THE BROOKINGS INSTITUTION

CYBERSECURITY: INCENTIVES AND GOVERNANCE

Washington, D.C.

Thursday, July 21, 2011

PARTICIPANTS:

Welcome and Introduction:

DARRELL WEST
Vice President and Director, Governance Studies
Director, Center for Technology Innovation
The Brookings Institution

Moderator:

ALLAN FRIEDMAN
Fellow and Research Director, Center for Technology Innovation
The Brookings Institution

Panelists:

BRUCE McCONNELL
Senior Counselor and Director, Cyber+Strategy
National Protection and Programs Directorate
U.S. Department of Homeland Security

LARRY CLINTON
President and Chief Executive Officer
Internet Security Alliance

* * * * *

P R O C E E D I N G S

MR. WEST: (in progress) -- in the Harvard Computer Science Department, where he worked on cybersecurity policy, privacy-enhancing technologies, and the economics of information security. He also has served as a fellow at the Belfer Center for Science and International Affairs at Harvard, where he worked on the Minerva Project for cyber international relations. He has a degree in Computer Science from Swarthmore College and a PhD in Public Policy from Harvard.

Before turning the program over to Allan, who will introduce our guests, I want to mention that this afternoon at 3:30 we are hosting a forum in this room on ways to protect privacy. We will be hearing from John Leibowitz, the chairman of the Federal Trade Commission; Cameron Kerry, who is the general counsel for the Department of Commerce; Mark Cooper of the Consumer Federation of America; and Allan will be back as well. So, this is a double-hitter day at Brookings, with cybersecurity in the morning and privacy protection in the afternoon. So if you have time, please join us for this afternoon's session.

And with that, I will turn it over to Allan.

MR. FRIEDMAN: Thank you, Darrell. And first, I'd like to thank Bruce and Larry for coming out this morning.

The program today is basically going to start with some of the basic lessons that those of you who have been in the cybersecurity field for a while are going to say, gosh this is obvious. But the problem is, I think we need to keep hammering them home until they're sort of standard talking points. Then we can actually move on to some of the real questions, which is what are we actually going to do? And hopefully we'll be able to get to there in the discussion today.

Before I sort of briefly summarize what's in the paper, I just want to introduce the two gentlemen with me up on the stage. We're joined by Bruce McConnell, who is the senior counselor for National Protection and Programs Directorate of the Department for Homeland Security. And he's senior advisor on a host of strategic and policy matters relating to national protection. And prior to that, he was a member of the Obama/Biden presidential transition team focusing on a wide range of technology issues. He has a previous stint in government from 1993 to 1999 as the chief information policy and technology in the U.S. Office of Management and Budget. And in-between, he had a consulting firm where he talked extensively about the relationship between information technology, policy, and government behavior.

Someone who has also spent time in government but now sort of represents the private sector approach is Larry Clinton, who is the president of the Internet Security Alliance. It's a multi-sector trade association with members from virtually every one of the designated critical infrastructure industry sectors. The mission of the ISA is to combine advanced technology with economics and public policy to create a sustainable system for cybersecurity. Larry before that also spent time on the Hill as a staffer for Rick Boucher, and he's spent a lot of time communicating some important cybersecurity issues to the press. And he's testified before Congress to talk about it. His paper, the ISI's paper on cybersecurity from the market perspective is important enough it is both the first and last cited paper in President Obama's 90-day cyber view paper.

So -- (laughter) -- the -- yes, I've got to be careful about citation counts. That's the means to success, we all know.

So, thinking generally about cybersecurity, I think there are a few critical points to make. The first is, cybersecurity is a type of risk. And it is a subset of risk. So whenever we're dealing with challenges of thinking about infrastructures, there is going to be some risk that we're going to be tolerating.

To say this is a unique problem or this is a problem that is somehow apart from other points of risk, it does us a disservice. I'm going to talk a little bit about the need to disambiguate. But I think the general approach is to say, listen. If I take my smart phone and hurl it over at

Larry, I have not engaged in a cyber attack. I think colleague Peter Singer at Brookings said, you know, we have something like a teenager being irresponsible with bottle rockets, we have criminals using handguns, we have insurgents who have homemade explosive devices, and we have states with cruise missiles. They all use gunpowder, but to treat them under a common framework doesn't make sense.

But I feel that we are. So, recently Senators Lieberman and Collins wrote an op-ed in defense of their cybersecurity legislation. And leaving the specifics of the legislation aside, they motivated by saying, listen. This stuff is important, look at the recent headlines. We have Stuxnet, we have the attack on RSA, and we have the recent attacks on Citigroup. But these are wildly different types of attacks targeting wildly different things.

Against Citigroup, some fairly innovative attackers took advantage of a truly preposterous defensive structure wherein knowing an account number would allow you to capture someone's Web session. Essentially, allow them to log into an account. And it turns out they were sequential. So it's fairly easy to do, once you realize the idea happens. They were able to take the account numbers and do some damage. But they were interested in profit.

Against RSA we know it started with a simple e-mail that people shouldn't have opened. We can talk about the mechanism to prevent people from opening e-mails that they shouldn't open. But we've known about this vector for a while. They were -- escalate this attack and obtain a critical piece of intellectual property, a critical trade secret that then allowed further exploitation. So, started off simply, escalated in a very clever fashion for a very targeted attack. They knew what they wanted, they were going after a certain thing.

Targeted attacks I'll talk a little bit imply some sort of budget. Some amount of saying, I want this and I'm going to expend a certain amount to get it. And that should be part of our calculation.

And finally, we have this question of Stuxnet, which is one of the first examples of an IT-based attack that had very real world kinetic implications. It affected another country's national defense posture. This is a very big issue. But to put it on the table at the same time we're talking about electronic bank fraud doesn't make sense. There is no intellectual framework, there is no academic discipline. There is no government agency that can or, indeed, should be able to think about all these things at once.

So, why do we need to disambiguate these? So one, is they have very different scales and scopes. If we're saying this is an important enough issue to talk about it here in D.C., it has policy issues -- there's a public interest in it. But we need to learn more about what the public interest is. We should prevent crime. I think everyone here is in favor of less crime. But no one says we should make this a primary national priority to prevent certain types of fraud.

Now, one could say listen, yes. We should because we're worried about some critical failure to our infrastructure. But then we need to focus explicitly on that and say, what is the tipping point they're worrying about?

Similarly, we can talk about cyber war. Now, there are some people that have said this is an existential threat. That attacks could come and they could destroy our critical infrastructure. I tend to fall on the skeptical side of that line for a number of reasons. I guess back when I was an economist, I was a Bejanist. Bejanists say, you have to understand the probability of everything in relationship to everything else. So, once a country decides to attack us or once someone with sufficiently large capacity decides to attack us then, in fact, yes. We can say they are motivated. A sufficiently advanced country would have the capability to do something right now.

But you also have to say, well what else does the world look like when we are at war with a major industrialized adversary? And I would say that a lot of other things change. Most of my intellectual models fall apart. There are people here at Brookings and elsewhere who are paid to understand what war between two major industrialized countries look like. But I feel that we can't take those assumptions and map them onto the everyday world.

Finally, we have the question of intellectual espionage. And this is something that I think a growing number of people said, this is the key important aspect. This is something that should be driving all of our attention. In fact, Undersecretary of Defense Lynn said this is potentially -- espionage is the main threat.

But if we're looking at espionage in government, this is a state issue. And this is part of a broader framework of how states interact. If we're looking at it in the private sector I would say, yes. Now we're talking about something that is new. That we actually have the capacity to have wholesale exultration of data.

However, in as much as there is a public interest that we as a country lose a lot from this lack of competitiveness. The people who should care even more than United States taxpayers are the shareholders of these companies that are under threat. So, the approach should be, how do we examine this?

In the paper I talk a little bit about why economics is a useful framework. The sub-field of the economics of information security is now about 10 years old. And it's very interesting. It has sort of recapitulated the history of economics. It started off with a bunch of people who said, in the late-'90s and early-2000s, you know, gosh. We should think about this in terms of incentives. Similar to, you know, Adam Smith in the late 1700s.

And then some people say, you know what? If we can think about incentives, I bet we can throw up some Greek symbols on the chalkboard to describe these incentives. And so everyone spent some time writing some interesting equations. And then someone said, you know I'm not sure if these equations actually describe reality. Let's do some econometrics. And just now, we're getting into the field of behavioral research for information security. Understanding why we have -- you know, what are the incentives that actually count? What is the bounded rationality decision? Are humans the weak link? And how do we change actual human behavior? How do we make things useable?

And you know, for example, one interesting result that was just released at a recent conference on this is that we have strong evidence that good information lasts in people's minds less than bad information. It is discounted at a different rate. Which means, if you're a company trying to assert something about yourself, it's going to be much, much harder to say, hey. I am a good actor, you should remember that and reward me for that in the future than saying you're a bad actor. Saying you're a bad actor has a much longer lasting impact in terms of saying you've been risk -- you have been punished. So that points the fact that we can't necessarily use the tools of deterrence -- or rather, we can't use the tools of positive affirmation of good behavior. We have to rely on deterrence.

So briefly going over a few of the policy frameworks that we talk about in the paper. One is the question of low-hanging fruits. There really are some very straightforward, at least, technical fixes. Go through all of the recent headlines. Oh my goodness. This contractor got hacked, that bank got hacked, we have a number of groups out there that are trying to do -- they're anarchists. We've dealt with this as a society before. But the question is, what are they doing?

And the answer is, they're not doing things that are terribly sophisticated. They're taking advantage of a vulnerability in the way dynamic Websites work.

No one should be vulnerable to a sequel injection attack. I think you just sanitize your inputs. Make designing a Website slightly harder. But then you don't have to worry about that vector.

So, there is a set of things -- and we can talk about what those things might be. We can say, listen. This is the easy stuff. Why are we still doing this? The challenge is, how do we actually get this to happen. Because while it is easy, it is not free to implement it.

So there are two basic frameworks we can talk about for promoting good behavior. One is affirmative standards. And these can come from industry, or they can come from the government. So, in some specific sectors -- healthcare, finance -- the government comes out and says, these are the standards you need to have for your protection.

This leads to the compliance problem. If people are, in fact, complying, does that make them secure? And the challenge of changing the incentives, now it's not about making yourself secure. Now it's just about complying with the law. So the trick is going to be to understand where there is a mismatch, where there is a divergence, and try to have a dynamic posture where compliance is as cheap as possible and also as flexible as possible.

