Prepared Remarks of U.S. Attorney Preet Bharara
Citizens Crime Commission
The Cyber Threat: Are Government and Industry 'Outgunned'?
April 16, 2012

Thank you for that kind introduction. I'd like to recognize the Citizens Crime Commission and especially its President, Richard Aborn, for all the great work that you do on so many important issues facing law enforcement today.

Any good prosecutor's office has to be on top of emerging threats, and we have so many to worry about these days.

There is the developing threat of domestic lone wolf terrorists.

There is the movement of violent gangs away from the streets of major cities into smaller, more rural communities where single gangs can monopolize entire police departments and terrorize entire towns.

There is the developing threat of synthetic dope, which as we speak, is sending young people to the hospital and, tragically, sometimes to the morgue.

These all merit discussion and attention. But today I want to focus on one of the great emerging threats to our safety, our markets, and our economy.

It is the cyber threat.

Cyber crime is ubiquitous and costly, and it threatens the security of everything from our individual bank accounts to our financial markets; from our personal privacy to our public infrastructure; from our corporate secrets to our national security.

This very group has recognized this more than most. Three months ago the Citizens Crime Commission and NYU hosted a panel of law enforcement, industry experts, and policy makers who discussed the unique challenges and dangers that cyber crime presents. Among others, panelists included a United States Senator; the Associate General Counsel of a major company; and the FBI's Cyber Special Agent in Charge, Mary Galligan, who is here.

As discussed during the panel, the cost of cyber crime has reached billions of dollars per year and law enforcement is doing its best to keep up, devoting more and more manpower and resources to addressing the threat.

On average a single data breach costs American businesses $6.6 million. And every hour, the FBI processes 35 cases through the Internet Crime Complaint Center.

So it is true that the cyber threat is on people's minds and on governments' agendas in a way that is more serious and sustained than ever before. And that is a good thing.

But we should all be worried every day that we are still doing too little; that we are not responding aggressively enough; that we are not working hard enough; that we are not thinking creatively enough; that we are not sharing information or best practices enough; that we are not educating the public enough.

To be sure, the papers seem to be filled these days with startling articles about the multifarious threats to economic and national security posed by hackers and computer criminals and even nation states.

There is, to be sure, a daily drumbeat of stories, warnings, and alarm bells—which scream the urgency of a threat that is mostly invisible, fairly incomprehensible, and largely intangible to the general public. But, as you know, it is an intangible threat that can cause—and has caused—calamitous and concrete harm. Although it once may have been, it is no longer a hypothetical hazard.

But notwithstanding that drumbeat, leaders in the United States and elsewhere find themselves using more and more dramatic language to impress upon the public and policy-makers alike the truly astonishing magnitude of the cyber threat.

Defense Secretary Leon Panetta uttered one of the most attention-grabbing formulations in recent times when he suggested that a cyberattack on our markets and infrastructure could be "the next Pearl Harbor."

Director Panetta is a man who tends to know what he's talking about—as a longtime member of Congress, former Budget Director, White House Chief of Staff, CIA Director, and now Defense Secretary.

The now-departed Chairman of the Joint Chiefs of Staff, Admiral Mike Mullen, has issued an even more eye-popping assessment. In a speech last fall, Admiral Mullen said that he believes there are but two existential threats to the United States. Existential threats—meaning two threats to our very existence.

One is the stockpile of nuclear weapons that still exist in Russia. The other is the threat of cyber attacks, which he said could "actually bring us to our knees."

And Admiral Mullen actually thinks that while the nuclear threat is under control, the cyber threat is not. That is a deeply unsettling thing to hear from the top military officer in the United States.

When people as serious and sober as Admiral Mullen and Secretary Panetta speak about the cyber threat and make comparisons to Pearl Harbor and nuclear annihilation, people need to not only pay attention, but take action. Urgent action.

While the threat to the United States is unmistakable, in the current climate—no country is immune; no corporation is safe; and no individual is fully secure. And the responsible parties in every country—policy-makers and prosecutors both—have to understand that an existential threat to one nation is an existential threat to every nation.

