GOVINFOSECURITY

Is Cyber Threat Overstated?

June 26, 2009 - Eric Chabrow

Warnings of catastrophic harm caused to government and the economy by cyber assaults are exaggerated, and such overstatements could misdirect government leaders in developing cybersecurity policy.

That's the essence of testimony given Thursday by Jim Harper, director of information policy studies at the libertarian think tank Cato Institute, before the House Subcommittee on Technology and Innovation. In his prepared testimony, Harper said:

> "Overuse of urgent rhetoric is a challenge to setting balanced cybersecurity policy. Threat exaggeration has become boilerplate in the cybersecurity area, it seems, and while cybersecurity is important, overstatement of the problems will promote imbalanced responses that are likely to sacrifice our wealth, progress, and privacy."

Though Harper may underestimate the true threat to the nation and economy from cyber attacks, his view raises an important point that urgent rhetoric must be balanced by facts regarding real threats.

In his testimony, Harper analogized the real world with the virtual one - PCs represent homes, corporate and government networks are cyberspace's office buildings - and concludes harm caused to a nation or economy in the real world are far worse than those envisioned in the virtual one. Here's a comparison he makes between a cyberattack and conventional military attack:

> "The Center for a New American Security is hosting a cybersecurity event this week, and the language of the invitation says: "[A] cyberattack on the United States' telecommunications, electrical grid or banking system could pose as serious a threat to U.S. security as an attack carried out by conventional forces.
>
> "As a statement of theoretical extremes, it is true: The inconvenience and modest harms posed by a successful crack of our communications or data infrastructure could be more serious than an invasion by an ill-equipped, small army. But as a serious assertion about real threats, an attack by conventional forces - however unlikely - would be entirely more serious than any realistic cyberattack. We would stand to lose national territory, which cannot be reconstituted by rebooting, repairing software and reloading backed-up files."

Harper contends a more plausible strategic use of attacks on communications and data infrastructure is not "cyberterrorism" or "cyberattack," but what might be called "cybersapping" - infiltrating networks to gain business intelligence, intellectual property, money, personal and financial data and perhaps strategic government information. He said:

> "These infiltrations can slowly degrade the advantages that the U.S. economy and government have over others. They are important to address diligently and promptly. But they are not a reason to panic and overreact."

Harper reminds me of the Y2K skeptics of the late 1990s, who dismissed the argument that not to remediate the computer date problem would create worldwide fiscal chaos. Nearly 9½ years later, I'm still unsure whether the Y2K threat was exaggerated or not.

Harper advised Congress:

> "Cybersecurity is important, but exaggerating threats and failures as a matter of routine will lead to poor policymaking. Do not let the urgency of many statements about cybersecurity 'buffalo' you into precipitous, careless and intrusive policies."

He's right, laws shouldn't be made by exaggerated threats. The question is: Are these threats overstated?

I believe threats can be overstated. That is why it is crucial to use a risk management process and continuous monitoring to evaluate threats and their impacts on systems. Unless Mr. Harper has conducted a risk assessment on the telecom industry and has the data to backup his assertion, he runs the risk of understating the threat.

While a real world attack on U.S. territory is not the same as a virtual one, there is still an attack, and there still is cyberterrorism, especially when an individual or group is trying to cause fear to U.S. citizens. That is no different than someone who bombs a building to create fear and panic.

Destroying or causing significant degradation of the telecom infrastructure may not cause as great a loss of life as a gang driving down a street and shooting people randomly, there can still be a loss of some life through the panic caused or by emergency responders not being able to get where they need to be when there is an emergency.

So the bottom line, in my opinion, is to conduct risk assessments and understand the threats and their impacts and use continuous monitoring to stay up-to-date on the threats, so all efforts spent on protection and defense are well spent.

Posted by **CISSO** on June 26, 2009 @ 08:08 AM

Close Window