Against this idea of saying, here's a positive adaptation, we can rely on a deterrence model. Say, listen. If you don't invest in security, if you remain insecure, then there will be some mechanism for punishing you. And we can do this in a lightweight fashion or a more strenuous fashion. Lightweight fashion depends on reputation. The market will punish you by itself.

I have an earlier paper, which looks at companies that have suffered a data breech. Does the stock market care? And it turns out that the stock market does care. And we can measure it just to the barest degree of significance. It's a small effect. So, then I can say, listen. This will take care of itself. There should be no more data breeches now that we have public disclosure laws. Which of course, we know isn't true. There are public disclosure laws. There is some evidence that data breeches are going down under certain types of organizations. But certainly not across the economy.

So, we can look at a stronger approach -- and I talk about this more in the paper -- of liability. Of actually holding companies accountable for this. And we have a challenge there of saying, what is going to be the standard of liability? It is very easy to sort of tell a story of saying, we'll hold you accountable. It's much harder when we actually dive into the specifics of saying, what are the actual approaches?

If you produce buggy software and something bad happens because of your software -- if you are held accountable for all the damages for anyone using your software, then it's quite difficult to imagine why anyone would create more software.

Transparency is also useful for intellectual property theft. So, we talk a lot about this idea that, you know, the United States is going to lose its innovative edge. We are a country that is built on not building stuff, but coming up with the ideas for stuff. So, if someone steals all of our ideas, then we've wasted a lot of effort and lose our competitiveness. And I think there's some truth to that. But again, in as much as the government should care, the shareholders of companies need to care even more.

Several senators on the Commerce Committee recently wrote a letter to the SEC saying we'd like you to evaluate what counts as a material breech of security. So that if a company does, indeed, lose something dramatic, investors know. And we see that there isn't this disclosure.

So for example, last January's attack on Google. The so-called Aurora Attacks. We know that between 20 and 32 other companies were involved in those attacks. We still don't know very many of them at all. We know very little about who lost what data. So, we can say, this is a big deal.

One of the interesting things is, when asked in her response to the senator's letter the chairwoman of the SEC said, well, happy to look into this. We're going to focus on it. But frankly, this is not something we've seen a lot of investor demand for. And I find that fascinating to understand why this isn't something we see demand for.

So, I'd love to have Bruce and Larry come up and talk a little bit about what they see some of the issues are in terms of incentives in governance. And we can sort of drill down from the top and try to get a -- to some more specific policy frameworks.

So, I'd like to have Bruce come up and share some remarks.

MR. MCCONNELL: Thanks so much, Allan. And it's always great to be on a discussion with Larry, because we always have good differences of opinion. So I think this should be an interesting morning for all of us.

Thanks very much, Allan, for that paper. I think it provides an excellent survey. I haven't read every word on it, because I just saw it this morning. And I think you're absolutely right. It's helpful to get a better understanding of the problem. At the same time, we do have to figure out what to do about it. And of course, coming to you from the Department of Homeland Security, that's part of our responsibility is to think about and propose and come up with ideas and execute on ideas about protecting the homeland, and the cyber area is one of our five mission areas in the overall mission of making America as safe, secure, and resilient place where the American ways of life can thrive. So, we are definitely focused on cybersecurity at DHS.

It's refreshing, of course, to step back a little bit and think about this problem and its economics. And what is the impact of that kind of analysis on the solution set that one comes up with. Because not all decisions in

Washington are made on a rational basis. And so, it's always good to put some rationality into the decision process. And in this case, particularly there's a big lack of data. So, we're in a situation where we can make logical arguments. We can make analogies, we can make suppositions. But we don’t have a lot of proof to do. So we have that challenge as well.

But it seems clear enough, anyway, to us that there is not enough investment in cybersecurity in the world today, in the country today. So if you look at, for example, the losses compared with the costs of protecting against those, or the gains from -- to the attackers against their costs for conducting the attack, there's a wide gap. So, right now the U.S. government, for example, spends about $10- or $20 billion -- somewhere between $10- and $20 billion on cybersecurity for its unclassified and some of these other systems.

If you look at the attacks that have -- that Secretary Lynn talked about, which may have compromised the integrity of a weapons system, and you think about the costs of building a weapons system. And if you have, through an attack, you know, compromised the effectiveness of that in a battle situation, then you have a situation where the loss just for that one compromised weapons system -- the cost of that, probably just the investment that was made probably exceeds the entire federal cybersecurity budget. And certainly, the costs of conducting that attack are very much less than the potential gain to an adversary who has that information and can use it. And the secondary effects, obviously, are even greater.

So, I don't think it's a close call at this point, the amount of investment is too low. And -- but, the ways which attacks and compromises can occur is so broad that it's unclear exactly what to invest in. And I'm going to talk about that a little bit more. But when your example of throwing the phone not being a cyber attack -- so in the paper this morning there was a description of a burglary. So at a high tech company in Silicon Valley, some guys or guy came in and in five minutes, went exactly to the server which contained the source code of this company, grabbed it, and out the door. So was that a cyber crime? I'm not sure. And who is he going to sell -- who is he working for, who is he going to sell that intellectual property to? Low cost for the value of what was being, you know -- was not being very well protected.

So in this kind of asymmetry, what you have to do is raise the cost to the attackers. You have to make it harder for them to be successful. Or, you have to make it more worrisome to them, more likely that they're going to get caught. So we were very happy when the FBI was able to arrest 16 people the day before yesterday associated with the anonymous hacking group who had been involved. The crime they committed was taking down Papal for a day, and that's a federal crime. And each incident of that can get you up to 10 years in prison. And any computer that is connected to the network is basically protected under the current federal law. So, that was good that we arrested -- the Dutch arrested four people and the UK one. So that was a good thing. So that's one kind of deterrence.

Maybe people say, oh. I have to be more careful. Obviously that attack and the tactics of anonymous are not the high-end of the attack spectrum. So, the other way to do that, of course, is to invest in better defenses so that it's harder, so that you have to be better resourced. So that not just anybody can do attacks, but that you have to -- it costs you more to do attacks.

So, the question is, why, though? Why are we investing too little in cybersecurity? And as Allan suggests, it's a lot about a lack of information. So, we are in a commercial market situation right now with, for the most part for cybersecurity, there's not a lot of requirements on anybody to buy anything or do anything. And so, we're letting the market work. And markets don't work if there's a lack of information. If imperfect information -- you have a less than efficient market. And there is a lack of information among a lot of people. Decision makers in companies outside of the chief information security officer, who talks in some strange language that the CFO can't understand about the vulnerabilities, the incidents, and the potential losses. So, the fact that we're now starting to see quite a bit of reporting on this is very good. That will reduce the information gap, because companies and firms don't know how to value the confidentiality of information. They don't know how to value the integrity of information, they don't know how to value the losses that have come from the attack affects, whether it's short-term losses or long-term losses.

So, the problem -- thinking about it that way, though, is it leaves out one important aspect of this. Which is that we're all in this together. So as the computers are all, as you know, connected to each other, that's a big part of the advantage. But that means that in some -- to some extent, anyway, we're only as strong as the weakest link in whatever network we're talking about. And so that networked situation means that it's possible that a weakness in one place can serve as a launching point for attacks in other places. And so the investment in local defenses may not provide the maximum societal benefit that's needed when there are potential consequences elsewhere.

And so firms will only invest up to the value of their resources that they're protecting. We just talked about how they may not be valuing those correctly. But in any case, in some situations there may be losses that are societal losses that are broader than that. And so there's no reason why a firm would rationally make investment beyond its own individual cost.

So we have some interesting data. And this kind of relates to this afternoon's discussion on data breech -- on privacy, because we have a situation now where we have security breech notification if you disclose or if you have had stolen or otherwise lost a laptop, you name it, information about individuals over a certain level. What we call in the government personally identifiable information. And that requires you to notify the consumers or the individuals who are affected about that. There was just an article in the paper that -- the Government Accountability Office saying that -- criticizing the IRS for being slow in notifying taxpayers about data breeches that it has.

And so -- but if you look at the private sector ones, you can see that they are really quite expensive to the companies to notify everyone. And so it's possible that this is creating a proxy, anyway, for the costs of security failures. And maybe that will provide some data over time as we watch that, to use that data in risk and return and investment calculations and that kind of thing. So that's an interesting thing that's happening.

Part of the Administration's Cyber Bill, which I'll talk about in a minute, includes a provision that would make a uniform data breech notification requirement across all the states. Because they're different in each state. We have 47 different ones. And so, that's not easy if you do business in more than one state, how to comply with those things. And so the national law would reduce the cost to companies of compliance. It's not -- we didn't pick the highest standard, though, so some privacy advocates argue that, you know, we're watering down the standards in the states that have stronger requirements.

So, if it's true that we're not making enough investment and the reason for that is, at least in part because of a lack of information. And also because there are network effects, there's a public good aspect to this, then where should we make investments to increase the cost? How do we increase the cost? Where's the best place to make investments? Should we, in fact, as Allan suggests, require computer software manufacturers to be responsible for something other than what they're responsible for under the user licenses, the ULAs, in which they're responsible for nothing? Should we require some sort of liability for unsafe products?

And the argument there, of course, is that it's very difficult to figure out whose fault it actually was for the unsafe-ness of this product. Because it may have been improperly installed, or it may have been improperly used.

Allan mentioned that the RSA attacks were result -- the opening to them was a result that here you have a large security company and somebody was a victim of spear fishing in which they got a very authentic-looking e-mail that had a link in it that sent, you know -- that created a vulnerability that allowed the attacker to get inside the firewall and set up a presence there. So you would think that they have good training at that company, and that person should have known better. And as we say, there's no patch for stupidity. So, you know, you can make the best software but you can always find ways around it.

And so, the spear fishing attacks are getting very sophisticated. They're getting very tailored. And again, because the value you can get versus the cost of -- to you either in terms of the probability that you'll get caught or the -- just the basic costs of your time and technology that you need to do it is so out of balance.

So, if you look at the kinds of threats, then, that we are trying to think about in order to determine, well where should we stimulate this investment? Then as you said, it's not all attacks are equal, right? So there's a bunch of attacks. Some of the anonymous attacks, for example, and others where more careful configuration of systems following basic security practice, basic hygiene, things like that. You know, putting up more access controls and various things is -- would be able to solve or defend against, you know, a large number of attacks that we have out there. And so there is a situation where the entity is just not making the investment on its own. But the effect is fairly limited, and those I would call in the basic category.

