UNITED STATES DEPARTMENT OF JUSTICE

KEYNOTE ADDRESS OF THE HONORABLE JANET RENO

ATTORNEY GENERAL OF THE UNITED STATES

AT

THE ITAA CYBERCRIME SUMMIT:

A LAW ENFORCEMENT/IT INDUSTRY DIALOGUE ON

PREVENTION, DETECTION, INVESTIGATION AND COOPERATION

EDS Building

13600 EDS Drive

Auditorium

Herndon, Virginia

Monday, June 19, 2000

P R O C E E D I N G S

ATTORNEY GENERAL RENO: Thank you, Harris Miller, for all that you have done, both in promoting educational opportunities for our young in this area and bringing law enforcement and industry together. And thanks to you, Mr. Brown, and Mr. Dvoranchik, for your hospitality. I think that this is so important that we hold this conference in Northern Virginia where so much innovation is taking place.

I come today to ask you a question. And I look forward to receiving your answers later this afternoon. What can the Department of Justice, what can I as Attorney General do, to build trust and confidence between law enforcement and industry so that we can work together as partners in responding to the growing challenges of cyber crime?

What can we do to meet our obligations to ensure the public safety, to enforce the law, in a manner that fosters and promotes privacy and the civil liberties of all concerned, allows the Internet to flourish with all the innovation that you can muster, and at the same time causes the victim as little inconvenience as possible?

The Department of Justice does not seek in basic government regulation or monitoring of the Internet. We would rather work together as partners with separate but overlapping areas of responsibility and accountability.

The private sector in that regard should take the lead in protecting the security of private sector computer systems. And we should protect government systems. We must share, however, the information about vulnerabilities so that we can each take steps to protect our systems against attack.

We have a common goal to keep the nation's computer networks secure, safe and reliable for America's citizens and its businesses. We have a very important moment. We can become strong partners. We can enforce this common goal. We can maintain the Internet for the extraordinary tool that it is for learning, communication, commerce and so many other aspects of our lives.

Or we can go our separate ways. We can watch the Internet subject to attack in the different forms that we have seen it. And I'm sure that some creative genius has some other idea out there that we haven't even considered yet. And we will not have this tool that think just has opened up the economy, opened up learning, opened up opportunities that we never dreamed of.

From my discussions with industry representatives and my

colleagues in government and law enforcement, I know we are in agreement that we must do this in a way that respects the constitutional rights, the privacy and other rights of all Americans and that focuses on the innovation that is occurring in industry so that we do not stifle it in any way. We must do it in a way that is least disruptive. And in this instance, I think we have much to learn from traditional criminal justice activities.

While law enforcement alone can't solve the cyber problem, any effective strategy must involve us all. For example, let's look at what happens in the non online world.

When someone's home is burglarized, it is important that the victim notify law enforcement as quickly as possible. If they don't, if the crime scene is messed up, if fingerprints are intertwined, if clues and pieces of evidence are vacuumed up, the police are going to have a very difficult time in solving your burglary. A prompt response from law enforcement can minimize the loss of critical evidence and provide clues while the trail is still warm.

In addition, if similar burglaries have occurred in other areas, law enforcement may be able to link the burglaries to a single person or a crime ring. And law enforcement may be able to work with community crime fighting groups to boost patrols and empower individuals with the knowledge they need to protect their own security.

This example also proves, however, that law enforcement alone is not the solution. Rather, it's law enforcement, the victim, community groups and individuals working together to provide the most effective strategy for preventing such crimes.

The parallels in the cyber world are obvious. If we don't get it reported right away, we're not going to be able to trace it as easily. With prompt reporting of cyber crimes to law enforcement, cyber criminals can be caught and brought to justice. Prompt reporting can help us to identify and correct vulnerabilities.

As in the off line world, the most promising approach lies in a cooperative effort between law enforcement and the community. We'd far prefer for you to prevent it, and we'd not like to tell you how to prevent it. We'd not like to tie your sense of innovation up in regulation that we impose on you. But we would like to share with you vulnerabilities that we observe so that you can take steps to prevent it. And we would like for you to let us know what problems you see so that we can be more effective in the law enforcement effort.

