"Cyber Security: Responding to the Threat of Cyber Crime and Terrorism"

Statement of Stewart A. Baker

Partner, Steptoe & Johnson LLP
Former Assistant Secretary for Policy, Department of Homeland Security

Before the Committee on the Judiciary
Subcommittee on Crime and Terrorism
United States Senate

April 12,2011

Good afternoon, Chairman Whitehouse, Ranking Member Kyl, and members of the subcommittee. My name is Stewart Baker. I have been involved in cybersecurity issues since the early 1990s, when I was General Counsel of the National Security Agency, and most recently as Assistant Secretary for Policy at the Department of Homeland Security during from 2005 to 2009. I appreciate the opportunity to address this vitally important issue.

Everyone knows that cybercrime is a problem. But everyone also seems to believe that the problem can be solved with modest additional effort.

In fact, cybercrime -- and the vulnerabilities on which it feeds -- will soon pose a profound challenge to our way of life, and perhaps even to America's role in the world.

Those who think the problem of cybercrime can be easily solved have embraced little myths that help them avoid taking harder steps.

I'd like to begin by identifying those myths and debunking them, because we won't begin to address the problem until we recognize that the easy solutions will not work. (I discussed several of these myths in my book, *Skating on Stilts*, and I've drawn on that material for today's testimony.)

Law Enforcement in Cyberspace: Not Even a Myth

Before I do, though, I'd like to address one solution that isn't taken seriously enough to even qualify as a myth: the notion that law enforcement can solve the cybercrime problem. It is true that federal authorities occasionally catch and prosecute a successful hacker. But those successes are dwarfed by the massive number of uncaught, unprosecuted, and even unreported hacks that occur every day. Very few victims even bother to go to the authorities any more. It would be like complaining that someone stole a wallet from your unlocked car in a bad neighborhood. You know, and so do the authorities, that the chances of solving the crime are so remote that even going through the motions of a report and investigation isn't worth the trouble.

Most problems of social disorder are contained by the threat of punishment. Human society depends so profoundly on social punishment as a survival mechanism that it is built into our genes. We have reward centers in our brains that fire when we punish rule-breakers – even if we can expect no individual benefit from a change in the rule-breaker's future behavior. Many of us will even incur costs just to punish rule-breakers we will never see again. (I probably don't have to tell you that if you've ever driven in Washington traffic.)

Yet the ease with which attackers can hide in cyberspace makes it almost impossible to punish criminal conduct online. We simply cannot identify the criminals. And so we find ourselves trying to build an online society where there is no real punishment for lawless behavior. Whether this is even possible is open to question. Those who think it is possible are counting on computer security – a bombproof defense – to make up for our inability to punish wrongdoers.

Counting on a bombproof defense would be a dubious proposal in the best of circumstances. It is particularly dubious when one realizes just how much of our defense is built on myths rather than reality.

The Myths That Keep Us from Dealing Squarely with the Cybersecurity Crisis

Myth 1: It's a Microsoft Problem. I know plenty of people who still believe that Microsoft's products are uniquely insecure, and that we could solve the problem if we could just get Microsoft to clean up its act. For some, the security of Linux was an article of faith; its source code is open to inspection by anyone, so it is protected from exploit by all those watching eyes. And Apple, which didn't even offer an antivirus program for decades, was protected by Steve Jobs's sheer coolness.

The last few years have been hard on those illusions. As Apple gained market share, malware authors began writing for its operating system, and they didn't have any trouble finding holes. And all those eyes on Linux's code? In August of 2009, two Google researchers discovered a bug in the central core of Linux; it would allow an attacker to acquire complete administrative control of any machine to which he had physical access. You might call that a success for open source, except that the bug had been hiding in plain sight for at least eight years.

Why, then, is there so much more malware running on Windows than on Linux? Almost certainly for the same reason that there are more applications of every sort running on Windows than on Linux. Like other application developers, malware authors want to reach the largest number of users with one piece of code. And the way to do that is to write your application for Windows.

Myth 2: It's a Password Problem. It's an article of faith among the security-conscious that passwords are a big security hole. People can't remember the hard ones, and hackers have assembled dictionaries of all the memorable ones. Plus, it's easy for hackers with access to a machine to capture the user's keystrokes as he types his password in.

So for real security, companies and government rely on tokens. RSA makes a common token. Every thirty seconds it displays a different security code, known only to the user and his network server. Even if a hacker could compromise my machine and record all my keystrokes, he couldn't know what the token was going to say thirty seconds from now. But hackers have demonstrated in two ways that tokens of this kind are no long-term solution. First, RSA recently announced that hackers had broken into RSA's network and compromised the security of the system. RSA is not providing a lot of details to the public, but it seems quite possible that, at least for some tokens, the hackers can now predict exactly what the token will say every thirty seconds, for years to come. And even those who cannot predict the token's future code have found a way to beat these token systems. Now, when the owner of a compromised machine starts typing in his temporary code, the malware immediately sends a real-time message to its sponsoring hacker. As the owner types, each digit is sent to the hacker, who simply logs in right along with the owner.

