THE WALL STREET JOURNAL.

Support Grows to Let Cybertheft Victims 'Hack Back'

June 2, 2013

By: Christopher M. Matthews

As companies weather a spate of high-profile computer attacks, support is growing for an option that for now is probably illegal: fighting back.

The Justice Department has long held that if a company accesses another party's computer network without permission, for whatever purpose, it is breaking the law.

But the idea of allowing the private sector to retaliate against hackers, euphemistically known as "hacking back," has gained momentum as U.S. companies wake up to the pervasive threat of cybercrime.

A commission led by Dennis C. Blair, President Barack Obama's first director of national intelligence, and Jon M. Huntsman Jr., the former U.S. ambassador to China, said last month that "without damaging the intruder's own network, companies that experience cybertheft ought to be able to retrieve their electronic files or prevent the exploitation of their stolen information."

In coming weeks, an influential panel of the American Bar Association is expected to release a report that will explore gray areas that might leave companies legal room to engage in "active defense." The report also will explore possible changes in the current law.

On its face, the issue seems simple. Hackers who have stolen corporate data should have limited expectations of a right to privacy.

But cybercriminals frequently hijack the systems and networks of unwitting third parties to launch their attacks and store stolen data, making the issue of retaliation more complicated and contentious.

A company might access a server it believes is storing its stolen data only to find that the server belongs to a school district in Tennessee, for example, and not to the actual hacker, who might be located in Eastern Europe.

Orin Kerr, a law professor at George Washington University, said that because it is so easy to disguise cyberattacks, there is a real risk that retaliatory measures could affect innocent bystanders, which raises a range of privacy concerns.

Most cybersecurity legal experts agree that hacking into a server believed to be involved in an attack, and destroying or damaging it, is neither legal nor a good idea. But advocates of active defense say there is a middle ground.

"This is not about shooting back, this is about investigating back," said Stewart Baker, former assistant secretary for policy at the Department of Homeland Security.

"No one wants to damage the computers of innocent third parties or misuse their data, and I would think the owners of the compromised systems would want to know they've been compromised," he said.

Cybersecurity experts say some companies have privately pressed for increased latitude to hack back, but are so far unwilling to go public because of the issue's delicate nature.

Kimberly Peretti, a former senior litigator for the Justice Department's Computer Crime and Intellectual Property Section, said she was unaware of any prosecutions of companies that had hacked back.

But she added that during her tenure at the department it routinely received inquiries from companies seeking tacit approval of such measures.

"We'd politely remind them there's a federal criminal statute barring that," said Ms. Peretti, who is now a partner at law firm Alston & Bird.

The coming report of the ABA's Cybersecurity Legal Task Force is expected to focus, in part, on a practice called "beaconing," essentially inserting code into your data that, when the data is stolen, can signal back to you where the information is being stored.

Harvey Rishikof, a law professor at Drexel University and co-chairman of the task force, said the legality of this practice isn't entirely clear.

"There's the black-letter law, and there's the gray area," he said. "Can you put a beacon on your data? Another level is, could you put something on your data that would perform a more aggressive action if the data was taken?"

A more-aggressive strategy could include inserting code that would cause stolen data to self-destruct or inserting a program in the data that would allow a company to seize control of any cameras on the computers where the data were being stored.

When it comes to active defense, the principal law of the land is the Computer Fraud and Abuse Act, adopted in 1984, which many lawyers and legal scholars say is outdated.

The traditional understanding is that the act largely prohibits active defense and, according to Mr. Baker, who is now a partner at Steptoe & Johnson LLP, prosecutors have threatened to charge companies under the statute if they employ such tactics.

Mr. Baker has called for amendments to the law to carve out protections for companies to hack servers involved in breaching their systems as part of an effort to investigate who is behind the incursion.

Justice Department officials said that nearly all active-defense practices are illegal, and rightly so. In certain circumstances beaconing could be legal, as long as the concealed software wouldn't do other things like allow a company to access information on the system where the stolen data were stored, one official said.

According to Mr. Kerr of George Washington University, any legislative fixes could be difficult because it would be nearly impossible to prescribe protections solely for "justified" retaliatory hacking.

"The people advocating this are thinking of Fortune 500 companies who want to hack into a [computer] address in China," Mr. Kerr said. "But there's no obvious way to [contain] that power. Could an 18-year-old who thinks he's been hacked by the White House start hacking back?"

So far, the issue hasn't found a congressional champion.

The Cyber Intelligence Sharing and Protection Act, a major cybersecurity bill passed by the House of Representatives in April, contained an amendment that specifically stated that the bill didn't permit hacking back.

Rep. Jim Langevin, the Rhode Island Democrat who wrote the amendment, said in an email: "Without this clear restriction, there is simply too much risk of potentially dangerous misattribution or misunderstanding of any hack-back actions."

Sharon Bradford Franklin, senior counsel at the Constitution Project, a nonpartisan civil-liberties group, said that business lobbying groups had indicated in private conversations that the issue was a priority on their cybersecurity agenda.

Ms. Franklin declined to disclose which groups are focused on it. The U.S. Chamber of Commerce and the Business Roundtable, which lobbied heavily on the legislation the House passed in April, declined to comment.

Critics of active defense say that even if hacking back became legal, it would be dangerous to take on hackers, who have shown they are technologically sophisticated enough to hack your systems.

"There's a good chance you won't know who's hacking you," said Jody Westby, chief executive of advisory firm Global Cyber Risk LLC and a member of the ABA panel.

"Say it's the [People's Liberation Army of China]; is that a group you really want to tick off?" Ms. Westby said.

Write to Christopher Matthews at christopher.matthews@dowjones.com

A version of this article appeared June 3, 2013, on page B6 in the U.S. edition of The Wall Street Journal, with the headline: Cybertheft Victims Itchy to Retaliate.

View this article on wsj.com