Today I call on leaders in the high tech industry to address this problem, to take concrete steps to encourage others to report cyber incidents to law enforcement authorities. And we at the same time pledge to do our part to make such cooperation easier and to minimize the impact our investigations have on victims.

But what you will say is, hmm. Have you looked at how the federal government talks? If we give you this information, confidentiality which is so important to us will be ignored. And we will find sensitive information out on the street where we don't need it. Or we will be embarrassed because our lack of security, our lack of prevention, will be made known to the world.

These are issues that we need to address in a candid, frank way to understand just what is involved. The same is true in the non online world. The banker doesn't want to report his embezzlement because he's embarrassed. The banker doesn't want to report the details because it will lead to confidential information that is important to the bank being out in the public. How can we work together to ensure confidentiality?

The next point that you will raise is don't you know how inconvenient and burdensome the criminal justice system is and an investigation is? You're going to have all my employees down before the grand jury. You're going to have them tied up in interviews after interviews. Ah, forget it. I'll protect myself. I don't need you.

Then comes the denial of service attack or other similar situations. And you say, oh, wait a minute. Maybe we do need them. Let's start now to minimize the problems that victims perceive in the criminal justice system.

Then there will be a, okay. You've assured me of confidentiality. But I don't know what's happening. Nobody ever lets me know what's going on and what the next step is. Let us sit down together and help each other understand the two worlds, the worlds of cyber technology and the world of the criminal justice system. Let us try to be candid with you in what we can and can't do.

Then, okay. We got all that done. But after that effort, they just get a tap on the wrist. Nothing happens to them. Let us work together to focus on sentencing guidelines so we get sentences that mean what they say and serve as a deterrent. Let us figure out what we do for that 15 year old hacker that makes sure that he knows never ever to do it again.

But then I hear, look. You're a nice lady. I think your heart's in the right place. But you don't understand. Law enforcement doesn't begin to have the equipment to match wits with the bad guys. And until you get the technology, it's just not going to work and you're not going to be successful. We need you to join with us in letting the world know what is needed in law enforcement to properly protect law enforcement interests that coincide with industry interest.

Harris has alluded to one of its next problems. You say you've got these great people working for you. And as soon as we form a relationship with one, he goes off to the private sector. Then the next one goes off to the private sector. And they're not there long enough ever to establish any contact.

Well, we're trying to develop concepts such as cyber ROTC where we can attract people to government for a longer period of time in return for a system such as ROTC produced. But we have a long way to go. And that goes to

educating our young people. How can we look at all of America, not just some of America, and identify -- and Harris, I'm really intrigued with this -- how can we identify young people of 10, 11 and 12 years old who are not do well in school, who are not supervised at home, who do not have motivational or inspirational parents at home, how can we reach out and identify them through aptitude testing that gives us resources that we never thought we had in the United States so that we are not as dependent on the world?

And finally, you will say, but even if we work all this out, we're going to have to extradite somebody. And you'll say, well, we can't extradite because it's a national from another country or because it's too expensive? We need industry to join with us in letting the world know that there is no safe place to hide. And that although borders are meaningless with respect to cyber crime, we have got to effect alliances around the world that will ensure that there are no rogue nations, no rogue jurisdictions, that permit cyber attack around the world.

We've got our work cut out for us. But so do all who have contact with the criminal justice system. There are those that take the challenge -- and I think we should -- for there are those who have used otherwise magnificent tools to really inflict harm on others.

Let us make sure that the Internet is not part of this history. Even in the Internet's relatively short existence, we have seen a dizzying array of the criminal use of the technology. They are not trivial crimes. We have investigated computer attacks on our nation's information infrastructure, including serious breaches in the Department of Defense and NASA in numerous instances in which cyber criminals have stolen credit cards from consumers and posted them on the Internet, not only harms these individuals, but undermines the confidence of the public in the Net.

