FEDERAL TRADE COMMISSION

I N D E X

WELCOMING REMARKS:	PAGE:
BY TIMOTHY J. MURIS, CHAIRMAN, FTC	4

PRESENTER:	
DICK CLARKE	10

PANEL:	PAGE:
I	35
II	118
III	153
IV	190

FEDERAL TRADE COMMISSION

In the Matter of:)
CONSUMER INFORMATION SECURITY)
WORKSHOP)
---)

MAY 20, 2002

Room 432
Federal Trade Commission
6th Street and Pennsylvania
Ave., NW
Washington, D.C. 20580

The above-entitled workshop was commenced, pursuant to notice, at 9:05 a.m.

P R O C E E D I N G S

MR. EICHORN: We're getting a little bit of a late start this morning ironically because of security downstairs, but we're ready now, so let's roll on.

I just have a few brief announcements. On the mundane side, in your packets you'll find order forms for sandwiches from the cafeteria upstairs. If you're interested in pre ordering a sandwich, you can fill out that form and pass it to the end of the room, find me or some other staff and hand us that form, and we'll make sure that you have a pre ordered sandwich.

Also, as many of you have already discovered, there's no coffee outside, but there is coffee upstairs on the seventh floor in the cafeteria, so if you need coffee at any point, it's right off the elevator bank.

Also I would ask that you all turn off your pagers and phone ringers just as a reminder.

In our workshop today, we're going to be having questions from the mike here at the end of each panel, so if there are people in the overflow rooms who want to ask questions, we ask that you come up to the room at the appropriate time in the panel. The moderator will indicate that people can come up for questions, so if

you're in 532 or 332, you might want to come up here.

Also, the record for this workshop is going to be open for another month, until June 21st, so if there's any comment that you want to get into the record that you want to provide to us, we would be happy to receive that. You can email those to us at Security underlined Workshop at FTC.GOV.

At this point, it's my pleasure to introduce Chairman Muris.

CHAIRMAN MURIS: Thank you very much, and welcome to our workshop on consumer information security. We're here today because information security has become not just a business issue, but an important consumer issue as well.

Computers are black boxes for most people. Their workings are a mystery. Unfortunately, for too many, that same sense of mystery extends to the threats that exist. Too many consumers learn about security the hard way, after they've set loose an email virus in their system or their computer has been taken over and used in a denial of service attack.

I want to thank you for coming to help educate us on these issues. I especially want to thank our panelists who traveled from near and far to be with us.

We've lined up an impressive groups of experts to discuss the current state of consumer information security, as well as new and emerging ways to improve that security.

Because the audience will also ask questions, we look forward to learning not only from the panelists, but also from you.

I believe in the value of information. The average American enjoys access to credit and financial services, shopping choices and educational resources that earlier Americans could never have imagined.

Today we can check our credit card and bank balances over the phone 24 hours a day. We can order books, clothes or gifts online while we are having our first cup of coffee in the morning, or we can review our finances in a convenient, consolidated statement whenever we like.

Even with the decline in Internet stock prices, the impact the Internet has had on our economy is hard to overstate. The free flow of information that computers and the Internet make possible is of enormous value. We marvel at the ways that the computer and the Internet have changed how Americans live, work and play.

With the enormous benefits have come new

challenges. Instead of lions, tigers and bears, there are viruses, hackers and worms. The destruction theft or disclosure of consumer's data are serious problems. Sure, consumers use their computers to email jokes and play Solitaire, but they also use them to store sensitive information such as passwords, financial records and health data.

Just cleaning up a virus infected computer can be time consuming and expensive, and as ever more powerful computers get hooked up to broadband Internet connections, the potential consequences from security incidents grow.

Consumers' security affects everybody. When hackers harness many computers together to attack a particular target, the operation of the network as a whole is affected.

Many businesses, such as small ones without full time systems administrators, face the same security challenges that consumers do. Businesses as a whole hold more information in their databases about consumers than consumers hold themselves.

Thus, the security of businesses that maintain consumer information, whether that information was originated online or off, is an important consumer

issue. Businesses that transact with consumers online have another reason to care about security. B-to-C e-commerce would suffer if consumers were to lose confidence that they can transact safely online.

To educate ourselves about these issues and to see what role we might be able to play in encouraging strong but workable security practices, last October I publicly raised the idea of having a workshop on security. Since then Commissioner Orson Swindle has taken the leading role in making this workshop happen.

Many of you know that Commissioner Swindle has been heading the U.S. delegation to the working group that is advising the OECD security guidelines. Tomorrow morning he will be speaking to you about that process.

