Remarks by the National Counterintelligence Executive
Dr. Joel F. Brenner

Applied Research Laboratories
University of Texas at Austin

Business Strategies in Cyber Security and Counterintelligence

April 3, 2009

AS PREPARED FOR DELIVERY

DR. JOEL F. BRENNER: Thanks so much for the opportunity to be with you this morning and join a conversation about business strategies and opportunities in an area of deep concern for our national security and our economy: the security of our electronic networks. These networks are the nervous system of virtually every economic, social, and governmental activity we engage in, and they're vulnerable to failure and in many cases are under constant attack.

I work for the Director of National Intelligence, Dennis Blair. His mission is to integrate the nation's intelligence activities; I do the same for our counterintelligence activities.

Counterintelligence identifies and deals with threats to the Untied States from the intelligence services of foreign states and similar organizations of non-state actors, such as al Qa'ida and the Lebanese Hizbollah. We have a defensive mission — protecting the nation's secrets and assets against foreign intelligence penetration — and an offensive mission — finding out what foreign intelligence organizations are up to in order to defeat their aims. To most people, counterintelligence just means counterespionage: rooting out spies. It is that, but it's much more. If you can penetrate a nation's – or a company's – information systems from the comfort of your office in Moscow or Beijing or Tehran, why run a spy? Remote information operations are cheaper and a lot less risky. So in a networked world, counterintelligence has a technical mission too. Understanding who's trying to penetrate us electronically and what they want, and driving higher levels of network security – these are a large part of what we do.

The Threat

I'm going to start by describing the threat to those networks, because in threat lies opportunity – and because we won't get far toward understanding that opportunity unless we understand the problems we face. The government, acting alone, cannot possibly change the threat environment we now live in, or reduce our vulnerabilities.

I say this for several reasons. First, the threat and the vulnerabilities exist in the private as well as the public sector. Second, so much public business nowadays is intertwined with private

firms through contractual arrangements. And third, most of the infrastructure on which the government communicates is privately owned. When a field officer sends a cable to Langley, that cable travels over the same telecommunications network that you and I use – or that al Qaeda uses.

Counterintelligence used to be challenge for the FBI, CIA, and the military. Now it's a challenge for every private firm that lives on a network – which means all of them. Here are a few examples – all real – of threats you face:

- A leading US firm enters negotiations with the Chinese, only to realize midway through that the Chinese know every one of their bottom line positions as a result of having hacked their network.

- A US computer security expert gets off a plane in Beijing with a new PDA, turns it on, and by the time he gets to his hotel, finds a handful of beacons remotely inserted. Some are designed to track his movements, others to infect and investigate his home server when he emails home.

- A US computer security firm wanting to do business in China hires a group of Chinese. To do what? Research security vulnerabilities. Do they vet them? Apparently not. They include at least one hacker with ties to the PRC government.

- A PRC intelligence officer approaches an ethnic Chinese, US citizen who is highly placed in the CIO organization of a US firm. They want him to spy on his own company. He turns them down. Later he's approached again — this time to say that his mother in China needs hospitalization, but the hospitals are, you know, crowded. Does he want to reconsider?

- Data loss stories now too numerous to keep up with—often relegated to inside pages of newspapers.

- Criminal scams getting much more sophisticated. There's now a well-developed black market for stolen information. The Russians are into this big-time.

- We're also seeing counterfeit routers and chips, and some of those chips have made their way into US military fighter aircraft.

I've just changed the subject. Did you notice? All my examples until the last one related to data theft. But you don't sneak counterfeit chips into another nation's aircraft to steal data. When it's done intentionally, it's done to degrade systems, or to have the ability to do so at a time of one's choosing. There is no longer a meaningful difference between data security and operational security. Our operations depend on our networks – the same networks on which we create, move, and store data.

The simplest form of system degradation is a distributed denial of service attack. We saw that in attacks coming from Russia on Estonia. We know how to deal with these, and they're temporary

in any case. Chinese penetrations of unclassified DoD networks have also been widely reported. Those are more sophisticated, though hardly state of the art. Frankly, I worry more about attacks we can't even see, which the Russians are good at. The Chinese are relentless and don't seem to care about getting caught. And we have seen Chinese network operations inside certain of our electricity grids. Do I worry about those grids, and about air traffic control systems, water supply systems, and so on? You bet I do. Our networks are being mapped. We have also seen both Chinese and criminal network operations in the networks of some of our banks. Do we worry that the Chinese government wants to bring down our banking system? No. They have too much money invested here. Our electricity grid? No – not now. But if there were a dust-up over Taiwan, these answers might be different. Meanwhile, criminals in our banking networks are giving new meaning to the notion of "grand theft."

On every level we face an anarchic e-culture.

Government Cyber Responses

I said earlier that government alone can't deal with this problem set, but government can – and at last is – taking the lead. This is one point on which the Bush and Obama administrations are in broad agreement, and the new administration has taken the essential step of moving cyber governance into the White House, where Melissa Hathaway is finishing a 60-day review of the cyber issue. Here are some of the basic points of what's underway:

- We will go on the offense by taking steps to detect and prevent intrusions as they happen and before they can cause significant damage.
- We are integrating defensive cyber capabilities, optimizing and coordinating cyber activities, and improving performance of cyber resources.
- We are integrating offensive and defensive cyber capabilities with law enforcement.
- We are synchronizing disparate funding sources into a coherent integrated portfolio.
- Our initial focus has been the threat to federal government systems, but we are committed to a dialog with the private sector to strengthen awareness of the threat and find solutions to protect the nation. Which is why I'm here.