We must not forget that the Net is being used with increasing frequency to commit traditional crimes, including global distribution of child pornography, fraud

schemes, cyber stalking and the like. We have this unprecedented moment.

We have to make sure that we join together now while people are learning about the Net, while they're learning about what can be done and not done on the Net, to know and let them know that there is going to be enforcement. It's an unusual time in history where we can shape the whole public attitude and acceptance of what's right and what's not right.

Just think about it for a moment. It's rare in history that a collection of people, both in law enforcement and in industry, have a chance to say this is the wrong thing to do. This is the right thing to do. These are the sanctions that you face if you do it. We're going to have to be together in that effort.

We have made gains. The Internet fraud Complaints Center provides a centralized repository for filing complaints of Internet fraud. Since it's opening on May the 8th, the center has received an average of approximately 1,200 complaints per week. Through the Center, the FBI and the National White Collar Crime Center, collect, analyze, evaluate and disseminate Internet fraud complaints to the appropriate law enforcement and regulatory agencies.

But that's not going to work if we continue to build complaints, generate backlogs, those backlogs don't get addressed, people don't think anything's going to happen to them, industry loses confidence in law enforcement and it goes from bad to worse.

Yes, we've made some progress, but we've got a long way to go. Senior officials from the Department's Computer Crime Section meet regularly with representatives from Internet providers, telecommunication carriers and others through industry information groups. FBI's National Infrastructure Protection Center and its computer crime squads have worked together to develop the intraguard program in communities around the country.

I think these efforts are critically important, but we've got more to do. We've gathered here today people who I think can address the issue. Each of us has a role to play.

I urge you to talk frankly and openly. Don't be afraid that you will hurt my feelings or make me mad. I won't get mad and I won't get my feelings hurt except if I don't come out of here with some really specific suggestions about what we can do to be more effective.

Law enforcement like industry has its duties, its tools and its constraints. I want your opinions, your suggestions about what we can do to work in harmony with principles of our constitution and impose the least disruption on your undertakings.

I want you to know that I am not interested in searching people's computers except that we do it the right way. I need your advice in what we do if France is investigating somebody, a French businessman. He's never been out of France. He's got all his records stored in his computer. France gets our equivalent of a search warrant and discovers that he's a customer of America On Line and the records are right over here or over here.

How are we going to deal with those issues? How are we going to deal with the issues of cross state searches? There is so much to be done?

Finally, if you're not interested in working together in just common business good sense because you don't think we can do the job, there is something more important than anything else. It is this nation and all that we hold dear, because of your brilliance, because of your sense of innovation, we are very dependent on cyber technology. We have not kept up with cyber security.

So much of this nation's critical infrastructure, defense, banking, power, emergency services, finance, so much of it is dependent on what you have created. Being dependent, it is also at risk of cyber terrorism.

Let us not wait until we get to the crisis of cyber terrorism before we have learned to work together to solve our problems with lesser crimes. And then, God forbid, that they should come, we will be prepared again and again to prevent whenever possible and to pursue when it has occurred so that these people are brought to justice with a sentence that will serve as a deterrent?

I will be back this afternoon with pen and paper in hand and looking forward to your report. And I am deeply grateful to you all for taking the time today to be with us. It is very important to the Justice Department and to law enforcement.

MR. MILLER: We now have an opportunity for a couple of questions before the Attorney General needs to leave. If you have something written, did people get cards? You should have gotten cards? Oh, in your little packet, you have cards. Actually, if you just want to put your hand up and ask a question. As long as it's on the topic, that will be okay. Nobody has any questions? They've stunned you into silence? We should have planted one in the audience. There's one over there. Yes, sir.

QUESTION: How many (inaudible) or agencies have implemented a complete intrusion detection system, have policies and best practice.

MR. MILLER: The question is how many organizations attending have attending have implemented intrusion, detection and have good solid policies and practices in place?

