FINANCIAL TIMES
MONDAY APRIL 25 2011

Comment

To win the cyberwar we have to reinforce the cloud

Mike McConnell

Many challenged my grim assessment early last year, when I called for America to develop a new strategy to address the kinds of cyberattacks that could cripple our nation's infrastructure. If there were a cyberwar, I told Congress, we would lose. The unfortunate truth is that, a year later, we are no better prepared – and the stakes have risen.

Since then more details have emerged on the early 2010 attacks on Google and two dozen other companies, connecting them to China. Alongside the revelations about the Stuxnet attack on Iran and the WikiLeaks saga, the question today is no longer whether the cyberthreat is real – that was last year's discussion. The challenge now is what to do about it, while balancing security, privacy, openness and innovation.

We should immediately focus on protecting critical infrastructure – the power grid, financial networks, air traffic control and other transport infrastructure — by realigning their use of the internet. To do this we must create new "protected lanes" inside the global superhighway. I call this potential area "dot.secure": a series of highly protected lanes for those operating vital infrastructure, within the free and open world of the .com global network.

The WikiLeaks saga has generated intense debate about whether the release of classified government information is in the public interest. To be clear, I am not an advocate of doing away with the freedom of our citizens and their use of the internet. But I would also argue that we are a nation of laws, and everyone is entitled to privacy – individuals, businesses and, yes, government.

To do its business effectively the government must be able to exchange information with other governments in private. Businesses must be able to protect innovation and patented information; individuals must be able to keep the ownership of their new ideas.

There also need to be defined areas of the internet where that can take place – where individuals can post to blogs, create videos, comment on the news and be completely anonymous – and other places where access to specific data is restricted. Equally, we must develop access systems for sensitive business where an individual is limited to data essential to his or her task.

We must create new protected lanes inside the global superhighway for those operating vital infrastructure

Highly secure and open areas of the internet do exist today. The defence department runs ".mil," a domain with limited gateways, military grade encryption, perimeter security and support from the National Security community to identify foreign threats. The government's ".gov" domain has a similar goal of limited gateways, but will also benefit from high-grade encryption.

On the other side of the information highway, the .com lanes are open with easy movement and access, requiring only the level of security that an individual or business requires for themselves. These open lanes are less costly to maintain, and will benefit even more from the economies of cloud-computing, a powerful, cost-efficient shared computing environment.

What's missing is the middle ground: dot.secure. The nation's finance, electric, power, water, land transport, air traffic control, industrial control systems must be protected within the security of the restricted lanes. Each month, we understand more about how to heighten security in the "cloud", and our technicians develop more nuanced approaches to security architecture. Beyond that, cloud operators can focus on network intrusion prevention and response to protect information and its users.

We need to apply the evolving knowledge of cloud-security to our infrastructure through a new government/private partnership. The administration and Congress know the seriousness of cyberthreats, but they are not moving fast enough to address them.

We must remember that cyberspace is more than just the internet. It is a domain itself. For America to protect our economy and way of life as we have in the other domains, we cannot wait for the next big attack to shock us into action.

The writer was director of the National Security Agency in the Clinton administration and director of national intelligence in George W. Bush's second term. He is executive vice-president of Booz Allen Hamilton