Myth 3: Really Important Transactions Can Be Confirmed Offline. More sophisticated users know that their home machines simply cannot be trusted. To protect their financial accounts, they've locked them up; they may bank on line, but no serious money can leave their account unless the bank calls to verify the transaction.

In fact, even those who haven't locked everything down may get a verifying call. Like the credit card companies, mutual funds and financial institutions have stopped trusting their customers' computers. For risky transactions, they insist on offline, or out-of-band, confirmation.

Out-of-band communication is today's most common fail-safe solution for computer compromises. But using another line of communication won't solve the problem for long. Finding a truly offline method of communication is going to get harder. Businesses and consumers are switching in large numbers to "voice over IP," or VoIP, telephony. They cannot resist the allure of bringing to voice communications the cheap, flexible features of Internet communications. But the switch means that they are also bringing to voice communications all the insecurity that plagues other Internet communications. In fact, telephone insecurity could be worse, as users download apps from unknown providers to no-name phones made cheap in the People's Republic of China, where hacking remains widespread. If an attacker who has compromised your computer's online bank account is also able to divert calls to your Internet telephone, then it will be easy for the attacker to confirm that you really do want to transfer your life savings to Moldova or Nigeria.

Myth 4: If Worse Comes to Worst, We'll Disconnect Our Critical Systems from the Internet. The government used to have its own special illusion about security. Maybe our unclassified networks are compromised, Defense Department officials would say, but the classified networks are still bombproof. They can't be compromised because they aren't connected to the Internet. There's an "air gap" between the two. That assumes, of course, that network security decrees are perfectly enforced—and that the most important secrets are only discussed on classified networks—notions that contradict everything we know about human nature. But never mind, because the air gap illusion, too, has fallen prey to the exponential empowerment of hackers that we've seen in recent years.

The French navy's Rafale Marine jets train out of Villacoublay air base, in the southwest suburbs of Paris. These fighters are state of the art, packed with stealth and electronic warfare capabilities and capable of landing on carriers. But to do that, they first have to take off. And for two days in January 2009, the jets couldn't take off.

They'd been grounded by a hacker.

The "Conficker" computer worm had been exploiting vulnerabilities in Windows servers for months. It was the most ambitious computer infection in years. At the time it had infiltrated as many as 15 million machines around the world. One of the ways it spreads is by infecting the USB thumb drives that carry data from one machine to the next. Even classified or isolated networks could be captured if a bad thumb drive was used to transfer data to a machine on a secured network.

That's what grounded the French fighters. Before the navy even knew it was under attack, the worm was coursing through its internal network. Rushing to contain the damage, the navy told its staff not to turn on their machines, and its systems administrators began quarantining parts of the network.

Too late for Villacoublay. Its systems were already hosed.

The Rafale fighter downloads its flight plans, a far more efficient process than paper-based systems. But once the contagion had spread to Villacoublay no flight plans could be downloaded. Until an alternative method of delivering the flight plans could be cobbled together, the Rafales were no more useful than scrap iron. The French press reported the embarrassment in detail.

Perhaps as consolation, the papers were careful to note that things could have been worse—and were, in Great Britain. There, the French press said, twenty-four Royal Air Force bases and three-quarters of the Royal Navy Fleet had succumbed to Conficker. The British and French navies may have been unintended victims of a worm designed for criminal ends. But after Conficker, no one can believe that an air gap is a security fail-safe.

Indeed, the Deputy Secretary of Defense has acknowledged that hackers successfully jumped the air gap to compromise DOD's classified networks. And it is hard to believe that the Iranian government did not keep its Natanz enrichment plan far from the Internet – a tactic that evidently did not prevent the Stuxnet malware from making the jump via thumb drive.

Myth 5: They're Not Looking for Me. The last of our illusions is that we're just not that interesting. Other people have more money. Other people have more valuable secrets. Who's going to come looking for me?

That's the last hope of every herd animal. The predators can't eat everyone. If you lie low and blend in, they won't pick you.

Wrong on two counts, I'm afraid. First, take this test. Add up your savings, car value, house equity, and investments. Is the total over $65,000? If so, you've got a lot of company on the

globe. Probably 10 percent of the world's 6.8 billion people have assets exceeding that amount—say 700 million in all. Being one in 700 million sounds like pretty good herd-animal odds until you realize that, for every person with more than $65,000, there are nine people with less. As computers become exponentially cheaper, most of those nine people will be able to get online. Then there will be nine people to see you as a rich outsider who deserves to be relieved of his assets. And another nine for your spouse, nine for your neighbor, and nine for each of your business partners. Maybe nine each for every person you know.