And then, there's a more advanced category that is -- where it's required to have a lot of capital investment in order to do the attack, in order to conduct it. And those are kind of the high-ends of things. That are the ones that we worry about the most, and where there are externalities. And so, may require some additional stimulus to getting the investment right. And it's a spectrum. There's not one size -- you know, there's not a bright line between those two kinds of things. But there's sort of -- there is a general problem, and then there's the more specific problems. And it relates in particular to what things need to be protected and what the potential effects are on the economy, or otherwise from the attacks.

So, the way we try to think about it, then, is more on a -- is on a risk-based approach. Meaning, what are the risks to the country? And for these various attacks. And so, attacks that tend to, you know, affect just individuals are probably less worrisome than ones that affect small businesses where there could be economic effects. And then you have the larger firms, defense firms, critical infrastructure, defense, and other agencies where, you know, the consequences of inadequate protection are more significant.

So at that point, then, you start to think about, well, what are the tools that -- and obviously I'm bringing to you a governmental perspective. What are the tools that the government has to influence this situation? And so the way we think about it at DHS is that we -- our role in cybersecurity allows us to do three kinds of things. We enable others to protect themselves, primarily through education. We, to some extent, require -- we can require people to do things. And then, we can do. So, enable, require, do. We can actually protect things, the government can actually protect things itself.

So, in those -- so, no one-size-fits-all. That's our toolkit. And within each of those baskets, there are a variety of things that can be done. So in the enable part, we spend a lot of time on sending out alerts to the public and to critical infrastructure owners saying, watch out for this kind of malware. Be sure and -- you're checking for this. Here's something new that we're seeing. Trying to get those out to the people who are responsible for securing. We get that information from a variety of sources. We get them from some of our private sector partners who we share information with, we get them from other government agencies. And so, that kind of education and alerting is a piece of the enable part.

Another longer-term has to do with creating generalized awareness in the private -- among the general public. So we have our stop, think, connect campaign. Stop and think before you connect. And we also have something called the National Initiative for Cybersecurity Education, which is trying to improve the general level of cybersecurity professionals and get more of them. Because everyone who is trying to do cybersecurity in today's environment is facing a shortage of trained professionals in this area. So, those kinds of things and others to create and promote standards of what good cybersecurity practices are all in the enable area.

Now, in the require basket, at the moment the government except in a few select cases does not have the ability to require the private sector firms to do very much about cybersecurity. There is, in some sectors -- in the nuclear sector there are requirements laid out by the Nuclear Regulatory Commission. In the chemical sector, DHS requires chemical facilities to have cybersecurity plans. But in general, there's -- it's a pretty spotty arrangement.

And so the -- in this area, the administration has proposed what we're calling a light touch regulatory approach, which would empower DHS to set out a framework for critical infrastructure owners, power plants, and transportation systems, and telecommunications, and those kinds of things that are essential to the functioning of the economy and whose -- damage to whom would be very bad for the general public.

Excuse me -- the legislation that we propose would have us -- require us to list what are the risks that people need to address? And then we would ask -- and we would do this all through a public process of interaction through a rulemaking process, so that would be very collegial with the private sector and with the affected entities, obviously. So we would say, these are the risks that you need to address. And then we would ask the private sector to identify some risk frameworks. What are some good ways of addressing these risks? And there's some out there already, some international standards and other ones that might be proposed.

But anyway, at some point we would say, okay. We think these are adequate risk frameworks for addressing these risks that we have identified. And then, companies would have to plan -- take a plan, make a plan to address those risks. And they would be audited by a third-party auditor to see if they were, in fact, implementing their plan.

So it's not a compliance-based approach, it's not a technology-specific where we're saying you have to, you know, buy this kind of firewall. It's a framework that allows firms to select the most economically-efficient ways of addressing what the risks that we've identified in cases where the societal cost of not addressing them is judged to be too high in the current situation.

So finally, then, in a last piece of our toolkit is the do part. And at the moment, again, our focus, just like in the regulatory part of our current activities, is on the federal government. So in the regulatory part and the federal government, DHS requires the federal agencies to pay attention to security through a variety of techniques. And similarly, in the do part we have a system -- the National Cybersecurity Protection System -- which creates a kind of a big advanced firewall around the federal agencies to help them stop bad traffic from coming in, stop known malware, and neutralize it. It's called the Einstein Program.

We are now -- the government is now piloting the use of that kind of technology with some of the defense companies to see whether or not that would work by working with the Internet service providers, to give them information that is about threats that they may not know about, and have them block those threats before they get to these participating defense companies. It's an experiment to see if that works, if it enhances the protection that the ISPs and the defense companies already have, or whether it doesn't. So that, we're going to be evaluating for another 60 days. But that's another possible activity in the do category.

Just one last thing to say. And that is, over the longer term, of course, we're still in this catch up mode where the -- in a very asymmetrical situation. The Internet was not designed to be protected, and so that is what we are facing. We -- in the strategy that DHS is developing for cybersecurity which will be out later this year, we spend quite a bit of time talking about what we're talking about now, which is how do we protect critical infrastructure today. But we spend also time on the other half, if you will, of the strategy. Which is, how do we create an ecosystem which is more secure in the future so that it's not a matter of expensively bolting on security after the fact. But, that it's built in and that we're using the machines to help protect themselves and thus help us.

Because there are advantages to the highly distributed nature of cyberspace, and we should take advantage of those advantages to help in its own security and its own defense. So I won't go into that more this morning, because we're trying to focus more, I think, right now anyway on how do we get more quickly off the bad -- out of the bad situation that we're in.

So I look forward to the discussion in a few minutes.

MR. CLINTON: I want to thank you all for being here. And thank Allan for inviting me. And I, too, am looking forward to the conversation with Bruce. It's true, we do have some, I think, very friendly but some clear disagreements.

And so I want to start off by agreeing with Bruce one something. Bruce started his comments by saying he was sure that Allan's paper was an excellent paper even though he hadn't read every word. And I want to agree with Bruce. I am sure that Allan's paper is an excellent paper, and I haven't read a single word. (Laughter) But, I am certainly pleased to be here.

Allan gave a correct summary of what the Internet Security Alliance is. We are a multi-trade association organization focused exclusively on cybersecurity. One thing that we didn't mention is that we were created in 2001 -- or, 2000, actually. So that's nearly 2 years before the tragic events of 9/11. It's four years before the government created the Department of Homeland Security. It's six years before the government decided that we needed an assistant secretary for cybersecurity, seven years before the government filled that position, nine years before they came out with their original proposals. And, 11 years before they came out with a legislative proposal. So, we are delighted to have our government colleagues joining us more aggressively in this fight.

I -- it is correct that I've been testifying in Congress -- every single Congress in 2004 pleading for greater government attention to the issue of cybersecurity. And so we are delighted to see the Senators Lieberman and Collins, as well as Rockefeller, Snow, and a number of others. And of course, the Administration now moving more aggressively to address this sort of problem. This is a critical problem to the economy, to us as individuals, and of course to national security.

But let's talk a little bit about what exactly that problem is. Allan also gave you the mission statement of the Internet Security Alliance, so let me repeat it. Our goal is to take advanced technology and economics and public policy and merge them to create a sustainable system of cybersecurity. We are less interested in discrete solutions than we are in creating a sustainable system. I noticed that Bruce also commented that he thought it was going to be refreshing to take a step back and look at this from an economic perspective. And that is exactly what we are urging our government partners to do.

Cybersecurity, ladies and gentlemen, is not an IT issue. It is an enterprise-wide risk management issue. And the main reason that we are not making more headway on it is because we are not dealing with the economics of the issue. To quote some of those earlier economists in this field, two fellows named Anderson and Moore did a fairly extensive study. And they found that -- we found that misplaced incentives are as important as technical design. Security failure is caused at least as often by bad incentives as by bad technological design. Economists have long-known that liabilities should be assigned to the entity who can manage risk, yet everywhere we look in the online world, we see that risk is allocated poorly. People who connect their machines to risky places do not bear the full consequences of their actions, and developers are not compensated for their efforts to strengthen the code.

So, we talk a little bit about the incentives for cybersecurity. So, let me ask you to envision a balance here of the good guys and the bad guys. And here is the economic equation for cybersecurity. Cyber attacks are currently pretty cheap. You can get them on the Internet for almost nothing. They're easy to deploy, you can actually outsource for it. They are tremendously profitable, as Bruce just mentioned. You can make millions, maybe billions. One estimate, a trillion dollars on it. And by the way, the business plan is terrific. You can use the same product over and over and over again, you know, with little additional cost.

The defense side? It is almost inherently a generation behind the attacker. It's really difficult to demonstrate return on investment because it's hard to come up with metrics for what you have prevented. It's -- and notwithstanding, the 20 people who got arrested for cyber crime that Bruce mentioned. Prosecution is little to nonexistent.

So here is our economic cybersecurity equation. Okay? It doesn't make any difference what kind of technology we deploy. The incentives to attack are so overwhelming that unless we rebalance the economics, we are not going to be able to develop a sustained model of cybersecurity which is what we should be about.

One of the -- if I had to have one criticism. And as Bruce knows, I have a number. But if I had to have one criticism of our government partners in this, it is that they have not focused enough attention on the economics of cybersecurity because it is the economics that are our biggest problem.

I have -- I brought some statistics with us on this, if I can find them. Well, both the CSIS report for McAfee and a study done by PricewaterhouseCoopers came up with several discrete findings that all say that cost is the major reason that we are not solving our subsequent -- here we are. These are a series of quotes from CSIS from McAfee, and the PricewaterhouseCoopers surveys in 2010.

Overall cost was the most frequently cited as the biggest obstacle to ensuring security of critical networks. "Making the business case for cybersecurity remains the major challenge because management often does not understand the scale of the threat or the requirements for the solutions. The number one barrier is that the security folks haven't been able to communicate the urgency well enough and they haven't actually been able to persuade decision makers of the reality of the threat. So, until we deal with these cost issues, we're not going to make any progress."

Now, I was on another panel yesterday with one of Bruce's government colleagues. Again, like Bruce, a terrific leader in this space. A fellow named Ron Ross over at NIST, some of you may know him. And he gave an exhaustive description of the excellent work NIST is doing on standards for cybersecurity. List after list -- we have this standard and we have this standard and we have this standard and we have this list. In fact, the joke in the cybersecurity standards world is that the thing about cybersecurity standards is that there are so many of them. You know, we've got tons of these things.