To make matters worse, some experts are exceedingly pessimistic about whether we even have the ability to meet the threat.

Just two weeks ago, the Wall Street Journal published an article entitled "U.S. Outgunned in Hacker War." The article quotes Shawn Henry, the FBI's departing Executive Assistant Director and the top official on cyber crime, in addressing our efforts to stave off infiltrations of corporate data networks, saying simply that "We are not winning" and our current approach to the problem is "unsustainable."

Part of the problem is that the threat is not singular, but multi-faceted:

- There are the so-called hacktivists who target computer networks for penetration, data theft, and data destruction. Stratfor, HBGary, Sony, Fox and other companies have all been the victims of hacktivist attacks. Hacktivists often claim to be motivated by perceived social causes, but many are nihilistic and randomly destructive. We recently charged a number of them.

- There are company insiders, generally disgruntled current and former employees who infect systems with damaging malware (*e.g.*, "logic bombs") or who steal valuable data.

- There are hackers motivated by financial gain. This type of hacker generally seeks to break into company systems and steal valuable data, such as bank account information, which can be monetized. Financially motivated hackers may also seek to extort victim companies by threatening to disrupt their computer networks or publish embarrassing details about vulnerabilities in victims' computer systems. We recently charged a number of these, too.

- And then there are nation state actors. This type of hacker often uses the most sophisticated techniques to compromise computer systems over long periods of time with the object of slowly and covertly stealing data, including trade secret information.

Hacktivists often seek maximum publicity for their illegal activity—including disclosure of confidential personal information about company executives—with the object of embarrassing their victims, individually.

And so while many leaders rightly focus on the existential threat posed by bad actors in cyberspace, the fact is that individual corporate officers are also a target. As detailed in a Booz Allen report from 11/29/11, there is a specific and escalating threat to the executive suite at financial institutions.

And here is something that every business person in America should find disturbing. While it may sometimes be comforting for smaller entities to think that only big institutions are at risk, nothing could be further from the truth.

A former hacker makes a chilling point in the Wall Street Journal on July 21, 2011, making clear no one is immune. He said, "Even a pizza place has addresses, names, and credit-card information." Indeed, common sense tells you that smaller businesses are less likely to have the proper firewalls and controls in place.

Even worse, small business may suffer from a false sense of security and complacency—as that same Wall Street Journal article reported, a 2010 survey showed that 64 percent of small and medium-size retailers believed their businesses weren't vulnerable.

Anyone who thinks that is fooling himself. And that foolhardiness puts millions of people at risk.

So we are making concerted efforts at every level.

Law enforcement is getting better and better at looking behind the screen—by combining the power of the latest technology, often the same technology being used by cyber criminals themselves, and the strength of the most aggressive, traditional law enforcement techniques. The world's nations are forging new partnerships and relying on existing ones to coordinate efforts against a common enemy.

As one of our recent cases shows, even hackers now have to worry about whether other hackers are true cohorts or cooperating witnesses.

We are also coordinating better than ever before. I participated in a meeting convened at the NASDAQ by Secretary Napolitano last October. Everyone was there—Eastern District of New York U.S. Attorney Loretta Lynch was there; Shawn Henry was there; Jan Fedarcyk of the FBI was there; Brian Parr of the Secret Service was there; the Manhattan DA, Cy Vance, was there; representatives from financial institutions and stock exchanges were there—and we talked productively about how we can all work better together and that conversation and cooperation continues.

I want to commend the work of the FBI, the Secret Service, and District Attorney Cy Vance for doing such great work in this area. DA Vance has been wise and visionary enough to make cybercrime an important priority and he should be congratulated for that. Not every district attorney has such foresight.

Every agency is responding, including my office. We have added resources to the effort; we have made cyber crime a top priority; and we have for the first time created a position called Deputy Chief of Cyber, held by Assistant U.S. Attorney Tom Brown. There are others in my office, including Lisa Zornberg and Michael Bosworth, Chiefs of the Complex Frauds Unit, Yusill Scribner, and Ellen Davis, who are here today, all aiding in this effort.

