discussion on government's role in cybersecurity sponsored by the Center for Strategic and International Studies in Washington DC.

Putnam warned IT company leaders, however, that any private sector efforts to build consensus on cybersecurity best practices may be washed aside by Congress if there is a major cyberattack on US infrastructure.

Any one of 1,000 cyberattack scenarios - from an attack that takes out part of the power grid to an attack that causes the dams to open on a major river - could prompt Congress to act, Putnam said.

"The bottom-line foundation that's driving our action on this issue is that Congress makes very poor decisions in the wake of a disaster. If the industry doesn't get serious about being proactive and putting in place a cybersecurity plan that works now ... any one of those [scenarios] would lead to legislation from this body that would not be what the industry would sit down and write if they had the time."

Putnam listed examples of legislation passed quickly that later caused problems for private industry, including the Sarbanes-Oxley financial reporting law passed in 2002 after accounting scandals involving Enron and other companies. He urged tech leaders to support a cybersecurity working group of IT security experts he set up after deciding not to introduce his legislation.

Some opponents of the proposed legislation questioned why it applied only to public companies, and others questioned if such legislation is needed. "Some people don't think that the time has come," Putnam said. "My response to that is the time will at a time of someone else's choosing in a disastrous situation."

But IT industry representatives said they opposed most government cybersecurity mandates on private industry, including the Putnam proposal, during the discussion on the government's role in cybersecurity.

Private industry should soon come up with a set of best practices, said Greg Garcia, vice president of information security policy and programs at the Information Technology Association of America.

"I want to just step back and say, 'We're getting there'," Garcia said. "(Cybersecurity) takes time, it is hard, and it is complicated. Legislation is not the answer now ... but we're glad for Putnam

Print this page >>
Send to a friend >>
Subscribe to E-mail >>

Related Articles

- Software glitch hits Akamai
- Birthday celebrations marred by questions about source code leak
- Management tools could do better
- Cisco's security management on networks too 'high maintenance'
- Efficiency must be balanced with security
- Hackers on the move
- Nokia boosts security with IPSO
- Microsoft eyes merger of two e-mail specs
- US spam law makes little impact so far
- Linux suppliers patch CVS flaw
- @stake product helps clean code
- Cisco 'unnaturally quiet' on code theft
- Spam clogs German government's e-mail system
- Thought for the day: Thumbs down for ID cards
- Rock guitar maker reduces virus threat with mixed infrastructure
- Reports of phishing scams skyrocket in April
- Symantec to acquire Brightmail in $370m deal

Top Stories

- Head of e-government unveiled
- Thought for the day: Cards put finance at risk
- Monitoring software gives House of Fraser advance notice of server and network blips

stimulating our thinking."

Garcia and other panelists urged Congress to let the marketplace and not government legislation shape cybersecurity decisions at private companies. The technology industry is heading toward an approach of policing itself with companies receiving a seal of approval for using best cybersecurity practices, Garcia said.

"The technology companies are taking action," said Art Coviello, president and chief executive officer of RSA Security. "Quite frankly, it's a matter of our survival."

Some panelists questioned if the US government has any role in ensuring cybersecurity at private companies, beyond using its "bully pulpit" to raise awareness of the issue. But Coviello suggested the US government should take action to protect individual privacy and critical infrastructure.

While Putnam suggested his legislation would have been the "least intrusive" option for a cybersecurity law, others on the panel raised several objections. The legislation would have required third-party auditors to review a public company's cybersecurity report to the SEC, but Cary Klafter, vice president for legal and government affairs at **Intel**, questioned whether such cybersecurity auditors now exist.

The SEC would also have to create a cybersecurity division to review the reports that would have been required in Putnam's legislation, Klafter added. "The SEC has zero cybersecurity expertise. It has no staff to deal with cybersecurity issues."

The government may have more influence on cybersecurity by adopting security-focused procurement requirements than by passing the Putnam legislation, said representative Zoe Lofgren. "Disclosing our vulnerabilities to the Securities and Exchange Commission so that they might be published might not make us safer," she said.

Grant Gross *writes for IDG News Service*

- **Feedback sought for web services security draft**
- **More information released on Cisco code theft**
- **Learn to identify the new generation of security threats and protect your network**

Print this page >>

Send to a friend >>

Subscribe to E-mail >>