QUESTION: (inaudible)

MR. MILLER: The first question was kind of a survey of the group. Maybe we'll do that later today. But I think the second question, maybe Dick or the Attorney General wanted to comment. Where if some company or organization were looking for some best practices now, where might they find them? Where would those be available to help a company implement those practices?

MR. BROWN: Well, I don't have a lot of survey data on your question, but I know one company that has. And it works. But, you know, if you look at, for example, EDS, we go through protection and training and operating systems and recovering. A lot of companies don't even know they've been attacked or are state and federal government agencies. They don't know when an attack has occurred and what the residual effect is. So you can work with companies in the IT industries. But then forums, I think, like I referenced in my remarks and have been referenced elsewhere are a gathering point for best practices that we share very freely across the industries of communications and IT and other industries.

ATTORNEY GENERAL RENO: I think if there is not a central place, in many instances law enforcement will go out and do it. We have been careful in this regard because we don't want to be perceived as putting regulations. And we would like to pursue the law enforcement and enforcement side of it. But, Harris, this may be -- you may know better than I do. But if there is not a central place where people can go, perhaps we should be about designing that.

And the other issue that has been raised on a number of occasions, those in the security field know what needs to be done. But sometimes their CEOs need to be advised of what needs to be done and the importance of the effort stressed. We would look forward to working with you in any way that you thought appropriate to address the creation of some central system for understanding the best way to go about it and whatever we can do with CEOs.

MR. MILLER: The ITA has been working with the federal government. We had a meeting last month hosted by the federal CIO council, particularly John Gilligan, who is the Chief Information Officer of the Department of Energy, to talk about best practices. And we brought together industry people as well as senior officials from the government agencies to begin that dialogue, General Reno.

So I think we're going to see that begin to evolve. And the assumption is -- it may turn out to be an incorrect

assumption -- is as the federal government develops best practices, those in turn will devolve down to state and local governments and may also migrate into private industry. Obviously, various companies that are specialist information security have their own proprietary methodologies. But whether those are generic enough, we don't know yet.

MR. BROWN: Harris, if I could just also follow-up, and Attorney General Reno mentioned this as well. A lot of companies that I interact with, maybe you do too, there's a conclusion people erroneously jump to that says I'm not sure I've got the best technology to combat this. But more often than not, they do. What's lacking is the policies and the clear thinking about how a business or any organization should apply that technology, the layers of defenses taking advantage of existing technology that needs to be instituted and then the disciplines that people must be expected to adhere to in organizations so that this kind of thing can be thwarted off. And I think that kind of information also if we can have the right forum to share that would be immensely valuable.

MR. MILLER: Thank you. Stuart, last question.

STUART: The Defense Science Board asked me to look at legal issues on the information warfare defense. And one of the tentative conclusions that I think we're coming to is the NIPC can't really effectively deal with the private sector and take into account non law enforcement considerations if it is buried as deep as it is in the FBI. And I wondered what thought had been given to making it more truly inter-agency and getting a higher level of political attention within the government.

MR. MILLER: The question is, I guess primarily to the Attorney General, whether the National Infrastructure Protection Center, NIPC, is placed in the right position within the government currently which is within the FBI in terms of its ability to deal most effectively with the broad based commercial sector.

ATTORNEY GENERAL RENO: I think it's important because there is no other agency in terms of law enforcement that has the jurisdiction and the authority to make the NIPC's actions real. I think it needs more and more focus as it comes into its own. And I will take back your words.

MR. MILLER: Okay. At this point, General Reno has to leave for another appointment. She will be back this afternoon.

ATTORNEY GENERAL RENO: If anybody has any other questions.

MR. MILLER: Oh, okay. Well, she still wants to stick around. Listen, hey. She's the boss. As long as it's on this topic.

QUESTION: (inaudible) the FBI agent is going to cart away their servers and that's their livelihood if they do make such a report.

ATTORNEY GENERAL RENO: That's the reason we're here today about what's going to be carted away and who's going to be inconvenienced. One of the problems that you face as you prepare a case is developing the evidence sufficient to prosecute. And to develop the evidence, you've got to go through it, make it available to the prosecutor, make it in a form that can be introduced in court.