And later this month, we will be conducting mandatory training for the entire criminal division of my office on the latest trends, technology, and law relating to cyber crime and electronic investigative techniques because it is so important.

But still we need to ask, are we doing enough? Because unlike any threat we have ever seen, the cyber threat seems to proliferate and metastasize faster than any opposing force can properly mobilize.

And because it is not nearly enough for one nation's law enforcement agencies and intelligence apparatus and academic thinkers to confront the cyber threat—no matter how aggressively and intelligently we do so.

Industry too must do its part. Industry must play a central role. Industry has to step up with industrial-strength solutions.

Now, let me talk about the essential role of private industry for a moment.

As I said before, cyber crime cases require collaboration, not only among law enforcement agencies, but also between the government and industry. Victim companies are on the front lines of this battle, and are often the first to realize that a cyber attack has taken place. Unless we

know about the problem, we cannot help. That is why our private sector partnerships are so important.

Three things I want to say we need from industry, that we all should encourage from industry:

1. A culture of disclosure;
2. A culture of security; and
3. Focused and high-level leadership from the top

First, we need a culture of prompt disclosure of breaches and hacks. Delays in disclosure make it harder—much harder—to capture the bad guys.

Now, I understand there is trepidation. I understand that there can be hesitation on the part of a hacked company whose immediate concerns are focused on employees and shareholders and customers and clients. It is for some industry types not natural to partner up with agents from the FBI or to talk to federal prosecutors.

I understand that that there has traditionally been a divide between businesses wishing to maintain the security of their networks and law enforcement investigations. Businesses may feel that they lose control of the process, and that confidential business information could be exposed. Companies might even think that reporting a breach may harm their competitive advantage.

But I have a three-word message for anyone in private industry who – in this day and age with the gathering cyber threat being what it is – insists on maintaining an outdated and outmoded short-term mentality that is the equivalent of sticking one's head in the sand: "Get over it."

When industry delays in disclosing to us, it is harder to tell who the next victim might be and it becomes harder to prevent further harm.

When industry delays or minimizes, it is harder to assess vulnerabilities and harder to formulate solutions.

When industry delays in disclosing to us or minimizes, it is harder to get the bad guy.

And when we don't get the bad guy, other victims are injured and justice is not done.

And given what we understand about the overall cyber threat, that is no longer tenable or acceptable.

A bank would never think to delay in reporting a conventional bank robbery involving a mask a note and a gun. But that is what institutions routinely do now. They wait wait, and such delay can be disastrous.

Now the good news is this—businesses should know that we will do everything that we can to minimize disruptions to their operations, and to safeguard confidential data.

Where necessary, we will seek protective orders—orders signed by a federal judge that help to preserve trade secrets and business confidentiality. And we will share with victim companies what we can, as fast as we can, about a particular attack.

It takes dialogue and trust and discussion—discussions that I and the people in my office are happy to have to assuage any concerns.

At the end of the day, we can and must help each other, by maintaining clear lines of communication between law enforcement and the businesses that are affected by cyber crime.

Second, every company should be creating and fostering a culture of security.

There is a recent and stunning report from Verizon. It says, 97% of data breaches in 2011 were completely avoidable. It goes on to point out that 79% of attacks involved targets of opportunity. The report reads, "The findings suggest that while companies are spending increasing sums of money on sophisticated new security controls, they are also continuing to overlook fundamental security precautions."

We have this false image of most hackers as hyper-sophisticated. Many are, but most companies that are the victim of cyber crime aren't hacked by Tom Cruise rappelling down a building in a highly sophisticated intrusion. Most often, companies are breached by hackers essentially walking down corridors, looking for unlocked doors.

And when it comes to computer hacking, one unlocked door can mean entry into the entire data network, introducing a criminal element to the whole company.

Companies don't need to learn the hard way the importance of locking their doors. If they are not aware and they are not prepared, companies can go from having a great reputation and all the value associated with it, to having that reputation trashed completely overnight.