And unfortunately Ron had to leave. But the first question I asked the audience after he left was, if you gave that presentation to your CFO, what would be the firs question he would ask? How much is that going to cost? And Ron was asked during his question and answer session, you know, what about the budgetary considerations? And he said, well, industry is just going to have to bite the bullet. That is not, my friends, a sustainable solution. We're going to have to come up with something a little bit better than you have to bite the bullet or get around the bureaucracy.

Un-economic investments are not sustainable. And this is a problem that we're going to continue to have with us, and therefore we need to come up with a sustainable solution. We need to address the cost issues.

Now let me get into this with a little bit more detail. And I'll try not to get too boring. But as I think both Bruce and Allan talked about before, you can divide cybersecurity attacks a thousand different ways. But one way to do it is to divide them into this basic category and the ultra-sophisticated category. The basic category is the vast majority of attacks; 90, 95 percent of the attacks. Now, just because it's a basic sort of attack doesn't mean it can't be devastating. These are really -- can be really very devastating attacks.

But what really characterizes them is that there is a tremendous consensus in the field that these attacks are manageable. And when I say a tremendous consensus, I mean the CIA, the NSA, the Secret Service, private sector companies like Verizon, PricewaterhouseCoopers have all agreed that somewhere between 80 to 95 percent of these basic-style attacks could be successfully prevented or mitigated completely. Because lots of times, you don't actually stop the attack, you just manage it. Simply by deploying standards and practices that are already existing in the marketplace, many of which are not that expensive. Okay? 80 to 95 percent.

So, the data seems to indicate that that's where the expenditure ought to be, is to provide the economic incentive to have the investment done to deploy those things that are going to solve 80 to 95 percent of the attacks.

One of those studies we mentioned particularly from Verizon was, I thought, a really good study. Actually, it was not a Verizon study. It was Verizon in conjunction with the Secret Service together. It came out last year. They did a forensic analysis of 400 actual breeches, went back in to see what happened. Tens of thousands of data points. And they determined 94 percent of those breeches could have been successfully mitigated or prevented simply by adopting this best practices and standards. So that's where we ought to be focusing some of our attention.

Now, on the other hand, we have these ultra sophisticated attacks. This is NFL level stuff here, okay? These people are really, really good. These are not kids in basements, this is not Ferris Bueller we're dealing with. These people are highly organized, well funded. They have suites of attack vectors that they keep coming after you with. They are probably state-supported, in many instances state-supported. These are what we like to call the APT, the advanced persistent threat. And what really characterizes the advanced persistent threat is that they are going to get into your network. You are not going to keep them out. No best practice, no standard, no magic widget is going to come up to stop these guys. They are going to keep coming after you and they are going to get in.

Now, that doesn't mean that we have no defense. It means that we have to alter our strategy of defense away from awareness and perimeter defense to internal investigation and mitigation. And we can do this and have done this successfully in certain instances. And we need to put in place the appropriate incentives so that we can generalize that model.

Now, some of the things I was asked to -- in illustrate some of the things that ISA does -- and I'm not interested in giving a -- well, I'm very interested, actually, in giving an ISA commercial. But I'm going to try to not do that at the moment. But, we do on our own try to address these issues. So, among the sorts of programs that we have developed is this one, which deals with the financial management of cyber risk.

We've issued a couple of publications on the financial management of cyber risk, because we went back at the start of this program in 2007 -- went back and we found that -- and I think Bruce alluded to this. There is a tremendous misperception of what cybersecurity is, particularly in the corporate suites. I, as well as a number of us here in the audience -- I think are what we call digital immigrants. You know that term? Those of us who were not born into the digital world we currently inhabit. We're digital immigrants. As opposed to my daughter, she's a digital native. Okay.

Most senior managers are these digital immigrants. And they have been thinking of cybersecurity as an IT issue. So they put the IT guy in charge of it. That's the wrong way to go. The number one single threat we have has nothing to do with information technology, frontally, anyway. It's insiders. Badly-trained insiders, corrupted insiders, not too bright insiders, et cetera, et cetera. Insider threats are the biggest threat. The WikiLeaks was an insider threat. That wasn't a technical issue, it was a bad management issue.

So what we have done is try to come up with an enterprise-wide model to take cybersecurity out of the IT guy's control and give it in control of an enterprise-wide structure within the organization with an enterprise-wide cybersecurity budget. So that the communications people, the legal people, the compliance people, as well as the IT people, as well as the human resources people and the financial people are all deciding on cybersecurity by their own.

We started the program in 2008, when at that time only 7 percent of corporations had an enterprise-wide cyber risk management team. Carnegie Mellon just did a study for us. They said that number is now up to 87 percent. We are seeing a dramatic increase in more corporations locating cybersecurity not as an IT issue, but central to the business of the issue. That's where we need to begin to focus.

We've done other programs where we're attempting to take things like mobile phones -- and by the way, if I throw a mobile phone at you it is, according to the FBI, a cyber crime. Any crime committed with a computer, according to the FBI, that is a cyber crime. Including if I hit you over the head with a laptop. Those are cyber crimes.

Now the problem with the mobile phones -- and we all have mobile phones -- is that none of us care about security. How many people here have a smart phone? Come on. How many of you asked about the security in the smart phone when you bought it? Good thing that Allan raised his hand and two others.

We don't care about security. We care about cheap and we care about usability. Same thing with our -- this is not properly being rewarded in the marketplace. So what we have been doing in conjunction with NIST for several years is trying to take the SCAP model used for the federal desk space, try to apply it to mobile technologies so that we can secure the platform better, which will allow the vendors more economically to come in and provide security in a cost-efficient manner.

We're doing the same thing with our supply chain program, where we've done an exhaustive study over the last three years in conjunction with Carnegie Mellon and the U.S. Cyber Consequences Unit to look at the supply chain and find what are the cost-effective mechanisms that you can put into the supply chain to assure it.

The point that I'm trying to make here is that unless we jointly deal with this issue as an economic and technical issue together, which we can do, we're not going to solve the problem.

Let me return briefly to the issue of the advanced persistent threat. This is another example where we think that we need to rethink the model so that we can get at a cybersecurity issue.

Let me take a step back. Before I get to the APT. Let me make kind of a side comment. I think one of the problems we have here -- we'll probably get into discussing markets and failures and all those kinds of things later on -- sorry. Is that we don't really realize the revolutionary period that we are in.

One of the problems we had with cybersecurity is that this is all happened so fast. Lots of us in the audience here, we didn't grow up with computers in the classrooms. You know, we learned how to use them later on. Digitalization is changing everything. It is changing the way we conceive privacy. My teenage daughter has a completely different idea, growing up in the Facebook generation, of what privacy means that I do, and certainly more than my parents -- different than my parents. Our notions of national defense are entirely changed in this digital world.

Who knows what the two greatest defense assets in the history of the United States are? Anybody want to guess?

SPEAKER: (off mike)

MR. CLINTON: Yes, sir.

SPEAKER: (off mike)

MR. CLINTON: Close. Best answer I've heard so far, but wrong. Oh, sorry for playing. But very close. They both have the same last name. Ocean. The Atlantic Ocean and the Pacific Ocean. Two greatest defense assets in the history of our country. We chose what wars we wanted to get into, including the Revolution. They are irrelevant in cyber conflict. Totally irrelevant.

The notion -- there was an article -- we were talking about this outside. There's an article in the *Journal of New England Medicine* yesterday talking about how we have now decided that we are going to outsource memory to Google. Even the way we think about things is changing. That is true with regard to economics also.

The interconnection issue that Bruce mentioned fundamentally alters the economic equations of things. If Bruce is a terrific cyber citizen and does everything that he ought to do to protect his network, but his network is connected to mine and I'm a pretty lousy cyber citizen, Allan is liable to steal Bruce's data from me. I may not have any incentives to guard Bruce's data. Not my data. I don't care, you know?

On the other hand, Bruce's investments in his own security, which are terrific, are being undermined because of my insecurity. We have this growing throughout our economy. We actually have incentives to lower security. Think of voiceover Internet protocol. A couple years ago, all the rage. You know, hey, let's deploy -- in corporations, let's deploy VOIP. And so the security guys would go up to him, and he would say, hey. This stuff is really insecure compared to the old phone system. CFO would say, hey. I'm saving $500,000 a year. We're deploying. You know? Same thing with these extended supply chains, these international supply chains. They are being done for cost efficiency.

Same thing with cloud computing. There was another study done by Pricewaterhouse and *CIO* magazine came out a couple of months ago. That indicated 62 percent of the information security professionals that they questioned had "little or no faith" in the security of information in the cloud. And that included 50 percent of the people who had already put their data in the cloud.

Why are people doing this? Because of the economics. I talked to another -- a well-placed, well-known person in the field whose company is doing very, very well internationally but is hitting all sorts of security problems. He's telling me, I just can't go to my CFO and say, we're not going to enter a $4 billion market because I've got a security issue. It's not going to happen.

We want to be pragmatists about this. We have to bite the bullet and engage with our government partners to come up with a joint framework, because risk is assessed differently by the government than it is by the private sector. So, let me get back to how we can do this with respect to things like the APT.

As I said, the APT is an entirely different sort of attack. Okay? Very sophisticated. They will get in your system. But one of the things we now know is that although we don't have a lot of control over the bad guys out there in the infinite Internet interworld, we do have a lot more control over them when they are inside our systems. And so, we have to alter our perception of defense from perimeter defense to internal defense.

Most attacks are not successful when they break into your network. Most attacks are attempts at thievery. They're only successful when they get back out of the network. If you do sophisticated internal monitoring, you can detect unauthorized outbound traffic, which goes to unauthorized sites. If you block the outbound traffic, which is much easier to do because it's in your system, you can then stop the attack. It's kind of like locking the bank thief inside the vault, so he has a good look at your money but gains nothing from it.

So, we alter our perception of attack. If we instead of exchanging information about inbound threats, which are virtually infinite, to unauthorized outbound traffic, that sort of thing can be put in an economic basis so we can put in appropriate incentives for the elite people who can afford that kind of internal monitoring to share it with the Flowers dot com of the world. So what we have to learn how to do is take the interconnectedness problem that I just talked about, which is a risk. And instead, reconfigure it so that we use the interconnectedness to our benefit. We leverage the ability of the CERTs and the defense contractors and DHS and the sophisticates. And then, we distribute that information in a useable passive fashion to the rest of us in the outside world.

We have to rethink how we're doing this. And let me finally conclude with a couple of comments about incentives, particularly with respect to the legislation, and this is an area where Bruce and I will have some fun, I’m sure, as we go forward.