The world is already full of scam artists willing to work for less than minimum wage. Most of them know English and have access to the Internet. The relentless march of empowerment will soon give those scam artists new tools for finding and fleecing you.

They can send out ten million emails telling people that they've won the Spanish lottery. If one in ten thousand responds, even with great caution, that person has selected himself for fleecing, and the pitch can then be tailored precisely to his failings.

So what if that part of the scam is a bit labor intensive? There are as many as nine people with nothing better to do than sit around trying to get into the mark's head.

In fact, it's worse than that. Because Moore's Law is working for the outlaws too. The increasing speed of new computers means that outlaws can use the victim's own computer to decide whether he's interesting enough to rob.

Remember that real-time password-stealing program? Well, the thieves don't have to go looking for rich people to infect. Instead, they infect everyone, and let the malware find the rich ones. The password-stealing program consumes an infinitesimal part of a modern chip's processing power to run quietly in the background, watching and waiting until its victim logs on to one of about fifteen hundred predetermined financial sites. Anyone logging in to one of those sites, the authors figure, probably has enough money to be worth cleaning out.

So when an infected computer sets itself apart from the crowd by logging on to a financial site, the malware alerts its author, who can now focus on taking money from that computer's owner. Moore's Law has taken a lot of the work out of the hunt. And, thanks to the empowerment of information technology, it will keep making the job exponentially easier, year in and year out.

What Can We Do About Cybercrime?

In short, cybercrime is bad now, but it will be far worse in the future. The success of cybercriminals has already inspired more than a dozen governments to flirt with cyberweapons. And Stuxnet shows that some have moved beyond flirtation.

Stuxnet seems to have been highly targeted on the industrial control system for centrifuges in a single facility in Iran. But the tools it deployed could just as easily be used to bring down the power grid for a city or a region – and probably also to destroy the generating equipment on which the region depends, forcing city dwellers to live without power for weeks or months, if they can.

That kind of attack would change the nation. The leaders who failed to prevent the attack would be swept away, and massive changes would be made in our information networks to thwart future attacks.

Or perhaps we'll escape an international conflict. Even if we are that lucky, cybercrime will keep growing, for all the reasons I've already given. It is dead easy, and it pays remarkably well. We shouldn't wait for disaster if we can head it off.

The problem is that any change big enough to seriously address the problem is big enough to offend one or more well-represented lobby. With that in mind, and with some diffidence, let me sketch the kinds of changes that might change the direction in which we are traveling.

First, when you can't trust the devices on your network, which is increasingly true of all organizations, one successful defense seems to be back-office pattern recognition. The most obvious use of this technique is the system that credit card companies use to stop suspicious transactions; anyone who has used a credit card in an unusual context is familiar with the "just checking" calls that come from the card issuer. We need to create incentives for companies to deploy such systems more widely. Two examples: US home computers are badly infected and widely used for bot attacks and other crime. The ISPs that carry traffic from these infected machines can often identify the machines from their pattern of behavior. But the ISPs have no incentive, and much disincentive, to notify the owners, or to quarantine or restrict the machine's access to the internet. Similarly, small businesses that have been compromised with key loggers cannot protect their Electronic Funds Transfer accounts from hackers on their own. The banks that receive unusual EFT requests are in a much better position to spot a fraud in the making, but today liability for that fraud rests on the business owner, not the bank. Again, finding a way to encourage banks to use their central position in the payment stream to identify EFT fraud would likely make fraud less attractive.

Another way to reduce cybercrime is to reduce anonymity in cyberspace. Better attribution of machines and users on networks will make it easier to punish lawbreakers, and without punishment of those who break the law, all the defenses in the world are not likely to succeed.

There are no doubt other steps that could be taken, but at this point, the federal government doesn't even have authority to call on industry to take obviously needed security measures. The Defense Department lacks insight into the origins of critical supply-chain components. The federal government lacks authority to set high security standards for the industries on which our civilization depends. Congress has been considering bills to address these security gaps for many months; it's past time to enact one.

Finally, deep as this security hole is, we should at least stop digging. We should slow or stop initiatives that will increase our risk. The "smart grid" movement, for example, won't look so smart if it results in a whole new set of vulnerabilities for the populace as a whole; we need confidence in the entire security architecture before we deploy smart grid technology. By the same token, filling our telecommunications networks with unvetted equipment from vendors

beholden to the Chinese government makes little sense, yet the administration apparently felt compelled to approve foreign vendors as the beneficiaries of federal broadband stimulus funds.

I offer these ideas not because they will all work or they are all the best possible solution but to show the kinds of changes that we must be willing to consider if we want to bend our extraordinarily risky trajectory. But if you kept track of the industries, the foreign governments, and the civil liberties groups likely to be offended just by that short list of possible measures, you understand why we are still sliding down a slope that leads to serious trouble.

Thank you for your attention.