Meanwhile, the problem in the private sector is growing. It remains to be seen, for example, how much longer banks and credit card issuers can continue to absorb rapidly mounting losses from electronically enabled fraud, which they measure as basis points off return on investment. But the banks are between a rock and a hard place. The last thing commercial banks want is to shake consumer confidence in electronic banking. Just imagine a sudden return to teller lines and paper transactions and you can understand their dilemma.

Corporate America's Reaction

So what's the reaction in the rest of corporate America to the problem of network risk? It's all over the lot — form real concern to cheerfully oblivious. There are at least two reasons for this. First, in some industries there's a deep fear of liability that could arise from having problems you can't fix – in particular, shareholder liability under Sarbanes-Oxley 404. Some firms deal with this at the corporate level by preferring not to know things. Others deal with it by outsourcing as

much of their network operations as they can. This doesn't necessarily make them safer, but it does off-load potential liability.

Second, it's very difficult to monetize cyber risk. The problem isn't so bad on the privacy side, which so far is the aspect of cyber security that has received the most attention. Knowing the cost of leaking privacy data isn't difficult: You just add up the fines and the litigation costs, which are rising. The débâcle at TJMax cost that company millions.

Much harder is calculating the costs that a firm would incur if its networks were shut down. So far as I know, there are no Generally Accepted Accounting Practices that apply here. And worse than a sudden shut-down might be the slow but systematic degradation of a firm's data. Better to know your network is down than to keep using it after it becomes untrustworthy. A fighter pilot who can't trust his radar and a banker who can't trust his accounts both have the same problem. But how serious is this risk in the first place? And if you can't reliably tell your CEO what it will cost if it does happen, it's very difficult to drive investment. He knows the return on investment of capital currently deployed. When you tell him he should deploy some millions of that capital on cyber security, but can't tell him the ROI on the alternative use of capital, you're not going to drive investment.

So What's the Business Strategy?

Assuming you think I'm more or less right in my description of the problem, where does that leave an entrepreneur who's evaluating opportunities in creating or growing a business in network security? Let me address the question in two ways.

First, let's talk about who's investing in this kind of security and who's not. I don't have empirical data on this, but all my sources tell me that very few firms are putting money against this risk. This is partly for reasons I've discussed, and partly because we're in the worst economic circumstances I've seen in my lifetime. At the same time, the federal government is gearing up to put lots of money against this risk. To me, this means that a new firm that hopes to survive in this business in the near term would do well to think in terms of a business strategy with a heavy federal component. The picture may well change by 2010, but in the meantime, targeting the private sector alone would strike me as extremely risky.

Second, it's important to understand the degree to which the security issues are – and are not – technological. The trade space, especially around Washington, is already crowded, and every company in it wants you to think it has some sort of special sauce that sets it apart from the herd. As a marketing proposition, this makes sense, and in fact there are some superior tools out there. But we shouldn't kid ourselves that security is going to come to us through a new black box, though good tools are important.

Good security solutions require us to distinguish among technological problems, management problems, and behavioral problems. Failure to adopt available technologies is not a technological problem. It's a management problem. And the systematic subversion of reasonable managerial rules by a workforce (including managers) unwilling to permit security concerns to interfere with their convenience is a behavior problem. Of the three kinds of

problem, behavior is by far the worst, management second, and technology a distant third. Segmenting the problem this way is essential to clear thinking for both buyers and sellers in this market.

I like to segment the problem further by distinguishing what a company (and prospective client) can do alone to increase its security, from what the private sector can do collectively, from what you can't do anything about and must learn to live with. Here are some examples:

What a company can do alone: Automate patching, require serious workforce training like Apple insists on, implement safer server architecture, manage corporately your external connections and unauthorized hardware and software, manage corporately international travel behavior and comms equipment, and get visible C-suite support for the corporate CISO.

I think it is also important that the CISO does not report to top management through the CIO. Intelligent people differ on this. So here's my reasoning. Asking the person responsible for system performance, including security (that's the CIO), to report candidly on that system's insecurity is asking too much of ordinary mortals. The CISO, in contrast, represents the corporate counterintelligence function. It's his or her business to tell you what's wrong. These two officers should get along, but in a pinch, the CISO should be able to go straight to the top.

What private sector can do collectively: Support the corporate exchange of threat information, get louder in asking for government sharing of threat information, support a collective approach to security that may include in some cases VPNs or similar exclusive comms channels.

What you cannot affect: The post-privacy culture of your workforce, and a technology environment that, for now at least, favors offense over defense.

There is no single solution and no perfect solution to network security, data security, or operations security. To be commercially successful in this area, I'd want to be selling technology and services that emphasize the same three things we emphasize in the Intelligence Community:

- Defense in depth, or layered defenses;
- An approach that builds security into personnel practices as well as technical systems — not one that tries to bolt it on later; and
- An approach that seeks to lower an attackers' ROI.

This market is going to grow. How much it will grow in the next 12 months is another question. As you don't need me to tell you, times are tough.

That's enough from me. I'd like to know how things look from your vantage point. So let's start a conversation.