

Cybersecurity: DHS' Role, Federal Efforts and National Policy

Wednesday, June 16, 2010

Stewart A. Baker
Partner
Stephoe & Johnson LLP

“Cybersecurity: DHS’ Role, Federal Efforts and National Policy”
Hearing before the House Committee on Homeland Security
Wednesday, June 16, 2010

Chairman Thompson, Ranking Member King, members of the Committee, it is a pleasure to appear before you again on a topic of such importance. I am Stewart Baker, formerly the Assistant Secretary for Policy at the Department of Homeland Security, and I am speaking for myself.

I was responsible for cybersecurity policy while at DHS, and since leaving the Department, I have been practicing law and writing a book on, among other things, the risks posed by computer insecurity. I'm celebrating the release of the book today by attending this hearing, and I'm happy to share some of what I learned with you today. (Chapters of the book itself are also being made available for free on line at www.skatingonstilts.com.)

The first and most important thing to know about the cybersecurity crisis is that you no longer need a clearance to understand how bad things are. For a decade or more, Presidents told us that we faced such a crisis, but they were never able to provide much detail. The crisis was classified. As a result, Americans didn't pay much attention, and they certainly weren't galvanized to action.

Thanks to a group of security researchers in Canada and elsewhere, though, we now have a good, unclassified analysis of what a cyberattack looks like. It is not pretty. And it is certainly not reassuring. If anything should stir the country to action on cybersecurity, it is the story of what was done to the Dalai Lama's computer network.

The Dalai Lama and his office have been using the Internet since the 1990s. His network administrators understand security risks, and they've been careful about computer security for years. They've implemented the standard defenses against network attacks.

But even so, they kept getting signals that their communications had been compromised. So they called in a team of computer security experts.

What the experts found was deeply troubling, and not just for the Dalai Lama.

Some of the Dalai Lama's staff participate in Internet forums. They chat with other, like-minded individuals about the Dalai Lama's goals and activities. Sometimes one of their

online acquaintances sends them Word or .PDF documents relevant to those activities.

No surprises there. Most of us have done most of those things.

But the experts concluded that hackers had monitored these forums and then forged an email from a forum participant to a member of the Dalai Lama's staff. Attached to the email was a document of mutual interest. When the staff member opened the document, he also activated a piece of malware packed with it. While the staff member was reading the document, the malware installed itself in the background.

The malware was cleverly designed; two-thirds of commercial antivirus software programs would have missed it. (Hackers often subscribe to antivirus software so they can test their malware against it at leisure.) Even if one attachment were stopped, it was a simple matter to retransmit the message using a different bit of malware; the attackers could keep trying until something got through.

Once installed, the malware would "phone home," uploading information about the victim's computer and files to a control server operated by the hackers.

Next, the captured computer would download more malware to install on the staff member's machine. This was often a complete administrative program that would allow the attackers to completely control the staffer's computer, and in some cases the entire network.

The administrative malware took full advantage of today's technology. It featured a graphic interface with dropdown menus offering even an unsophisticated attacker a wide variety of options.

Want to record every keystroke as the user types so you can steal all his passwords? Check one of the options on the menu.

Want to turn on the user's microphone, turning it into a bug so you can listen to the office conversations? Check another box.

Want video straight from the user's desktop camera? That's just another option on the menu.

In the end, the Dalai Lama's office was living a version of Orwell's *1984*. Telescreens in each room spied on the occupants. But in this version of *1984*, Big Brother didn't even have to pay for this spy equipment. It had been purchased and installed by the victims.

Once the hackers had compromised a single computer on the network, it wasn't hard to compromise more. Every time an infected computer sent a document by email, malware

could be attached to the file. The recipient couldn't possibly be suspicious; the email and attachment were exactly what he expected to receive from his colleague, and it had been reviewed by an antivirus program. He opened the document. The malware installed itself in the background. The cycle began again. It was an entire network of surveillance, dubbed Ghostnet by the security team.

Ghostnet has lessons for all of us, including members of this committee. Do you rely on standard commercial antivirus software to scan attachments? Do you open documents sent by people you've encountered online? How about documents from sources, contributors, or constituents? How about colleagues, coworkers, and staff? Of course, you do. So do I. And that means that most of us are no more able to defend ourselves from this attack than the Dalai Lama was.

That means we have no guarantee that foreign governments have not penetrated our home or even our office computer networks in the same way as the Dalai Lama, no guarantee that they are not monitoring our every keystroke on line.

Indeed, when I talk to computer security experts about how to defend against intrusions, they usually tell me to assume that the intrusions have happened before and will happen again. Because there's no way to stop them. At best, you might be able to catch the intruders when they try to steal your data. But you can't count on that, either.

Now that we understand the scope of the problem, what are we doing about it?

So far, not much. That's not a recent development, either. President Clinton cautioned a decade ago, in January 1999, that, "We must be ready—ready if our adversaries try to use computers to disable power grids, banking, communications and transportation networks, police, fire, and health services -- or military assets." A year later he proposed a series of measures to address the security problem.

Two years later, President George W. Bush created a special adviser on cybersecurity who spent a year developing a computer security strategy.

