FBI Sharpens Focus on Escalating Cyber Threat Part 3

by FBI Executive Assistant Director Shawn Henry

Reducing Your Vulnerability and Managing the Consequences

In today's digital world, everything you or your clients depend on is either stored or transmitted electronically. Because of that, the data and information is substantially vulnerable. Intrusions into personal computers, corporate networks and government systems are occurring every single day. Now, it's not so much a question of IF your computer or network will be breached, it's a question of WHEN.

Before it was created, the Internet was something very few people could have imagined. It is arguably the greatest invention of our lifetime, but it can also be a dangerous place. As we look toward the future, it's crucial that we recognize the risk that exists with the environment we're working in and learn to manage it.

Managing the Risk

When it comes to the Internet, managing the risk means we must divide our resources and efforts to reduce each of the factors that put us at risk. To do so, it's important to understand the classic risk formula, which states, "RISK equals THREAT times VULNERABILITY times CONSEQUENCES."

If we lower any of the three variable factors, we lower the risk. If we can completely eliminate any of those variables, we eliminate risk. That is virtually impossible, however, so we must adopt a defense-in-depth approach — lowering each of the three.

Translating these concepts to the cyber security realm, we've already established that the threat exists and is increasing. We can reduce the threat by taking a law enforcement, intelligence or economic action to prevent or deter an adversary from acting. But how do we lower the vulnerabilities of the cyber threat? It could entail keeping certain pieces of information off the network — maybe in a physical safe. Managing the consequences of a cyber attack entails minimizing the harm that results when an adversary does break into a system. An example would be encrypting data so the hacker can't read it, or having redundant systems that can readily be reconstituted in the event of an attack.

Security at Home

As users of computers and other Internet-connected devices, you must take responsibility for being aware of the threats to your personal information and your hardware, taking those threats seriously, and protecting yourself from them as best you can.

Simple things like using strong, frequently changed passwords and updated security and anti-spyware software on all your devices are good places to start. Keep your operating system up to date, keep your firewall on, and don't open e-mail links or attachments from people you don't know.

Cyber crime victims also should report unlawful activity to law enforcement or on-line to the Internet Crime Complaint Center at www.ic3.gov.

Security in the Workplace

Physical security in the private sector is relatively straightforward: You have an alarm on the front door of your company. Who is responsible for responding if it goes off? What do they do if it goes off? Do you have someone walking up and down the hallways looking in windows with a flashlight? If someone's leaving the company with a bunch of boxes, do they have a pass?

Equating that to the digital world, how do we protect our data? What's the equivalent to the night watchman? We should be aggressively and proactively pursuing the adversary in our own networks rather than waiting for something to happen. We should be looking for changes on networks, determining who's accessing the system and what they are downloading. If someone's leaving the company, how do we know they haven't downloaded gigabytes of data on to a thumb drive? It comes down to active analysis and active patrol of the network.

A recent survey of U.S. information technology and IT security practitioners conducted by the Ponemon Institute for McAfee identified five key success factors in data protection programs. They include: A formal data protection strategy with metrics; regular testing of data protection solutions; centralized management of the data protection program; and automated policies for detection and prevention of end-user misuse of information — and the enforcement of those policies.

Moving Forward

Together, government, industry, and private citizens can work to manage the risks cyber criminals pose and make their costs more trouble than they are willing to bear. Start by locking your virtual front door. ✠

On March 31, Executive Assistant Director Shawn Henry retired from the FBI after 24 years of service. In his new private-industry position, he will continue to work at the national level to help develop solutions to protect and further insulate private industry and government computer systems from intruders seeking to do harm.