It's only common sense that any hacker or someone that wants to do harm through a computer system is going to choose the most vulnerable and easy-to-target company. The protection

against that is to make sure that you are doing everything possible to keep the doors always locked.

Third, we need leadership from the top.

As the FBI's Shawn Henry also recently suggested, companies need to get their entire leadership, from the chief executive to the general counsel to the chief financial officer, involved in developing a cybersecurity strategy. "If leadership doesn't say, 'This is important, let's sit down and come up with a plan right now in our organization; let's have a strategy,' then it's never going to happen," he said.

And as FBI Director Robert Mueller recently put it, "There are only two types of companies. Those that have been hacked and those that will be."

Waiting to react to an intrusion is no longer a viable option. Businesses must preemptively protect against hacks and be prepared with a plan for the worst case scenario. Because the operative question is quickly becoming "when," not "if."

And yet, how many companies have a concrete plan in place to deal with a hack?

How many have Chief Technology Officers?

How many companies have their boards engaged on these issues?

I gave a talk last week to a group of people that included business people and general counsels of major corporations. And I made the point that every company needed to have a high-level plan in place to deal with a potential hack, breach, or intrusion. You might be surprised to learn that two officials from significant companies said that they did not even know whom to contact in law enforcement to discuss the issue. That is not tenable in the current climate.

Let me tell you another anecdote. A few weeks ago, I spoke to members of various boards at the New York Stock Exchange. And I was asked the question: how are boards of directors supposed to deal with cyber issues when they can be technical and unfamiliar. I said that this was a very outdated way of thinking and that, as in every area in which directors may not have expertise, they nonetheless needed to get deeply involved in this issue because a chief responsibility of every board is to protect the institution against material risk. And, as I've described, the cyber threat is a most material menace.

Management and the Board need to be involved and asking questions. In the modern era, it is simply no longer enough to leave cyber security matters to the "geeks," to leave them to the "techies."

Companies can choose to do that, I suppose. But if they do, I can guarantee that they will be left behind.

They will be hacked.

And they will be sorry.

Cyber crime is, without question, one of the gravest of threats faced by this country, the most wired nation on earth. No one country, no one agency, no one company can alone stop cyber attacks. It is only together that we can minimize this law enforcement and national security challenge. Working together, we can and will continue to expand on the success we have had prosecuting cyber criminals.

Given what is at stake for our economy and our security, we have no choice.

And so the question again presents itself: Are we "outgunned?" Perhaps.

But in my view it is less a matter of being outgunned than being simply outdated—outdated in our thinking and outmoded in our vision. There is still too much apathy and ambivalence; too much misunderstanding and misinformation; too much self-delusion and too little self-awareness about our vulnerabilities in cyberspace.

But we all have to wake up to the threat all around us.

We need focused commitment from literally everyone who touches, and is touched by, the Internet—whether one serves in law enforcement or on Capitol Hill, works in corporate America or on a college campus.

Why? Because there is an army of computer saboteurs and spies and thieves and nihilists out there who wish to do us harm—who wish to upend our markets, drain our accounts, steal our secrets, halt our economic progress, and destroy our infrastructure.

But we have an army too. Or at least the makings of one.

And so, I ask, how can we tolerate even for a moment the suggestion that we are "outgunned" when the army that *we* can assemble to counter this gathering threat is so very vast—when the

army that we can assemble comprises the best law enforcement agencies in the world; the best intelligence agencies in the world; the smartest businesspeople in the world; the brightest thinkers and academics in the world—and all of them privileged to be operating in the most open and free society the world has ever seen.

Without any doubt, we have the wherewithal to withstand any cyber threat, no matter how large and how frightening.

The question is: Do we have the will?

Now, I have no doubt that we'll find the will once a true catastrophe strikes—just as we did after the Japanese bombed Pearl Harbor and after al Qaeda leveled the twin towers.

The question is whether we can find the collective will *before* that happens.

I hope we do.

Thank you.