Many substantive issues that the Commission is currently working on involve security. For example, we just issued a final rule to implement the safeguard aspect of the Gramm-Leach-Bliley Act. The rule requires, among other things, that financial institutions covered by the rule establish and maintain an information security program to protect their consumers' personal information.

We expect to issue educational materials about the rule for consumers and businesses very shortly.

We're also working to reduce identity theft, which is the leading source of complaints made to the Commission's Consumer Sentinel database. If a database holding consumer's personal information is not secure, it is easier for a hacker or disloyal insider to gain access to that information to steal someone's identity. And we're working hard to make sure our own house is order.

Here at the FTC, we've been going the extra distance at all levels of the agency to put tighter security procedures in place. Last month I sent a memorandum to all of our staff stressing the importance of information security to the Commission's mission and launching a new security program.

We're upgrading our equipment and infrastructure. We're developing security plans for all major systems and applications. We're initiating internal and external audits to assess our program. We're strengthening password requirements. We're going to be briefing all staff, not just IT personnel, annually on computer risks and threats, and we'll be teaching best practices for home computers. We believe that practicing good security at home will carry over to work.

These efforts parallel those being made all across government agencies to make cyber security a priority.

It's my great pleasure now to introduce the person who is leading those efforts on behalf of the administration.

Dick Clarke is the President's special advisor on cyber security issues, and chairs the President's commission on critical infrastructure protection. Like Tom Ridge, Dick has the formidable task of coordinating numerous agency security efforts, as I understand it, 23 different federal agencies.

I want to highlight just a couple of the issues on which Dick is working. He's formulating the national strategy for cyber security, a multi pronged strategy to improve the security of government agencies, businesses and consumers.

Another issue is consumer education. Dick's team has been very active in working with the private sector to get security information to consumers. Many of the organizations involved in the effort are present here today.

Before his appointment as special advisor to the President, Dick served as national coordinator for security infrastructure protection and counter-terrorism

on the National Security Council. As national coordinator, he led the U.S. government's efforts on counter-terrorism, cyber security, continuity of government operations, domestic preparedness for weapons of mass destruction and international organized crimes.

In the George H. W. Bush Administration, Dick was the assistant secretary of state for political military affairs. In that capacity, he coordinated State Department support for Desert Storm and led efforts to create post war security architecture.

In 1992, General Scowcroft appointed Mr. Clarke to the National Security Council staff. He continued as a member of that staff throughout the Clinton Administration.

In the Reagan Administration, Dick was the deputy assistant secretary of state for intelligence.

Dick's a career member of the senior executive service and began his federal service in 1973 in the Office of Secretary of Defense. I think you can see he's extraordinarily well qualified for his current task.

Dick, welcome.

(Applause.)

MR. CLARKE: Thank you, Tim, and thank you all

for coming.

I want to really thank Tim and Orson for putting this together because we see this two-day workshop as part of the national outreach effort that we are making as we develop the national strategy that Tim mentioned, the national strategy to secure cyberspace.

The President wants a national strategy, but he doesn't want it to be written by a bunch of bureaucrats who have worked in the Reagan Administration and the Bush Administration and the Lincoln Administration.

He wants it written by and with the public, and that's a unique challenge. How do we get the consumer, how do we get the enterprise operator to think that this is her problem or his problem to the extent where they feel that they need to help us draft a national strategy.

Today's meeting is part of a series of meetings that we're having designed to get public input, and we thank the FTC for setting up a mechanism where there will be an opportunity for public input.

We're also having town meetings. We had the first town meeting last week in Denver and next week in Chicago and then Portland and then Atlanta, again to ask people to think about the problem as part of our

awareness effort, but also to ask people to tell us what they think on key issues before the strategy is developed.

The other part of the openness and transparency of the national strategy is that it will be online. Sections of it will be written by the interest groups themselves. The section on how we secure the vast computing powers of American universities will be written by American universities.

The section on how we secure the banking and finance sector will be written by the banks themselves working together and so on throughout all of the key sectors of our economy.

The strategy will also be one that can be quickly changed. It has to be capable of living in Internet time and changing on Internet time, so that when we see the threats change, so that when we see that what we're doing isn't working, so that when we get new ideas after it has first gone online, it can still change and adapt. Our goal is to put the first strategy online before the end of the summer.

The topic today deals with privacy and deals with the consumer. Our strategy envisions five levels and policy at five levels, beginning with the global

level, global policy. Orson Swindle has been working with OECD as part of our international effort.