The Internet Security Alliance believes that the first thing that the federal government ought to be doing is finding incentives to increase the investment in approved or successfully -- not approved, I shouldn’t say approved -- in proven successful best practices, and as I’ve already indicated we’ve got a whole list of these. We do know what they are, do know what to do, we just have to actually do it.

Now, the problem we have here is the federal government, as you may have heard, has no money, or at least they’re not willing to spend any money, so what we are advocating is that we have to find incentives that do not cost the government any money but will have an economic impact for the user, and deploy those incentives, and there are a bunch of them -- liability incentives, procurement incentives, better use of cyber insurance, streamlining regulation, ripping out some of the old analog based regulation and applying it in a digital fashion. There are a variety of things that we think that we can do and that’s what we need our government partners to do, providing the incentives for people to make these investments and make them on an economic basis. It is simply not an acceptable solution to say the private sector is simply going to have to pay more for these things that are un-economic from their business. It won’t work. We’re in a world economy. Those businesses will move other places and that’s a terrible idea.

What we have a problem with in the Administration’s proposal is that they do nothing that we can see to address those core economic issues that we know are the core of the problem and address them and promote the actual cyber security best practices that we already know work. We don’t do that. Instead, and I think I would probably part with Bruce's description of the proposal, I mean, he wasn't inaccurate, of course, in anything he did say, but he left out the notion that these plans that the private sector has to come up with then have to get approved by the Department of Homeland Security --

MR. MCCONNELL: That's not true.

MR. CLINTON: Well, I have the (inaudible) and we can look at that.

MR. MCCONNELL: Okay.

MR. CLINTON: But the Department, as I read your bill, does have the ability to alter these plans and make the private sector do things that may be un-economic, and I think in even your comments you said that these -- you know, you want them to be making investments that are otherwise un-economic and that's unsustainable.

So, what we have to do is find a way to make these investments more economic by solving other problems -- liability insurance, et cetera, for them, regulation -- and make these sustainable. So, the other issue that we would have -- we would probably part company with, is -- the way I read your legislation anyway -- says that the incentive is this disclosure, this notion that we are going to tell everybody that you're not following your plan and supposedly this is going to impact stock price.

Now, who can tell me what company has lost the most from a security breach economically? Anybody remember?

SPEAKER: T.J. Maxx.

MR. CLINTON: T.J. Maxx lost hundreds of millions. What happened to their stock price? Up. You know, we have to understand that the market doesn’t look at cyber security in a vacuum. I personally believe that the smart guys on Wall Street saw all this publicity about T.J. Maxx and their stock price going down, and by the way, it tends to rebound pretty quickly when it goes down -- saw the price going down and said, hey, that’s a buy opportunity. They’ve got great inventory, good distribution markets, you know, low cost of -- said, I’m going to buy. So, the result of a bad security breach, stock price went up.

We don’t think that this is probably the right answer. Not only that, but if it is correct and this kind of disclosure would result in reduced stock prices, to me that’s an incentive for the bad guys overseas to attack the good guys here, because they can make their stock price go down. I mean, lots of the attacks we see are corporate espionages. Our point is, these are the wrong incentives. We do need to put the appropriate incentives into the model, but we need to work collectively with our partners in the public sector in order to do this, and that’s where I think we’re missing two things, we are not considering economics enough, and the public/private partnership is not functioning at the level that it really needs to, and that's -- I'll conclude with that. Thanks.

MR. FRIEDMAN: Thank you, Larry. So, let's see if we can start with something that both of you guys talked a little about which is data and whether we have it and what kind we want, so, for example, we've seen testimony before Congress saying that cyber crime is a $1 trillion problem, which for point of reference, the global pharmaceutical market is about $1 trillion. I don't know where that profit is coming from, but we can -- we have, sort of, some estimates that are associated with industry that say, you know, credit card fraud is $37 billion, whereas the Federal Reserve puts it closer to $3 billion. Is bad data better than no data?

MR. CLINTON: It depends on how bad the data is. It certainly can be. Bad data certainly can push you off in the wrong direction. I think, you know, with regard to the loss figures that you just cited, I think that they're basically talking about very different things. The $1 trillion number, which -- that's the result of a McAfee study and it was cited in the President's Cyber Space Policy Review, which gave it a lot more credibility, and a lot of us are a little dubious of the $1 trillion number. But what they're looking at is the loss of intellectual property, and it's really, really hard to assess the actual financial impact of intellectual property.

So, I would instead use this metric, you know, and offer this, so instead of $37 billion or $147 billion or $1 trillion, I would say a whole boatload of money, gone. Okay? There's a lot of loss out there, and it doesn't matter to me as much whether or not it's a trillion or half a trillion. There's a substantial economic impact, and by the way, that economic impact is going to grow, because as I pointed out in my presentation, this is a great business model. You know, organized criminals are going to move in this direction, and by the way, the people who do this for a living -- they are business men, and they are disreputable business men, obviously -- and they are available to hire to rogue nations and terrorist groups, and as these things get more and more user friendly, that is the attack vectors, things get worse and worse. So, I'm less focused on the trillion dollars than I am, a big problem needs to be solved.

MR. MCCONNELL: So, I would say that we should think about good enough data, so we shouldn't try to get great data, but if we had some good enough data -- so, whenever -- the way the regulatory process works inside the Executive Branch is that whenever an agency, such as Homeland Security, proposes to regulate the public, the Office of Management and Budget, where I used to work, requires them to do an economic analysis to see whether or not the cost of the regulation exceeds the benefits. So, economics is at the heart of any regulatory decisions that the government will be making. And on that basis you would think, okay, well how do you do an economic analysis when we have no data, which is difficult, but in particularly it's difficult to do when you're talking about the regulatory cost of preventing something from occurring because you don't know how many things you are going to prevent.

So, what you end up driven to -- being driven to in most of these analyses, is to say, okay, well what is the cost of compliance with this regulation, whatever it is, and then how much bad would have to happen in order to equal that, and how probable is it that that much bad could happen. So, you don't get -- and then it's more of a -- it's either obvious that the cost of the regulation is way less than the likely bad outcome or it's really close or it's, you know, the opposite end of things, but in this area I think at the moment, since we're doing very little, it would be likely that a small amount of regulation could have a good economic effect. So, you just need some data, good enough data.

MR. FRIEDMAN: So, following from the sort of macro data to the micro data aspect, both of you have talked a little bit about incident data, and Larry, you addressed the idea that, you know, if there's an attack on Bruce, we're all better off if Bruce tells us what happened, sharing some information so that we can learn about what’s going on. That seems to work in a tension against the idea of an accountability approach, where if something bad happens to Bruce and, you know, he’s not punished for it, then you don’t have the incentives we’re talking about. Now we have this problem where I have to face this decision of telling people what happened and risking some accountability, risking some administrative punishment or some liability versus sharing. And it’s hard not to see those two forces as working in tension, that any disclosure mechanism could lead to a fear of being punished, but if we don’t have that, we don’t have the incentives. How do you work with that tension?

MR. MCCONNELL: Well, the way we do it today in the financial sector is that banks get together and share data with a central organization that anonymizes it and then provides it to the banks so they can learn from each other without having to disclose it to each other, for business competitiveness reasons or to the government, so that can work in part. It’s not a great solution, but it’s a partial way of attacking that problem.

MR. CLINTON: Yeah, and we support that kind of notion, which is very different than public disclosure. Public disclosure sounds really, you know, politically correct, but we’re dealing with security here, so public disclosure of security may not be a great idea. Now, obviously, if there is harm, that's a different matter, but that is not the case in a lot of these things.

The other thing I want to mention about disclosure of attacks is that, again, we need to have the right incentives put in place. With these very sophisticated attacks I talked about, the APT style stuff, the whole idea of those is that you don't know that you have been attacked. In fact, the first thing the APT guys, or at least some of them did when they get into your system, is they clean it up for you because they don't want any lousy malware providers, you know, tipping you off in a penetration test. So, you come back and do a penetration test and it came up clean, okay, and it only turns on and off.

So, we have to put in place appropriate incentives for really good internal monitoring. If public disclosure, what's being called on the Hill "name and shame", is put in place, that's an incentive not to find this stuff and that's a really bad idea, and plus there's the incentive to, you know, make another company look bad.

So, you know, how we deal with disclosure is a really careful -- really touchy issue, and the model that Bruce identified, I think, is probably one of the best ones. It's not what we see in some of the legislation, but I think it is the appropriate one.

MR. FRIEDMAN: So, following up on this idea of sort of driving demand for good security, or driving demand for investment, it’s hard to imagine -- you talked a lot about that there are certain investments that don’t make economic sense. It seems to me the way that you change the economics or you make things cheaper, which may not necessarily be the best option for your members, or alternatively you make the cost of not investing in them greater. What is the path forward there if you want to actually change the incentives?

MR. CLINTON: Well, first of all, to be clear about who my members are, I don’t represent the IT industry. Okay? So, making things cheaper -- I mean, most of my members -- some -- I have a couple of IT members, but most of my members are defense contractors, banks, insurance companies, manufacturers, so, less price is great from their point of view.

So, what we’re trying to articulate is that there is going to be a degree -- and I don’t want to put words in Bruce’s mouth, but this is what I understood you say at the end of your presentation -- that there is going to be a degree of un-economic investment from a corporate perspective that may be required in the digital world that we’re now living in, from a national security perspective. Private sector and the public sector assess risk differently, and as we have articulated in the White Paper that ISA and BSA and Chamber of Commerce and the Center for Democracy in

Technology all did together, we have accepted on the private sector side, that we probably, in the national interest, are going to need to increase our investment to match the broader public interest. Essentially what this is is the private sector taking on some traditional government roles, because in the digital world, the private sector's going to be on the frontlines of cyber attacks.

But when you make un-economic investments, we have to do it in a sustainable fashion so you have to find some economic benefit for those companies to do that -- lower their liability, give them an insurance break, make it easier for them to get a government contract, you know, whatever. So, you provide an economic incentive to expand the perimeter of security, adopt these standards and practices, et cetera, and that will handle, you know, some of the basic attacks, and then for these ultra sophisticated attacks we need to find a way to get the elites of the world who are going to invest in these things because it is in their best interest -- the defense contractors and the intelligence community, et cetera -- they are going to have this data. We have to find a way to get that data then disseminated broadly throughout the population and we have provided to our government partners, we actually did several years ago, a paper, you know, which outlines exactly how that can be done and has been done successfully.

