



MARLIN RISING - Check Out the Marlin Steel Blog!

LEADING AN AMERICAN MANUFACTURING RENAISSANCE



Hackers pose a serious threat to U.S. small business

12:30 p.m. EDT, May 5, 2013

When I [bought Marlin Steel in 1998](#), the extent of its technology was an old fax machine. Today, our factory is full of industrial robots that are fed computer-aided designs and churn out steel containers for industry 60 times faster than before.

We're [winning jobs that used to go to China](#) and elsewhere. My employees, who once made \$6 an hour, average \$26 an hour now.

This isn't your grandfather's small factory: We depend on the Internet, cloud computing and other new technologies, just like thousands of other manufacturers our size. We [operate in high-tech ways](#) that only the largest plants could afford years ago. Yet we're vulnerable to our operations being exploited or disrupted by hackers with bad intent.

The U.S. House of Representatives recently approved the Cyber Intelligence Sharing and Protection Act (CISPA) in one of the most bipartisan votes of the past couple of years. Ninety-two Democrats voted with Republicans in favor of the House bill, while 29 Republicans opposed it. That two-thirds majority veto-proofed the bill should it clear the Senate and reach the President Barack Obama's desk.

The Senate, however, is indicating it might not take up the bill, and the White House has already vowed a veto should it pass the Senate. They say they are concerned about the threat to business, but talk is cheap.

I applaud the House for trying to confront the problem. The co-sponsors of the bill, Rep. Mike Rogers (a Michigan Republican) and Rep. C.A. Dutch Ruppersberger (a Maryland Democrat) worked for a year to address concerns about an earlier version of the legislation. Congressman Ruppersberger, who represents the district where my business is located, stood up to oppose Minority Leader Nancy Pelosi on this as well.

The more resources and energy that small business owners spend on network security to fight hackers, the less it's investing in things like equipment and training that help them win more jobs, grow their businesses and hire more workers.

And make no mistake: Small to-medium-size businesses are targets for hackers: Nearly one-third of all cyber-attacks are against businesses with fewer than 250 employees, according to a recent study by Symantec. The threats range from criminals overseas to disgruntled former employees at home.

Recently, a multinational investigation led to the arrest in Spain of a Dutch man on charges of arranging the biggest cyber-attack in Internet history. We've already come across dozens of instances where the designs of our material handling baskets were stolen by websites in China and India.

I attended a meeting in Washington this winter where U.S. Attorney General Eric Holder put businesses with trade secrets in two categories: Those that realize they already have been compromised by hackers and those that don't know it yet.

Freeing up business and government to share information, as the House bill would do, is a vital step to fight this growing threat. It's unacceptable for the U.S. Senate to say this issue is too complex and to walk away from it again.

Drew Greenblatt, Baltimore

The writer is president of [Marlin Steel Wire Products](#).

<http://www.baltimoresun.com/news/opinion/readersrespond/bs-ed-cybercrime-bill-20130505,0,113854.story>

Marlin Steel 2640 Merchant Drive, Baltimore, MD, USA 21230-3307

[Engineering Services](#) | [Precision Steel Fabrications](#) | [Steel Wire Baskets](#) | [Wire Forms](#)

Quality Engineered QuickSM Call Today → 443-552-5400