The fourth level counting down, the fourth level, national level issues such as what's our research agenda, what awareness program should we have, what education program should we have.

The third level involves the work of the various sectors of our economy like banking and finance, like transportation, like electric power, what should they do together.

The second level is what should be done at the large enterprise, how do you secure a big company.

The first level is the topic we're dealing with today, and that is what should be done to help the average consumer, the home user, and the small business?

This is a new thought. In the past, national plans and activities focused on cyber security have not focused on the average home user, and most of us, whether we work in banking and finance or the government or the press or academia, are home users, and there are important questions, which we need to address as we put this national strategy together.

Let me suggest some of them. I know many other

speakers here are going to raise them over the course of the next two days. Particularly since I see so many familiar faces in the audience, I know these questions are going to be raised, but nonetheless, let me suggest a few for you.

How can the home user without knowing it hurt other people? Tim mentioned distributed denial of service attacks, and we've seen that happen already. This is not a theoretical possibility where the home user, without knowing it, has their computer attacked.

Their computer is then -- a part of their computer is then covertly taken over by an automated program, and it sits waiting for instructions or it sits waiting for a time, and then when that time comes, it launches what's called a distributed denial of service attack, firing messages out many times a second, and it does it in concert with hundreds or thousands of other computers, and those messages from all of those computers are aimed at one site on the Internet.

The effect can be that that site closes down under the volume, that the routers and the servers crash under the wave.

Last July we had a similar experience, it was called Code Red where servers, not home PCs, but servers

were infected. Tens of thousands and then 20s of thousands of servers were infected by a virus that became a worm, and on signal it was going to attack one web site.

And as we became aware of tens of thousands, 20, 30, 40, a hundred thousand servers being infected, and we could watch the number go up by the hour, we worked in the government and in the private sector together as a team to try to figure out what to do.

The first question was, whose web site was it that was going to be attacked by this massive denial of service attack, and when was it going to occur. About four o'clock in the afternoon, I got the news, I was going to say the good news, but I got the news whose web site it was going to be. It was mine, that is to say, it was White House.GOV. And when was the attack going to occur? Four hours later.

We thought about that and said, Well, you know, maybe the White House web site will just come down for repairs this afternoon so we won't actually be knocked off and be embarrassed. Then we thought a little bit more. The White House web site wasn't the point.

The point was that a massive tsunami of that scale coming down the Internet, going toward one site

would knock off routers and switches as it came down the Internet, so it would damage much more than just our ability to put up the daily press briefing on the White House web site.

And so working together with the private sector, with government agencies, quickly scrambling between four o'clock in the afternoon when we figured it out and eight o'clock in the evening when it was supposed to occur, we developed a strategy, and that strategy was to go to the Internet service providers, the big ones, and say to them, Block traffic coming to us, not at the core servers but at the edges of the Internet.

Well, you might imagine the reaction when you pick up the phone and you call one of the large ISPs and you say, Hi, I'm from the White House, I want you to block all traffic to the White House. It took a little bit of persuading, but by eight o'clock, all of the major ISPs had not only agreed to do it, they had done it, and they had blocked all traffic to that IP address at the edge servers, and when eight o'clock came, virtually nothing happened.

That tsunami did not occur, and that denial of service attack was not successful, but that's one of the big ones that you hear about. In point of fact, denial

of service attacks occur every day. There are hundreds a month aimed at all sorts of different sites all over the Internet and all over the world, and many of them are happening because the home consumer hasn't been told how to prevent his or her computer from becoming a zombie. Many people don't even know when their computer has become a zombie.

How else can the home consumer hurt other people? If you work at home, as more and more people do, or if you are forced to work out of a hotel room when you're on the road, as more and more people are regrettably forced to do -- we used to play tennis and swim in the hotel pool, now we're online all the time -- you can hurt your company by doing that.

Sometimes you want to hurt your company when you're doing that, but without intending to because your home PC or your laptop that you take on the road can be infected with a virus or a worm, and when you connect to your office, sometimes you connect through what's called a virtual private network that allows you to go in securely behind your company's firewall.

Well, that's good, isn't it? It's a secure connection. Yes, the connection is secure, but the PC from which you're operating your laptop in the hotel

room, your desktop at home, may not be secure, and what you have just done is established a secure net that allows a virus or a worm or a back door to move unchallenged through the firewall of your company and into your company's network.

Because? Because you didn't have the latest anti virus software. You didn't have the latest patch on your operating system or application. You didn't have a firewall through your home system, and your company didn't require that you do, or if it required it, it didn't have a way of verifying your software was up to date.