Some of my members were attacked in the Google attacks, but they didn't suffer any damage, unlike Google, that's because they did this internal analysis and were able to manage it. Taking that kind of model and disseminating it broadly to the flowers.com of the world doesn't cost them anything, the flowers.com people, you know, the small player, and is already investment that is being done by the elites, so we're trying to leverage that. So, they're different things, but we have to think about investment and think about incentive a little bit differently and think about the partnership differently, but there are ways to accomplish these things.

MR. MCCONNELL: So, what Larry's talking about, it seems, is that one of the ways to deal with this is to get some people to make the investment and that will lower the cost for others, and so that, you know, that's part of -- half of your equation, right, just to lower the cost, so that by creating economies of scale, you know, that seems like it would make some sense.

On the -- so, these incentives that we've been talking about here, which would -- you know, the incentive -- when I worked at OMB, you know, we had a motto that, you know, to the effect of beatings will continue until morale improves. You may have worked in places like that. And so there are different kinds of incentives, right, so one of the things Larry mentioned is, well, we have incentives about liability, so you could be protected from being sued if you -- if you adopt security practices of a certain kind. Last I thought about it, you know, the absence of being sued was not a benefit, but it’s something that is definitely worth considering in the context of an overall framework. We don’t happen to have it in the Administration’s proposal, but that’s not because we’re opposed to it.

Procurement incentives, we do -- you know, that is part of the Administration proposal. It creates other effects. You know, there’s unintended consequences to everything so that has to be worked, but it’s something we’re talking about. The question about insurance, which of course is something that’s regulated at the state level in our country, is not something we’ve taken on at this point. Part of the problem with insurance is the lack of data. There’s no ability for companies, insurance companies, to write policies because they can’t do the actuarial analysis, so part of this transparency and disclosure piece could be helpful to actually promoting a more valid and viable security market.

And finally, on your point about reducing analog regulation, I’d be happy to hear about some of those, not necessarily now, but later, because we’re always trying to, you know, reduce regulations in the government, so that would be a good idea.

I would think that -- you know, the last point I’d make based on what we’ve been talking about so far is that although this is not primarily a technology problem, I think we're in agreement on that, you have been advancing the notion of data loss prevention, i.e. let's watch what's going out rather than what's coming in, ad part of -- you know, as a piece of the solution, and I think that is a technology that is part of the solution. It's easier to do on a homogeneous network where you know what's going on and one of the problems we face in the .gov, of course, is that we have a highly heterogeneous set of organizations and that kind of thing.

So, that is a technology with a lot of promise, but at the moment, I guess, at least my sense of the state of the art is it's still challenging and it is going to be the better, higher end players, that are going to be able to adopt that and perhaps bring the cost down.

MR. FRIEDMAN: So, let's drill down on this investment question a little more and talk about the sort of supply side.

So -- and Larry, you've been -- you're saying flowers.com, so let's compare flowers.com with missiles.com, and look to see, so, suppose there are incentives to invest in some measures. Are there general things we can say about the quality of information out there on the investment side? So, I tend to believe that there is a -- sort of a lemons market situation where because it is very difficult for venders to show that their stuff is different or, in fact, measurably better, everyone says our stuff does everything, and by the way, our stuff that we tried to sell you last year now protects you from that thing that's in the paper this year.

My favorite example for the market for lemons is, I don't know if you guys have seen the Trust-E seal as a way of showing that you're a good faith commercial vender. A study by a former colleague of mine up at Harvard Business School showed that you are more likely to receive malware from a site that has a Trust-E seal than from an arbitrary website. This is actually a bad signal rather than a good signal because, hey, we're just going to throw this out there and then see if it works.

So, is there a lemons market on the supply side that serves as an obstacle against firms who want to invest the money, who have the incentive to invest the money, of actually efficiently investing in security?

MR. MCCONNELL: So, I'm not familiar with the term lemons market, I assume that means you're selling bad cars?

MR. FRIEDMAN: Yes, exactly, it's (inaudible) model for essentially if you don't know whether the used car you're going to buy is good or bad, then if you have a good car to sell, you cannot get a good car price.

MR. MCCONNELL: I see, right.

MR. CLINTON: They didn't get the CarFax.

MR. FRIEDMAN: Yes, this is before -- this is pre-CarFax.

MR. MCCONNELL: Right, so this gets into how do you know if a product is any good, right, and so that's a whole other conversation about product certification or process certification, evaluation, who does that, and again, that costs money and who's going to pay for that.

MR. CLINTON: So, we are supportive of this as a role for our government partners and we have articulated this for quite a while. In order to put in -- again, what I'm arguing for is that we need to change the paradigm. I'm, in fact, arguing that the paradigm is changing anyway and we need to catch up with it, and we need to grow new roles and responsibilities between the public and private sector.

But there need to be roles for the government. We don't tend to think that a regulatory mandate role or an ability to review plans -- and I pulled out the language --

MR. MCCONNELL: We can review them. We don't review them ordinarily, but we have the ability to review them. If we have cause to do so.

MR. CLINTON: Well, the --

MR. MCCONNELL: Just to the point, if I can just make one point here. You know, this is a great -- it's great for us to have this debate here. The actual debate that needs to occur is the political one that will occur on the Hill and that's why we put this legislation out there so that we can exactly have that debate in full view of the public rather than in a small room and, you know, may the best ideas come out through the process.

MR. CLINTON: Absolutely. I'm all for it. But it does say that the secretary may conduct a review to see if the covered critical infrastructure meets the plan and then do several things including, C, which is take such action as may be determined appropriate by the secretary, which means the secretary can do whatever he or she wants --

MR. MCCONNELL: Whatever she is otherwise authorized to do. It doesn't authorize you to do anything you can't legally do.

MR. FRIEDMAN: This is an empirical question and what we'll do (inaudible) address it on the website.

MR. CLINTON: So, getting back to flowers.com. So, one -- so, we don't think that the government really -- the U.S. federal government should be in the position of setting mandatory standards for cyber security for a range of reasons -- they get outdated quickly, they'll be circumvented, et cetera, et cetera, et cetera. There's a lot of reasons why we shouldn't do it, but there are roles that the government should do and one of the things that we think the government should do is they should set up an entity modeled on the Semitech model that we used back in the '80s when we had a similar problem with computer trips, that is equal parts industry, government, and academic, to work on some of these problems, and one of these problems would be to set up essentially an underwriters laboratory for cyber security standards and practices, so their role would not be to create the standards and practices, we've got lots of people doing those kinds of things, but to evaluate the standards and practices for effectiveness and then these incentives I've been talking -- I talked about -- and by the way, there will be a sliding scale of these things, there's like an A level standard and a B level standard mostly associated with how much it costs. The incentives would then be matched up with the higher and lower degree of incentive. So, you may get a higher liability incentive, maybe immunity from punitive damages, you know, for adopting the A level incentive and you may get a B level incentive for liability, maybe the burden of proof has shifted somehow or whatever, according to these things, you get certain points on a government contract for the higher, less points on the lower.

So, we do need two things, we need somebody who is going to be the teacher and is going to do the grading. That person has to be independent. It can't be any national government because other national governments will compete for it, so it's got to be a recognized, independent sort of entity, and then somebody has to be providing the incentives for people who do the stuff that has independently been proven to work and that solves your lemon problem.

MR. FRIEDMAN: It's the CarFax.

MR. CLINTON: CarFax for cyber security.

MR. FRIEDMAN: So, the challenge there, by the way, is to make sure that you have a single independent unit. If you have multiple certifiers, then you have a race to the bottom, which you've seen in a number of other public certifications.

MR. CLINTON: What we're talking about here is what is going to qualify for the U.S. government incentives, and so what's qualifying for the -- now, if that becomes the standard for the world, so be it. We can be a market leader, I think that that's very progressive for our country. If we decide to instead outsource this to ISO, the International Standards Organization, I'm fine with that too, but we need some recognized body that shows not what is existing but what works, and then you tie incentives to doing what works.

MR. FRIEDMAN: Right. I think we'd love to hear some questions from the audience now. So, the caveat, as the microphone comes around to you, is to introduce yourself and where you're from and to remember that questions end in a question mark and seldom after a long speech.

So, we have one in the back corner there.

SPEAKER: Hi, I'm Paul (inaudible) from Booz Allen. Of the different like incentives maybe that I sort of envision that the federal government can do, which ones do you think are going to be like short-term, like six months to one year or two years, mid-term, like one year to three years, or long-term, three years to ten years? Like, and I would look at them as three different types. I think they match pretty closely to the DHS -- like, what is it, enable, require or do, and I guess the first thing is what I would consider like a carrot-like regulatory stance of basically liability insurance or procurement, and then the second would be maybe like collaborative, so maybe more of like direct pilots, that SNT and PPD are trying to promote or maybe a little bit less direct such as research with -- you know, research programs with different, like, research oriented parts of our federal government, like NIST or DARPA, and then I would say the third is the -- what I like, which is -- my preference, which is federal direct investments such as grants or, you know, like stimulus for programs that really -- you know, federal governments or NGOs or even, you know, institutes like Brookings can't really do but only private industry can really do that's innovative.

MR. CLINTON: So, let me take a quick swing at some of that. Yeah, I agree with you. By the way, both in the Cyber Space Policy Review and in the original IFA documents, they advocated tax incentives for cyber security among the incentives, and that's missing from everybody's proposal now because we're pragmatists, so I think you're going to have to wait a while for the direct grants, although I wouldn't be opposed to them personally.

Yeah, things like -- the things that probably can be done quickest are liability incentives and procurement incentives. I think that there's probably a good deal more work that needs to be done on the streamlining regulation. One of the areas, by the way, I would go to, Bruce, on that, is repetitive auditing requirements. I mean, we have -- if we could come up with a single, and it could be good, cyber security audit so that my firms are not doing multiple different audits which take away all their security personnel from doing actual security, by the way, and increase costs, that would be something that I think the federal government could do to streamline its own auditing requirements and then set that as a standard, but that's going to require a little bit more work and probably can be done in the Semitech sort of facility that I'm envisioning.

Another thing that is probably mid-term are the insurance issues, although I wouldn't put them long-term because I think Bruce is correct that there is a problem with actuarial data, but frankly, and unfortunately, it's not as big a problem as it used to be because there's been a lot more attacks, so we have a lot more data. The problem is, that data is not being shared. There are only a few carriers that have the data, so we're going to have to come up with some way to get the carriers who have the data to share it with the other ones who don't, but we can start a virtuous cycle by working with insurance.

