March 27, 2012

# The Cyber Threat

## Part 1: On the Front Lines with Shawn Henry

Note: Shawn Henry retired from the FBI on March 31, 2012.

Shawn Henry realized a lifelong dream when he became a special agent in 1989. Since then, he has traveled the world for investigations and become one of the FBI's most senior executives and its top official on cyber crime. FBI.gov recently sat down with Henry—who is about to retire from the Bureau—to talk about the cyber threat and his FBI career.

**Q: You were involved with cyber investigations long before the public had an awareness of how serious the threat is. How did you become interested in the cyber realm?**

**Mr. Henry:** I was always interested in technology, and in the late 1990s I started to take courses at the FBI related to cyber intrusion investigations. When I had an opportunity to move over to that side of the house, I seized it. I saw right away that the challenges we were going to face in the future were tremendous, and I wanted to be on the front lines of that.

**Q: How has the cyber threat changed over time?**

**Mr. Henry:** Early on, cyber intrusions such as website defacements and denial of service attacks were generally perceived to be pranks by teenagers. But even then, in the late 1990s, there were state actors sponsored by governments who were attacking networks. What received media attention was the teenage hacker and the defacements, but there were more significant types of attacks and a more substantial threat that was in the background. Also, those early attacks were much more intermittent. Now we are seeing literally thousands of attacks a day. The ones people hear about are often because victims are coming forward. And there are more substantial attacks that people don't ever see or hear about.

**Q: Where are the cyber threats coming from today?**

**Mr. Henry:** We see three primary actors: organized crime groups that are primarily threatening the financial services sector, and they are expanding the scope of their attacks; state sponsors—foreign governments that are interested in pilfering data, including intellectual property and research and development data from major manufacturers, government agencies, and defense contractors; and increasingly terrorist groups who want to impact this country the same way they did on 9/11 by flying planes into buildings. They are seeking to use the network to challenge the United States by looking at critical infrastructure to disrupt or harm the viability of our way of life.

**Q: How has the FBI adapted to address the threat?**

**Mr. Henry:** We have grown substantially, particularly in the last four or five years, where we have hired more technically proficient agents, many of whom have advanced degrees in computer science or information technology. We bring them on board and teach them to be FBI agents rather than trying to teach FBI agents how the technology works. That has given us a leg up and put our capabilities on par with anybody in the world. We have also worked proactively to mitigate the threat by using some of the same investigative techniques we use in the physical world—undercover operations, cooperating witnesses, and authorized surveillance techniques. We have taken those same time-tested tactics and applied them to the cyber threat. So we are now able to breach networks of criminal actors by putting somebody into their group. The other critical area we have been successful in is developing partnerships.