FBI Sharpens Focus on ESCALATING Cyber Threat

by FBI Executive Assistant Director Shawn Henry

(Editor's Note: This is the first in a three-part series about the cyber threat, what the FBI is doing to mitigate it, and what you can do to reduce your own vulnerability.)

Some of the most critical threats facing our nation today emanate from the cyber realm—not only from hackers out to rob us of our personal information and money, but also spies who seek to steal our nation's secrets, as well as terrorists who are looking for novel ways to attack our critical infrastructure.

The cyber threat is an existential one, meaning a major cyber attack could potentially wipe out entire companies, shut down our electric grid or water supply, destroy swaths of our cities, and ultimately even potentially kill U.S. citizens.

While it may sound alarmist, the threat is incredibly real, and intrusions into corporate networks, personal computers, and some government systems, are occurring every single day.

Sophisticated Adversaries

There are three primary actors in the cyber world: foreign intelligence services, terrorist groups, and organized crime enterprises. Dozens of countries have offensive cyber capabilities, and their foreign intelligence services are generally the most capable of our cyber adversaries. Their victims run the gamut from other government networks to private companies from whom they seek to steal secrets or gain competitive advantage for their nation's companies.

Terrorist groups have openly expressed an interest in launching a cyber attack on our electric power grid, water supply or other critical infrastructure. Though they may not currently have the capability to do so, the reality is that cyber criminals offer their services freely on the open market and often don't care for whom they're working.

Organized crime groups, meanwhile, are increasingly migrating their traditional criminal activity from the physical world to the computer network. Rather than breaking into a bank with guns to crack the safe, they breach corporate networks and financial institutions to pilfer data —including personally identifiable information — that they can monetize.

High Stakes

These groups, often made up of individuals living in disparate places around the world, have stolen hundreds of millions of dollars from the financial services sector alone, increasing the cost of doing business and creating a drain on our economy.

One company we notified that it was the victim of an intrusion determined it had lost 10 years worth of research and development — valued at $1 billion — virtually overnight.

The "2011 Norton Cybercrime Report" put the global cost of cybercrime at nearly $400 billion a year and found there are more than one million victims of cybercrime every day.

A recent study by the Ponemon Institute, a research think tank, found that the number of cyber attacks on companies it surveyed in 2010 were up 45 percent from the previous year and cost 70 percent more to fix. On average, each attack took 18 days and $416,000 to remediate.

In one of the more sophisticated and organized attacks ever on the financial sector, an international network of hackers accessed the computer network of RBS WorldPay, the U.S. payment processing division of the Royal Bank of Scotland, located in Atlanta. During the 2008 attack, the hackers compromised the encryption the company used to protect customer data on payroll debit cards. They raised the limits on compromised accounts, then provided a network of "cashers" with 44 counterfeit payroll debit cards. Those cashers withdrew more than $9 million from automated teller machines in more than 100 cities around the world — all in less than 24 hours. That is real organized crime.

This case illustrates how the offense far outpaces the defense in the cyber realm. Unfortunately, under the current Internet infrastructure, we can't "tech" our way out of it. That doesn't mean, however, that we should throw up our hands and surrender to our cyber adversaries.

Coming next month: "What is the FBI doing to mitigate the cyber threat?" ✣