The other, you know, that I'll just mention and I won't go into a great deal on insurance, is that what we really ought to have is the federal government -- and this is not probably any more practical than the tax incentive -- but what we really ought to have is the federal government recognizing their actual role, I mean, the role they actually have now, as the insurer of last resort. If they did that and acknowledged that if there was a cyber hurricane, they would come and they would pay the insurance claims, there'd be a lot more people -- insurance companies getting into the market because they know they have a backdrop, and you set up a revolving fund like we did with crop insurance and flood insurance in the past where eventually private sector money replaces the federal money. That's probably politically impractical, but the federal government has that risk now. I mean, if there's a cyber catastrophe, the federal government's going to pay for it just like they did with Katrina, and they're now not offsetting any of that risk to the private sector.

So, if they did that, that would tremendously stimulate the market. Some of the longer-term things like rewriting the protocols and stuff, those are further out.

MR. FRIEDMAN: Bruce, do you want to make an announcement?

MR. MCCONNELL: Just a couple things on that. I think, you know, if you're asking how long, you know, I mean, there are not very many short things we do in government -- short-term things, it takes us too long, so more medium- and longer-term, I think they all fall in that category.

Just a couple comments on some of those ideas. So, you know, the problem with flood insurance, of course, is it incentivizes people to build in the floodplain, so there's a problem with moral hazard here if we become the insurer, so you have to deal with that. It's not saying no, it's just like one of the things you have to consider. Similarly with the point of getting the companies to share with each other, the ISPs or telephone carriers to share with each other their security data, I think the last time we were together was with Ed Amoroso was also up here and he said that he would be happy for his competitor to fail because they had a security breach, that he had been successful in his firm to -- his telecommunications firm to protect against. So, again, in some places in the world security, better security, will become a competitive advantage and so you have to figure out how you don't create incentives for people just to lag behind and not take the risks because they're going to get the information anyway.

So, again, needs to be done but none of these things are simple and so that's why going back to, you know, what we have proposed with respect to, you know, taking some of the existing standards that are out there and suggesting to companies, the most critical companies, that we should follow them, is kind of a straightforward approach.

MR. FRIEDMAN: I would just add one point on the long-term incentives. I think one of the hardest components is going to be resilience through diversification and all of the incentives we have now inside networked industries takes advantage of -- it's called the Network Effect, Metcalf's Law, and the dynamic is moving strongly towards concentration across a small number of platforms, a small number of protocols, and I think especially for critical infrastructure, having diversity so that a local failure does not lead to a global failure or the attacker needs to learn to attack many different surfaces. It's going to be key. This also works against the strongest incentives we have in the IT industry today starting from cloud transition and going up.

Other questions? In the front here.

MS. GOODMAN: Hi. I'm Suzanna Goodman, I'm with

Common Cause in our voting integrity program, and I wanted to bring up an issue that is not usually part of -- you know, considered part of cyber security, and that is that close to half of the states allow electronic transmission of marked ballots. Voting -- basically voting over the Internet, allowing overseas and military voters and other voters to return their absentee ballots either, you know, directly, through e-fax, or something, through email or through a pdf program. And this sort of seems that it has fallen through the cracks of a cyber security problem and how to deal with it.

I would venture to say that none of the states and counties have the budget to protect against any kind of APT type of attack. They may be able to stop one or two of the kids in the basement, but not all, and, you know, we had an example of this last year, the D.C. Board of Ethics and Elections had a pilot where they were going to allow an overseas and military voting project. After a lot of objection from cyber security experts, they allowed a test period, they were very confident that they would withstand the test period, and it took 36 hours for a team from Michigan to break in and do all kinds of shenanigans and basically take over the server and shut it down.

So, this is a serious problem and there’s sort of no -- it’s not on the radar screen, and I just hope the panel can just, you know, give us some kind of grid and way of thinking about it and the genie is out of the bottle here unfortunately. I mean, you know, it's just -- it's happening and I would like to just say no, just don't do it. You don't have the protocol, you don't have the security to protect, but --

MR. MCCONNELL: So, it is on the radar screen and I would agree that there's a vulnerability there and if any of us who have all voted, you go to your local precinct, you can tell that there's no money in the electoral system, and, you know, so there's been a continuous -- I mean, it's not just the electronic voting, it's the integrity of the electronic counting systems and all that kind of things. I mean, in Virginia we've now gone back to the option of using a paper ballot, so I think this is very much in the radar screen. At the moment the electronic voting is, in most places anyway, limited to a small number of things like the military, but in this area it's very important -- it's all about maintaining citizen confidence and the last thing we need is for a lack of confidence in the integrity of voting results in the U.S.

So, it's very much on the radar screen. I agree with you, it's not traditionally thought of as a cyber security problem and one of the big problems in it in particular is the lack of investment and expertise in these small election boards, it's very localized, and there's a sensitivity as well for the federal government to be taking a hand in local election matters, so it's a complicated situation. But for the moment, anyway, I thought the D.C. experiment was very helpful to kind of slowing things down there until we get to the point.

MR. FRIEDMAN: I think this is an example of why the word cyber security works against us frequently. So, the field of computer security has been against electronic voting and Internet voting for a while. I did a lot of work on it in the first part of the decade when they were rolling out a number of systems and anyone who has studied these systems say it's a terrible idea.

Moving it to cyber security changes the framing and it leaves a number of important issues like this off the table. So, I think that's a great point.

Yes, the striped tie there.

SPEAKER: Thank you. The notion of liability got brought up a lot, and I was wondering (inaudible) panels here who might have very different ideas on this, but I was wondering what you guys, if you could (inaudible), how would you (inaudible) the liability and what standards would you use? Would you make it compliance based standard or just make it strict liability for (inaudible) breached and you pay for it and you (inaudible) some of the liability (inaudible)?

MR. CLINTON: Well, again, we think a new structure needs to be evolved for this. We don’t think the current structures are in place. What we’ve advocated, obviously, is that first of all you have to have this set of procedures that are worthy of the incentives, okay, and so then you would comply with that incentive.   And if you violate your agreement, we would know that when you have an event.

One of the things that we are trying to do is better use liability. As Bruce alluded to very correctly in his presentation, one of the big problems with liability -- people say, why don’t we just get tough on the software makers or the hardware makers -- is that these guys will point fingers at each other for decades and you will never get anything done. It took us ten years to figure out how to connect a cable wire and a telephone wire. That’s a lot easier than this.

However, if the liability -- if the penalty is not associated with the product, but rather the faulty accessing of the federal benefit, we do away with that. So, let’s say, you know, you have a firm and you say, you know, we’re going to comply with these standards and as a result -- you know, these proof standards, and as a result we are entitled to be -- you know, to have a lower standard of liability, whatever that standard might be, and then you have an attack. Well, then there would be an investigation of you and your liability would be -- and the penalty would be for falsely accessing the federal benefit, and so you wouldn’t be able to point your finger at anybody else. You accessed the benefit, so you are now liable.

MR. MCCONNELL: I'm sorry, I'm confused. The benefit here was lack of liability?

MR. CLINTON: Right. Right, and if you are -- if it can be shown in the investigation after your event that you did not actually deploy the standards, then you're guilty of a fraud.

MR. MCCONNELL: Okay, so you're both -- you have the basic liability plus you're guilty for a fraud, so there's also a criminal side in addition to the civil liability you would have presumably for being sued for -- I'm trying to understand that part.

MR. CLINTON: Well, we're trying to -- we're trying to put in place something so that he would actually deploy of the standards and practices. Obviously, if you can show that he actually did and he fulfilled his responsibilities, then he would get his liability benefit.

MR. MCCONNELL: We're interested in as many ideas in this area, so I'm just trying to understand that one, thank you.

MR. FRIEDMAN: To follow up a little bit, it sounds like, I believe, there is extant liability incentives right now.

MR. CLINTON: Well, as I say, you know, we don't think we have the structures in place, that's the first thing that I said. And as we do this, we would have to do a review of what the actual liabilities are. But there clearly are some liabilities that are in place. It is an unsettled area of the law, I would have to say, so we would have to make some decisions about that.

MR. FRIEDMAN: I would argue one place to start is to look at, rather than systems that were broken, bad decisions that were automatically made, so this is going after some of the intermediaries in the financial sector, in particular, that make decisions to grant new lines of credit, approve transactions, this is already built into the credit card payment system. I think it needs to be pushed out into the non-banking payment sector as well.

Yes?

MR. SADER: My name is Daniel Sader. I'm with Global Green U.S.A. I was hoping you'd be able to speak to the balance between the cyber security issues and the economic benefit of the evolution of a smart power grid.

MR. FRIEDMAN: That seems to fall under DHS.

MR. MCCONNELL: Well, so we're not deploying the power grid, but we are interested in the problem. Obviously we want the power grid to be secure and so the smart grid has the potential of being secure because we're building it now from scratch so we can build the security in.

I think there's increasing awareness about the importance of doing that, so I think we are -- have a good chance of catching that potential problem in the early stages.

As to the economics of it, of course, you know, as with all this we've been discussing, hard to measure exactly what's the potential effect, what's the downside, how much is that, and how much do you have to invest to protect -- you know, how much, therefore, is it worth investing to protect against it. Since we have no -- it's a new system, if you will, we have no empirical data about that so that making that tradeoff is hard, but I am pleased by the amount of awareness that there is going into that question at this point where as originally the discussion of the smart grid was just like, oh, it's going to be really cool that I can turn off my refrigerator from my office -- or turn it on.

MR. FRIEDMAN: I'd like the use case for that one.

MR. MCCONNELL: I'll turn off your refrigerator from my office. Sorry, really sorry.

MR. FRIEDMAN: Smart grid?

MR. CLINTON: No, we agree that smart grid is a great theoretical idea and there are enormous security issues that are a long way from being solved and the economics blend in, but it's a great idea.

MR. FRIEDMAN: A question on the aisle here.

MR. WALKER: My name is Jim Walker. I'm retired --

MR. FRIEDMAN: We've got a mic right next to you.

MR. WALKER: Jim Walker, I'm retired but I'm boards of directors. I'm trying to relate what you're saying to something I can identify with. Are you saying that we really need to hold companies to the prudent man theory, which is prevalent in boards of directors, but we don't have the basis of law set as we do in corporate directors?

MR. MCCONNELL: I think that's right. I mean, I don't think you have any lawyers up here so we're not speaking as lawyers, but it is the question of what's the standard of care, what is normal to be done in this case, and those standards aren't -- I mean, the standards are there, but the case law and the regulatory regime ahs not -- or the underwriter's lab -- has not empowered them in a way that allow predictability about, you know, I have to do this in order -- because it's common practice to lock my doors of my factory, and that kind of thing.