And what I think we have done is address the issue of just what you're talking about by figuring out what we can do to preserve records, how we can make copies, how we can continue the business without interruption in every way that is possible. And what we have again discovered is that industry often times has some very good ideas about how it can be done.

MR. MILLER: Jim, last question. Oh, there's one more back there. Jim and then the gentleman back there.

JIM: I have also a question for the Attorney General (inaudible). Michael Dell, founder and President, CEO of Dell Computers, spoke at the National Press Club a couple of weeks ago. He made a very interesting statement and I'll

just paraphrase. He said Americans can have privacy -- cyber privacy -- or they can have cyber security, but they can't have both. He said the two ideals are in conflict with each other. Do you agree with that?

ATTORNEY GENERAL RENO: I think you have hit upon the great balancing act of this extraordinary document that we live under, how you can have freedom of speech and yet security, how you can have privacy yet security and lawyers, newspaper people, people in industry have been walking that fine line for a long time.

What it requires is people in this instance who understand the technology, who also understand the legal issues and the constitutional principles applicable to this area. And that is why it is such a challenge to identify people who have the expertise, both in the law and in the technology that can give meaning to it for all of us. But you have -- that is the great balancing act of our democracy.

JIM: Do you think we can have both?

ATTORNEY GENERAL RENO: Yes.

MR. MILLER: On behalf of ITA, I concur. In fact, I hate to disagree with such a titan of industry as Mr. Dell, but I think without cyber security, you can't have privacy.

We had an incident a few months ago where a major online vendor who sold CDs online protected the privacy in the sense that they did not sell lists of their customers. They didn't give away information for marketing. They did all the right things in terms of the FTC privacy policy. Then someone stole their list by hacking in. So the privacy was all gone. Three hundred and some thousand credit cards were given away.

So they had the right privacy policy under the way the FTC defines it and the way the industry defines it, but everyone's privacy was lost because someone broke through the security. So I don't see that it's mutually exclusive. In fact, I think they're mutually supportive. Gentleman in

the back had a question.

QUESTION: Yes, the Attorney General mentioned using some models from the non online world as mechanisms to demonstrate how they work together. I'd be interested in some of those cooperative models that she sees that are working today in the government in the non online world for law enforcement industries. Are there examples you can draw from?

ATTORNEY GENERAL RENO: I think you can draw a number of examples. When prosecutors and the banking industry work together, they can understand what can be effective, what can't, how they limit how they protect confidentiality. The bank understands that if the case is prosecuted, that there will be -- we can assure confidentiality. But I think much has been done in that area. Much has been done in the area of white collar crime.

We have given much more attention in these last seven years to the whole issue of victims right in any area, whether it be terrorism, violent crime, white collar crime and similar instances.

And what it comes down to -- and I was going to make sure that I heard from everyone before I made this announcement. I'm asking the U.S. attorneys in the 93 districts across the country to sit down with industry in their communities to make sure that they establish the contacts.

There is nothing so effective as an FBI agent who knows what she or he is doing in the cyber world who goes to the banker and says let's sit down and talk. Or goes to the bank's security officer and says let's sit down and talk and then goes back and gets the SAC from the FBI to go talk to the bank president about security. And it really can make a difference. But it really comes down to personal contact.

So in terms of nationwide, I would hesitate to tell you that everything is perfect nationwide. I can tell you that where industry and the investigators come together and the

prosecutors come together there is tremendous cooperation, understanding and I think successful prosecutions are resulting.

MR. MILLER: General Reno, thank you very, very much for taking your time. We look forward to seeing you this afternoon. Dick Brown, again, thank you for hosting this and for being with us today. We'll now have a 20 minute coffee break. Please be back in your seats at 10:30 when we'll have a chance for everyone to introduce himself or herself and also review what came out of the meeting that was held in Silicon Valley in April. Thank you, very much. Please thank the Attorney General and Dick Brown.