Cyber defenders urged to go on the offense

July 26 2012, by Glenn Chapman

Former FBI cyber crime unit chief Shawn Henry, pictured in 2010, told computer security champions they should focus on hunting down and eliminating hackers, spies, terrorists and other online evildoers to prevent devastating Internet Age attacks.

Computer security champions on Wednesday were urged to hunt down and eliminate hackers, spies, terrorists and other online evildoers to prevent devastating Internet Age attacks.

The first day of briefings at a prestigious Black Hat computer security gathering here opened with a former FBI cyber crime unit chief calling for a shift from defense to offense when it comes to protecting networks.

"We need warriors to fight our enemies, particularly in the cyber world right now," Shawn Henry said in a Black Hat keynote presentation that

kicked off with dramatic video of hostage rescue teams training.

"I believe the threat from computer network attack is the most significant threat we face as a civilized world, other than a weapon of mass destruction."

The peril grows as water supplies, power grids, financial transactions, and more rely on the Internet and as modern lives increasingly involve working and playing on smartphones or tablet computers, according to Henry.

He rolled off a list of adversaries ranging from spies and well-funded criminals to disgruntled employees with inside knowledge of company networks.

"Cyber is the great equalizer," Henry said.

"With a $500 laptop with an Internet connection anybody, anywhere in the world can attack any organization, any company," he continued. "The last time I checked, that was about 2.3 billion people."

After 24 years of working for the FBI, Henry in April switched to the private sector as the head of a division at startup CrowdStrike specializing in cyber attack incident responses and identifying adversaries.

The computer security industry to expand its arsenal beyond just building walls, filters and other safeguards against online intruders to include watching for, and gathering intelligence on, culprits who have slipped through.

"It is not enough to watch the perimeter," Henry said, equating computer security to protecting real world offices. "We have to be constantly

hunting; looking for tripwires."

In the cyber world, that translates into monitoring system activities such as whether files have been accessed or changed and by whom.

"The sophisticated adversary will get over that firewall and walk around, like an invisible man," Henry said. "We have to mitigate that threat."

Tactics for fighting cyber intruders should include gathering information about how they operate and the tools used, and then sharing the data in the industry and with law enforcement agencies in relevant countries.

"Intelligence is the key to all of this," Henry said. "If we understand who the adversary is, we can take specific actions."

Teamwork between governments and private companies means that options for responding to identified cyber attackers can range from improved network software to political sanctions or even military strikes, according to Henry.

"You can't make every school, every mall, every university, and every workplace impenetrable," Henry said. "We have to look at who the adversary is and stop them in advance of them walking in."

Black Hat founder Jeff Moss, the self-described hacker behind the notorious Def Con gathering that starts here on Thursday, backed Henry's argument.

"Maybe we need some white blood cells out there; companies willing to push the edge and focus on threat actors," Moss said, calling on the computer security community to "raise the immunity level."

Moss is head of security at the Internet Corporation for Assigned Names

and Numbers, which oversees the world's website addresses.

"So, am I Luke, or am I Darth Vader; sometimes I'm not sure," Moss quipped about his roles in the hacker realm and the computer security industry.

"It depends upon which day and who asks."

Moss proposed that cyber attackers also be fought on legal fronts, with companies taking suspected culprits to court.

"I can't print money; I can't raise an army, but I can hire lawyers and they are almost as good," Moss said. "One way to fight the enemy is you just sue them."

Henry feared that it may take an Internet version of the infamous 9/11 attack in New York City to get the world to take the cyber threat to heart.

"We need to get down range and take them out of the fight," Henry said.

"As well-trained, well-equipped cyber warriors you can have an impact; the stakes are high."