So, because that's not clear and explicit, it's more difficult to be able to know what it is to do to meet that standard.

MR. CLINTON: Yeah, I think what we're talking about is the fact that we believe that organizations, enterprises, private sector enterprises, may need to be growing new responsibilities in this cyber security world, so the standard of prudence -- and I'm not a lawyer, so, you know, I don’t want to be off base here and I appreciate Bruce’s caution -- may need to grow. The responsibility, you know, I mean, short form, for most enterprises is to maximize shareholder value. They’re supposed to be making money for their shareholders, and what we are talking about is that there may be -- and so because they maximize shareholder value, they tolerate a level of insecurity that probably Bruce’s organization can’t tolerate. If you’re Wal-Mart and, you know, 10 percent of your inventory is walking out the back door every month, that’s okay with you if you’ve done a study that shows it would cost you 11 percent to hire the guards and put up the cameras, so you have a higher tolerance of insecurity, and that’s okay because it’s just you, it’s your board, it’s your company, you want to tolerate the insecurity, it’s your business.

In the cyber world, your insecurity could be vested on me and could be vested on the nation as a whole, and so what we have argued is that the private sector may need to grow less risk tolerance, but in order to do that on a sustainable level, the return from our public sector partners is going to have to be some sort of economic remediation to make that in your business interest, because we want you staying here and operating in the United States, we don’t want you going offshore because you don’t like this new regulation or whatever.

So, that’s the new sort of standard that we need to come up with. So, you will need to be doing new things, but you need to be compensated for those, otherwise it's unsustainable.

MR. FRIEDMAN: I also want to highlight a point that Larry made earlier which is treating this as part of the organization's basic risk framework. There's a study that came out of CMU that -- and I have my own issues about it that we can talk offline about, but I think it's an excellent starting point for understanding corporate governance in the face of cyber risk.

Question in the back. Yes.

SPEAKER: Could you speak a little bit about ISP liability -- ECPA put certain responsibilities on ISPs and much of the mischief that goes on is at the ISP level. You've been speaking a lot about defense contractors and others, but what should ISPs be thinking about here?

MR. CLINTON: Well, I have one ISP in my membership, so I don't really speak for the ISPs. We have a lot of people but not them broadly, so obviously we use the ISPs.

I think that there's a lot of work that needs to be done to get them to share information amongst themselves, as Bruce was talking about before. I'm kind of surprised by the chairman of AT&T's comment because my understanding -- and AT&T is not one of my members -- my understanding was that they are becoming more interested in sharing this information rather than looking at it as a market differentiator. But clearly, you know, the vast majority of traffic goes over the ISP networks and if we can find some way to engage them better, I think that, you know, we can probably make a lot of progress pretty quickly. We're going to have to do it in a way that is -- that works for them as their business model and that, you know, that's the problem.

MR. MCCONNELL: So, on that point -- and I think you're right, I agree that they are -- I mean, I made kind of an extreme comment, but, you know, there's a lot of sharing and cooperation that goes on.

But I would say that -- two things, your point specifically about the Electronic Communications and Privacy Act does allow -- puts requirements on them and this is about monitoring -- this gets into the question of monitoring communications -- so, it allows ISPs to monitor traffic if -- for the purpose of protecting their own network. So, this is their property and if there is traffic that's coming that's got malware that's destine to attack their switches or something like that, they're allowed to do that. It doesn't allow them, however, to necessarily share what they've learned with the government because that creates potential -- you know, there's a concern that creates potential privacy issues, so that gets into a complicated balancing act there and in the pilot program that we're doing with some of the defense companies where we're working with the ISPs who are monitoring the traffic that's coming into the defense companies, you know, we had to do a fairly extensive legal analysis to provide comfort that it was legal for them to do this, so that's one of the areas. Where most of the conversation today has actually been about, you know, we haven't talked about it this way, but it's true that better security can mean better privacy, but there are places where some security techniques can have a potential negative effect on privacy, and so that -- you know, you can kind of get that tradeoff issue there.

So, I think the bottom line of that is that, you know, it's very important to work with the ISPs. They can kind of do it wholesale but, again, we talked about government providing incentives, you know, to remediate, you know, to offset their costs, but it is possible that some -- and some ISPs are doing this now -- they're offering security as a market differentiator. You can buy, you know, if you want more secure networks, you can buy our platinum service which has more security, it costs more, and that is a way for the market to work without the government intervening, and so obviously that would be preferable, but it may not be enough to get at the large threats.

So, those are the pieces that we have to try to get right or we'll be going in the wrong direction.

MR. FRIEDMAN: So, just quickly on this point. I think there are some cases where the incentives align, for example, malicious behavior that involves packet floats for denial of service attacks. There are ISPs that have now said, hey, listen, this involves me sending lots of traffic to other networks, that's a cost for me. So, let's collaborate and understand how we can sort of pool information, identify things as they're coming on, do ingress filtering, egress filtering.

You have this monitoring idea at the customer level and there you have the challenge of how to overcome the cost of customer service. The number that floats around is that one call to a customer's ISP basically kills between two and four months of their profit on that customer. And then finally you have the question of actual infrastructure implementation, so DNS security or IP Sec, those benefits don't necessarily accrue explicitly to the ISP unless everyone adopts them. So, there's one of these network effect things.

We have time for just one last question, sitting in the back row, and -- yeah.

SPEAKER: Yes, I just want to ask whether or not the car industry has any kind of application here. In order to drive my car on the road I have to get it inspected, there are standards that it has to meet, the breaks have to meet standards, I have to get the exhaust checked periodically. If, as you indicate, industry, the government, and academia got together to set best practices or standards, is there any modeling from the car industry in the way that if I drive a car on the road, I could crash into someone else, there's insurance that's available to spread the risk. Is there any modeling from that that can be used in cyber security in the area that you're talking about?

MR. FRIEDMAN: So, this is for -- Bruce, explicitly says there will never be an Internet drivers license.

MR. MCCONNELL: Well, I was going to say, yeah, and you need a license to operate one, right? Except if you're just on your farm, you don't need to -- you can drive your tractor on your farm without a license, but we're all connected here.

So, these analogies are really great. I think they really help us think about -- there's another one about the air traffic control system, you know, which is kind of good also, and you have the certification of products in there, you know, air worthiness directives, there's a very rich regime around all that. And there's no -- I think all those tools and things are worth looking at. What to me is -- it points out that we're at a very immature stage of this today and if you look at what it took to get automobile safety standards to come about, it took years. And, you know, seat belts and drivers license and emission controls and all that kind of stuff, you know, years. We don't have years here so we have to figure out how to get a richer environment.

But I think it will, as this matures and becomes more of a part of everyday life, we will end up with some kind of regime that looks a lot more like that or the air traffic control and air worthiness stuff, than we have today. We're just not ready yet to do that and that's what we've been talking about is what do we need to get that balance right between the market and the government, because we don't know exactly where that is.

MR. CLINTON: Yeah, there's one major -- I mean, I think there are -- I agree with Bruce, you know, you can draw some things from this. We already talked about the need to involve the insurance market, for example, and that's one of your models, but I think that there's a fundamentally -- a fundamental difference that I really want to emphasize. Nobody's attacking your car, okay? Most of these attacks -- this is not an instance of defective products or corporate malfeasance. That's like saying that the problem with the World Trade Center was that they didn't follow their building codes. The problem with the World Trade Center is that they flew airplanes into the buildings. That's what's happening to our cyber systems. They are under attack.

Remember the incentive model? There's all these incentives to attack these things, so what we have to do is realize that this

-- sure, we need, you know, basic good standards to make the things work and as I've talked about before, we're trying to build those in, for example, with the mobile devices, et cetera. So, obviously that needs to be done, and Bruce is right, things will grow and mature. This is very new stuff. We don't realize it because it's so ubiquitous now, but it's very new.

But we have to understand that we shouldn't be blaming the victims here. You know, these are organizations that are under attack and they are helping us all to have this cohesive and ubiquitous system, so we have to broaden the perimeter of security, we have to secure everybody out, but we have to do it in a manner that is sustainable, both technologically and economically, because if we take the economics out of the equation, which is what we've been trying to talk about, we miss it, and so that's the difference between your cars.

MR. FRIEDMAN: I just want to point out one more similar -- I have one more interesting point, is the auto manufacturers bitterly fought many of the consumer safety regulations and now they are a major driver in the competitive marketplace, so the unknowns also mean that sometimes these can actually work out for the benefit.

So, last words before we wrap up? Do you have final thoughts on what is one takeaway that you think people need to understand?

MR. MCCONNELL: So, I guess the only takeaway I have is that, you know, the -- as -- this is a fun problem to think about, it's very complex and one can spend a lot of time admiring about it and worrying about it. We have -- you know, we are proposing some things to do and we -- I encourage you all to get involved in the conversation about whether those are the right things to do or not, but, you know, we do need to get some things done here in the short-term. And it does, I think, involve some kind of greater role for government than we have today to set the -- to make the markets work more effectively. So, in that -- from that standpoint, you know, the more brains we can put on this, the better.

So, thanks for being here.

MR. CLINTON: I would certainly agree. It really is a fun topic, I love my job, but I think that I would really emphasize that we need to be thinking of this not as, you know, what is the other guy doing that, you know, he needs to be beaten up with. This really -- we are an interconnected world and we need to be doing this in partnership. We need -- and particularly between the government and industry. And there are indications that that partnership is fraying. And I think that that's going in the wrong direction.

I would agree that there are more things that the government ought to be doing and there should be a role, but it has to be the right role because there are, as Allan just pointed out, there are unintended consequences to some of these things and we're dealing with an issue of national security, so if we do something legislatively or whatever, we need to do something that is right and that works, and I think that that needs to be done through the public/private partnership, as articulated in the NIP and not fundamentally change the model to a more regulated, regulator model. I mean, the one thing that, you know, to get back to the legislation and the legislative proposal, you mentioned, Bruce, that the meetings between industry and government under the proposal would be collegial, I think was the term you used, and I really think that's very optimistic. I've worked for regulated industries and the relationship between the regulator and the regulated tends to be minimalistic, legalistic, and antagonistic. That is exactly the wrong model, I think, for cyber security awareness on a sustainable basis.

MR. FRIEDMAN: All right, so, on that note I'd like to thank Bruce and Larry and thank you guys for spending your morning with us. This afternoon at 3:30 we're going to be having a session on privacy. That's all for now.

(Applause)

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

/s/Carleton J. Anderson, III

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2012