Stopping cyberattacks likened to a war and experts say the crooks are winning so far

August 12 2014, by Steve Johnson, San Jose Mercury News

After last week's stunning revelation that Russian crooks had stolen 1.2 billion user names and passwords, the biggest breach on record, experts say making the Internet more secure will take a huge global effort -bolstering website security, a stronger push to prosecute the cybercriminals and better vigilance by consumers.

How much all that might cost is unclear, with some experts estimating it could take billions of dollars, while others insist it's more a matter of redirecting what already is being spent toward more fruitful areas. But even then, critical information on the Internet may never be entirely safe, given the growing sophistication and ability of hackers to find new ways to steal it.

The attack by a Russian gang, uncovered by a Milwaukee security firm, has inflamed concerns about data protection on the Internet and whether the security practices of thousands of companies around the world are sufficient to protect financial and personal information. Security experts say businesses need to take the lead in countering the threat, particularly since the software and gadgets they make to access the Internet are frequently riddled with weaknesses that hackers can exploit.

"There is zero or very little corporate responsibility being taken to insure products in the market are safe," said Melissa Hathaway, a former top federal cybersecurity official with the National Security Council and the Office of the Director of National Intelligence, who now has a consulting firm. "If we continue to see the market the way it is, we'll see

more victims."

Critics have faulted many companies for being slow to address their vulnerabilities because of factors including ignorance about the extent of their flaws and the cost associated with fixing them.

Alan Paller, director of research at SANS Institute, an organization that trains computer-security experts, said that because software can be easily manipulated by crooks, it's essential to either make programmers responsible for the financial damage that results when their code is hacked, or, at least, make them demonstrate they know how to write safe software through a skills test.

Paller said companies also need to improve the ability of their security staffs to deal with cybercriminals who sneak into the corporate networks. I don't think they know how to do it in many cases," he said.

Moreover, he said companies should stop wasting money writing security-related reports - some of which are required by the federal government - and focus more on actually battling hackers. That's why he believes tackling cyber crime wouldn't require a huge additional expenditure, because "fundamentally, it's a shift from talking about the problem to fixing the problem."

But others argue that companies will need to spend substantially more, because many of them so far haven't taken the threat seriously.

Avivah Litan, an analyst with the research firm Gartner, estimated that many companies could protect themselves reasonably well by spending $50,000 to $100,000 a year on security, while larger firms might have to spend $5 million to $10 million. While that's a lot of money, she added, the cost of a breach that results in the company losing its commercial secrets or alienating its customers could be much higher.

One key measure companies could take is to shift from having their websites accessed with user names and passwords to employing biometric identification systems, according to Larry Ponemon, whose Ponemon Institute studies data protection and privacy issues. He noted that some companies already offer voice identification technology for accessing computer gadgets, and he predicts that retinal and facial identification devices could become widely available within five years.

Others argue that the best way companies can avoid having their websites or other operations breached is to think more like the hackers, pointing to Tuesday's disclosure about the 1.2 billion user names and passwords that were stolen from 420,000 websites.

"This breach illustrates how traditional security tools alone don't do enough," said Carl Wright of TrapX Security of San Mateo, adding that businesses "must be as nimble as the attackers themselves and be able to adapt in real-time to defend against evolving threats."

Several experts also implored the government to work more with foreign nations to crack down on cybergangs, and increase penalties for U.S. companies that lose personal information due to security lapses. And until better methods are instituted, consumers are advised to stop using the same passwords or other personal identifiers to access different websites, because that practice greatly increases their chances of having their identities hijacked and their bank accounts, credit card numbers or other data stolen.

Even with a concerted effort by everyone, experts say, it's going to be tough to stem the growing tide of cyberattacks.

"It seems to be getting worse and if we look at this as warfare we are losing most of the battles," said Ponemon, noting that "the cyberattackers are stealthy and smart and well funded." But over the next

decade, "we stand a good chance to win the war. I'm mildly optimistic."