Helping businesses defend against cyber threats

December 6 2011, By Matthew Hay Brown

Analysts with the National Security Agency see the threats coming at corporate America: viruses, worms and other malware targeting the computer networks that serve the nation's banks, utilities and businesses.

But the 64-year-old law that established the modern U.S. intelligence community prevents them from sharing the classified details with the private businesses in the cross hairs.

"I'm really concerned that we will have some type of serious attack within the year," said Rep. C.A. Dutch Ruppersberger of Maryland, who receives security briefings as the top-ranking Democrat on the House Intelligence Committee. "Air traffic control systems when the planes are flying. Grid systems for energy. Banks really concern me."

Ruppersberger and Mike Rogers, the Michigan Republican who chairs the committee, are co-sponsoring legislation that they say would begin to break down communication barriers between the nation's intelligence agencies and U.S. companies.

The bill would promote unprecedented cooperation between the government and the private sector by allowing the NSA and other federal agencies to pass classified information to vetted companies so they can defend against disruptions, destruction or the theft of trade secrets, business plans and private information about customers and employees.

But while many agree on the need for greater coordination against cyber

threats, some express concern about the potential impact on civil liberties - from government agencies gaining access to personal details about private citizens to the possibility of an information clampdown as threat data is labeled secret.

Estimates of the impact of cyberattacks on the U.S. economy begin in the billions of dollars annually, and analysts say the costs are growing. Web-based attacks nearly doubled from 2009 to 2010, according to Symantec Corp. The cybersecurity giant also reported encountering more than 286 million unique variants of malware last year.

The overall threat level is difficult to measure. Private businesses don't always know when they have been hacked; when they do, they often prefer to keep the information to themselves.

But Peter Kilpe, creative director of the Baltimore security firm CyberPoint, calls the threat "huge."

"It's probably one of the most important issues facing businesses right now," he said. "We're more connected than we ever have been in any other time in our history, and we're more dependent on computers. That's everything from doing business on your PC to computers being part of life-sustaining infrastructure - power, water."

Rogers speaks of an "economic cyberwar" being waged against U.S. businesses by "economic predators, including nation-states." U.S. officials have identified Russia and China as the most aggressive countries.

But Ruppersberger says terrorists concern him the most.

"I don't think China's going to try to attack our energy systems or anything like that, because we owe them too much money," he said. "But

al-Qaida and other extreme groups could hire some brilliant hackers - and they're all over the world - and pay them millions of dollars to make an attack."

The Cyber Intelligence Sharing and Protection Act of 2011, introduced Wednesday by Rogers and co-sponsored by Ruppersberger, is one of several proposals to address cybersecurity in the private sector.

But with strong bipartisan support - the measure cleared the Intelligence Committee on Thursday by a 17-1 vote - more than a year of consultation with the White House and the backing of several key Internet service providers and trade organizations, it might have the best chance of becoming law.

Critics say they recognize the need for better cybersecurity coordination between the government and the private sector, but they express concerns about the details.

Richard Forno, director of the graduate program in cybersecurity at the University of Maryland, Baltimore County, says a requirement in the bill that would require employees of private businesses to get security clearances to receive threat details would likely lead to more details being classified, which could impede the flow of information.

Forno also questions language that would appear to relieve companies of legal liability for vulnerabilities they have shared with the government. "That sounds like a giant get-out-of-jail-free card," he said.

Michelle Richardson, legislative counsel for the American Civil Liberties Union in Washington, says the bill could allow companies to share personal information about clients, customers and employees with the government.

"When they report cyber incidents or want to share cyber information with the government, it should really be limited to technical data and only the information that's necessary to deal with the threat," she said. "We're concerned also that once it's in government hands, there's no use restriction. ... It can be used in criminal cases, immigration enforcement or whatever."

Such objections recall criticism of the so-called warrantless wiretaps authorized by the Bush administration in an attempt to intercept communications by al-Qaida and other adversaries as part of the war on terror. The ACLU and the Electronic Frontier Foundation have sued the NSA and AT&T over the electronic eavesdropping program.

Ruppersberger says he shares concerns about civil liberties. At the urging of Ruppersberger and Rogers, the Intelligence Committee amended the bill to bar the government from searching data supplied by private companies for any purpose other than cybersecurity or the protection of national security.

The bill would not require private businesses to report cyber threat information to the government.

Ruppersberger says the legislation is aimed at improving communication about malware - "a bunch of ones and zeros that make up a computer code that will do bad things to your computer" - not personal information about individuals associated with a business. He describes the bill as a work in progress on an issue that demands immediate attention.

"We're getting attacked as we speak," he said. "It's getting worse and worse every day. I've made the analogy, if we knew that a country was sending a plane over to bomb us, we'd take it out."

He says the legislation should improve communication between the government and the Internet service providers that serve businesses and consumers - "the AT&Ts, the Verizons, the Qwests."

"NSA has this information, and they know that major companies are being attacked, but they're not allowed to pass classified information," he said. "Now you're saying, 'OK, providers, we are giving you the secret sauce. We're giving you the code so you can protect yourself.' "

The National Security Agency referred questions about current communication with the private sector to the Office of the Director of National Intelligence. That office did not respond to requests for comment.

Ruppersberger says the legislation builds on a pilot program that has allowed sharing between the NSA and selected defense contractors - and helped thwart hundreds of cyberattacks.

AT&T, IBM, Microsoft Corp. and Verizon have expressed support for the legislation, as have the U.S. Chamber of Commerce and several financial and communications industry associations.

"There is a critical role for government in securing cyberspace," said Walter B. McCormick Jr., president and CEO of the industry group USTelecom. The bill, he said, "sets forth a path that would enable government and network providers to better share information in real time."

Cyberattacks are a global challenge. In a heavily publicized recent case, a South Korean bank lost ATM and online banking service for several days in an attack this year and key financial information was destroyed. South Korean prosecutors blame North Korea.

Closer to home, a Hungarian pleaded guilty in federal court last week to transmitting malicious code to Marriott International Corp. and threatening to reveal confidential information about the company if he were not offered a job maintaining the network.

According to a plea agreement, Attila Nemeth, 26, sent the Bethesda, Md.-based hotel chain an email last year containing attachments that included confidential information that had been stored on company computers.

Nemeth acknowledged sending an infected email attachment to Marriott employees in order to install malicious software that gave him a back door into the network, according to a statement by the U.S. attorney for Maryland.

Ursula Powidzki, director of business development at the Maryland Department of Business and Economic Development, says large companies - financial institutions, insurance companies, retailers and supermarkets - know they are vulnerable.

"They have a lot of consumer data that is a very obvious target for criminal hackers," she said. "It's the small and mid-sized companies that don't fully realize how exposed they may be."

She speaks of a "very, very sophisticated" small-business owner in Maryland whose consulting website was hacked.

"They spent three days having to bring in outside people to help get the site back up," Powidzki said. "She had no idea why someone would do this or how they did it. They had to get up the learning curve very, very quickly."

Derek Gabbard, CEO of Lookingglass Cybersecurity in Baltimore,

predicted that private companies would welcome more information from the government.

"Folks that are running threat intelligence teams in the private sector are dying for more data," he said. "They understand that the adversaries are sharing information."

But he says businesses might be skeptical about government intentions and be hesitant to divulge information.

Gabbard said intelligence officials "need to share and not expect anything back for quite a while, until the private sector is comfortable that the government really is a partner and not trying to use them as a sensor grid."

"One of the old mindsets that hopefully is changing is that government just wants to collect information without producing anything back," he said. "It's kind of a one-way transmission."