Neither effort made much headway. The public didn't see the problem. The network attacks that alarmed official Washington were classified. Officials couldn't talk about them.

Meanwhile, privacy and business interests worked overtime to persuade the public that national security concerns were overwrought. The real risk was government monitoring and government regulation, they insisted.

And that, by and large, was the view that prevailed -- twice, and under two Presidents. Nothing was done about computer security that anyone in the privacy or business lobbies might object to.

In 2009, President Obama became the third president who promised to make computer security a top priority. Shortly after taking office, the Obama administration produced a security strategy. Once again, though, the strategy lacked punch. It failed to call for any action that could possibly irritate business or privacy groups.

Since then, the President has belatedly appointed an experienced security professional to the National Security Council. DHS has begun hiring a large number of security professionals, and it is rolling out the least controversial incarnations of the government's intrusion detection system, called Einstein. But the administration has shown no sense of urgency in addressing the massive problems we face, especially in the private sector, where most of our critical infrastructure can be found.

That's why I'm pleased to be able to say that the Senate Homeland Security Committee has risen to the challenge. It recently offered a bipartisan and comprehensive bill that would address the problem in a responsible fashion. Senators Joe Lieberman (I-Connecticut), Susan Collins (R-Maine), and Tom Carper (D-Delaware) have introduced a bill that offers a real opportunity to improve the nation's cybersecurity.

I'm going to set aside the "boxology" imposed by the act -- a new White House Office for Cybersecurity Policy headed by a Senate-confirmed director, and a new freestanding security office (the NCCC) at DHS, which would include the existing U.S. Computer-Emergency Response Team (US-CERT) and would be responsible for detecting, preventing, analyzing, and warning of attacks. This office too would be headed by a political appointee who would be Senate-confirmed and would report directly to the Secretary of Homeland Security. If that were all the bill did, it would not add greatly to our security.

The real substance of the bill lies in the requirements it would impose on those critical infrastructures selected by the Secretary for coverage. ("Critical infrastructure" is defined by statute as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters private sector.")

First, the NCCC would, in coordination with the private sector, identify cyber vulnerabilities in covered infrastructures, and submit the findings to Congress. After consulting with the private sector, the NCCC would then issue regulations creating "risk-

based "security performance requirements for covered infrastructures. Owners and operators of the infrastructures would then select the specific security measures they will implement to satisfy the security performance requirement, and submit a compliance plan to the NCCC. Owners and operators would have the flexibility to implement any security measures that the Director determines would satisfy the security performance requirements. But, they would have to certify that they are in compliance, and would be subject to penalties if an audit by the NCCC determines that they are not. Those companies that meet the requirements would obtain some protection from liability, including immunity from punitive damages and limits on non-economic damages.

Second, critical infrastructure companies would be required to report to the NCCC "any incident affecting [their] information infrastructure ... to the extent the incident might indicate an actual or potential cyber vulnerability, or exploitation of a cyber vulnerability." ("Information infrastructure" means the "underlying framework that information systems and assets rely on to process, transmit, receive, or store information electronically, including programmable electronic devices and communications networks and any associated hardware, software, or data.") This requirement would sweep far more broadly than the data breach notification rules that presently exist at the state level, since it would include "any incident" that indicates even a "potential cyber vulnerability." But information shared with the NCCC would be protected from public disclosure.

Third, the bill would authorize the President to declare a national cyber emergency, which would then trigger the issuance by the NCCC of specific emergency measures to protect the continuing operations of critical infrastructure. Those measures would expire after 30 days unless the President or NCCC Director extended them. The emergency measures would have to be the "least disruptive" means necessary, and could not be used to avoid the requirements of the rules for intercepting phone calls or emails for law enforcement or intelligence purposes. Owners of covered critical infrastructures would have to comply with the emergency measures unless the NCCC approved alternative measures suggested by the infrastructures. Those owners that comply would be immune from civil suit in some instances, or would be protected from punitive damages and damages for non-economic harm in others.

I have no doubt that this bill will prove controversial. Privacy groups will tell us that the government can't be trusted with any authority over the computer networks on which we depend. Business groups will tell us that government regulation will raise costs and stifle innovation. I have no doubt that the proposed legislation will need to be modified as it makes its way through Congress. But I strongly urge this committee to give it careful consideration.

Today, we have a new, and troubling, example of what can happen if government fails to

take responsibility early for avoiding a serious risk.

As I speak, oil has been escaping from BP's Deepwater Horizon spill for nearly two months. As the spill shows, private companies are quite capable of setting the stage for catastrophes well beyond their ability to remedy. We properly expect the government to regulate companies to address risks that can't be internalized by the companies taking the risks. And when disaster strikes despite those efforts, we expect the President to have the authority to respond. The government is paying the price today for the actions it didn't take in the months and years before the blowout.

The same thing will be true, in spades, if another country launches a computer network attack on US infrastructure. Do we want the government to look as helpless in response to such an attack as it looks today in response to the BP spill?

Bad as the spill is, the country still has electric power, working phones, and a banking system. If we are attacked, we can't count on any of those things. But without something like the Senate bill, the President will be even more helpless to respond to the attack than he has been to respond to the oil spill.

Put simply, the country can't afford a disaster on that scale. And neither can its leaders.