Some companies looking at retaliating against cyberattackers

June 13 2013, by Paresh Dave

Frustrated by their inability to stem an onslaught of computer hackers, some companies are considering adopting the standards of the Wild West to fight back against online bandits.

In taking an eye-for-an-eye approach, some of the companies that have been attacked are looking at retaliating against the attackers, covertly shutting down computers behind the assaults or even spreading a new virus to stymie the hackers.

Such retaliation is illegal in the United States, but companies see it as a way to curtail the breaches, particularly if the attack is originating from another country, where the legality of retaliatory attacks is unclear.

Companies also view counterattacking as a way to bypass U.S. authorities, avoiding publicly admitting that they've been attacked and exposing themselves to lawsuits from loss of confidential data or service disruptions.

Many companies that have publicly acknowledged costly breaches declined to say whether they retaliated or considered hacking back, and no company was willing to talk about the issue out of fear of additional attacks.

But analysts say hacking back has become part of a serious debate among companies, lawmakers and cyber-security experts.

"From a technical perspective, it's not that challenging," said Alex Harvey, a security strategist for the security solutions provider Fortinet. "Breaking in and shutting them down isn't hard, but a new one will just pop. You'll get a couple of minutes of peace and quiet."

Security platform provider FireEye says a single organization is targeted by malware about every three minutes. From detection to damage control, the average company of more than 1,000 workers spends nearly $9 million annually on cybersecurity, according a survey last year by the independent Ponemon Institute.

In a recent report about combating intellectual property theft, a private commission led by former U.S. Ambassador to China Jon Huntsman Jr. and former Director of National Intelligence Dennis Blair called for "informed deliberations" about whether corporations and individuals should have more flexibility to defend intrusions.

Federal lawmakers remain at odds about how to deter cyber crime. Many in the security industry strongly advise against retaliation. Federal law bars any unauthorized computer intrusion, and it offers no exception for digital self-defense.

"I don't think companies should be hiring gunslingers to fight back," FireEye co-founder Ashar Aziz said. "Before we encourage every random company to hack, we have to look at what makes sense to disrupt cybercrime."

Aziz and other information security experts promote what they say are smarter alternatives. For instance, companies can bolster security by creating multiple versions of sensitive data, with only one version being the legitimate one. In that case, attackers are likely to get their hands on worthless data rather than precious information.

Companies remain intrigued by the idea of shutting down an attacker's system.

The report from the commission chaired by Huntsman and Blair notes that counterattacks have the potential to deter hackers because the cost of doing business rises. But the commission stopped short of recommending legalizing retaliatory hacking "because of the larger questions of collateral damage."

Many cyberattacks rely on a network of computers. These infected machines might be owned by innocent Internet users who, for example, accidentally clicked on a bad link in their email. Surreptitiously accessing this computer violates federal law, even if it's to update out-of-date software or remove the malicious program.

"If Honda comes over and attacks Ford, then Ford can't send someone over to attack Honda," said Anthony Di Bello, head of strategic partnerships at Pasadena, Calif.-based Guidance Software.

But some legal experts say it's not so clear-cut. Under one legal argument, the hacker becomes subject to the rules and policies of the organization it attacks by virtue of connecting to that network. Counterattacks could be justified in the same way that an employer has the right to monitor activities on an employee's work computer.

Microsoft Corp. has taken another approach, considered by some to be a "responsible" counterattack. The company sues unidentified hackers and secures court approval to shut down computers engaged in malicious activity. But that approach may not be feasible for most companies, which don't have the computer giant's cash coffers.

Rodney Joffe, senior technologist at the security software manufacturer Neustar Inc. and a regular cybersecurity advisor to the White House, said

counterattacks and even legally sanctioned actions provide only temporary relief.

"It makes a great splash and creates a sudden vacuum, but there's hundreds of people who fit into that vacuum because it doesn't take attackers very long to climb back over the wall," Joffe said.

Criminal prosecutions are the best deterrent, but they require more cooperation between the government and the private sector, he said.

The Cyber Intelligence Sharing and Protection Act, passed by the House in April, frees companies from liability if they share information about incoming attacks with law enforcement. Senate leaders have said they may introduce a competing measure with stronger privacy protections for consumers.

Joffe said he expects some form of a safe-harbor law for companies by the end of the year.

"We need something that encourages sharing of information, and in some cases mandates it," he said. "Our enemies have almost carte blanche to walk over us right now, and there's little that can be done about it."

Some security analysts argue that lawmakers need to go even further, using a constitutional provision to grant a "letter of marque and reprisal" authorizing private companies to counterattack in self-defense. The nation's Founding Fathers wrote the provision as a way to help merchant ships fend off pirates.

Patrick Lin, director of the Ethics and Emerging Sciences Group at California Polytechnic State University-San Luis Obispo, said today's companies may be able to obtain the authorization and justify a

counterattack.

"To be sure, it would have to be a desperate situation to grant a letter of marque, but we may be in that situation now," he said.