It's a little more obvious how home users can hurt themselves. They can hurt themselves by leaving credit card information and other identity information on their hard drives and then again not updating their virus software, their operating system software, and if they have a cable modem or if they have a DSL line, not having a firewall.

I checked the other day a list of about ten providers of DSLs, and I found only one of them that in the course of saying, We offer you a DSL service, mentioned that, Oh, by the way, you ought to get a firewall.

It's strange. It's a bit like offering someone

a car without an airbag or seat belt, and yet almost every DSL provider with a few exceptions, almost every cable modem provider with very few exceptions will provide you that connectivity and say, Go for it, without ever telling you that by having a constant connection, by having a static IP address, you are enormously increasing the chances that your computer will be attacked, and if you don't have a firewall, almost ensuring that your computer will be attacked.

So what should consumers do? Should they go out every day to a web site and check for the latest virus software, for the latest fix to their operating system, for the latest fix to their firewall? It's a lot to ask.

Now, some operating systems, some very common operating systems in their latest version do offer automatic updates. There are questions there about whether or not you want someone doing automatic updating. It's a question about how you know what you're really downloading when you get that automatic update.

Some virus software, in fact most of the major providers now offer automatic updates, but should it be so hard? Should we put that much burden on the

consumer? Should we ask them to worry about all of these things, or is there a way in which we can encourage Internet service providers, perhaps by charging a premium, to offer secured service?

Frankly I think if most Americans were offered the choice of connectivity for $20 a month without security features and $22 a month with security, I think almost everyone would go for the $22 a month, and yet that offer isn't there for most Americans. Most persons cannot pay a little more and get their ISP to do that work for them.

The ISPs can send you a firewall when they give you a DSL connection or cable modem. They can scan the software that you use to see if it's up to date, if you allow them. They can automatically provide you updates for common applications. They can make sure that your anti-virus software is updated.

You really shouldn't have to worry about that all yourself, but today you do. Most Americans are even unaware that they need to do these things, so one of the things that's already become very clear to us in developing the national strategy is that we must give a higher priority to national awareness.

I see many people in the audience who have

helped us already by creating the National Cyberspace Security Alliance, companies, NGOs like SANS and others, have helped us to put online a very helpful site called StaySafeOnline.INFO. For those of you who haven't seen it, I urge you to go there.

It's designed for the home user to tell them how to secure their systems and how to get even more detailed information if they want it. It's also designed to help the parent who worries about letting their child online at an early age.

I knew children were getting online at an early age, but I didn't know how young until a week ago Saturday when I saw a young girl, who's not yet three, while I was talking to her parents, walked over, turned on the computer, went, found the CD, put it in and got up on the chair and started using the mouse and playing with her CD, not yet three years old.

That's great, but it also means that she can do it when her parents aren't around, and it also means that having parents know about safety and parental controls is becoming more and more important all the time.

The other topic for this two day session -- in addition to the issue of what the consumer needs to do,

the other topic is privacy, and many people have said to me, How are you going to reconcile the requirements of security on the Internet with the requirements of privacy, and one of the questions that we put for national discussion is to achieve IT security on America's critical infrastructure, do we need in any way to modify privacy rights.

I already know the answer to that, and it's no, but I want that issue discussed, and I think it would be a big mistake for us to develop an IT security strategy for the country without spending a lot of time as American citizens together talking about privacy rights and our desire to maintain our privacy rights and to not have them infringed as we increase security.

To me, privacy and security online are two sides of the same coin. It's absolutely impossible to achieve privacy without good IT security, and unfortunately, what we're seeing all across the country is that privacy information is being stolen because institutions are not practicing good IT security.

I spent the day Friday at a major university in the Midwest that told me of multiple incidents across the country where Social Security numbers and other information has been stolen at universities because

until now universities have thought that IT security was anathema and somehow an infringement on academic freedom. Well, not anymore.

Enormous computing power exists on university campuses, and students need to ask and professors need to ask of their university what is being done by that university to protect their privacy rights.

One of the questions that has become popular in the last six months is do we need a national identity card, and I also know the answer to that. No. American people, even in the wake of September 11, in all the polling data, a large segment of the American people say they don't want a national identity card, and I don't think we need one, but we have to be careful in saying no to a national security card that we don't say no to user identity cards.

One of the ways that we can enhance security on government systems is by having better identity cards for government employees. The Pentagon has been pioneering this with something called the Common Access Card, that is an identity card with biometric information on it that gets you into a defense department building. It has a building pass, an electronic building pass, and then also allows you to

log on to a computer.

Without that card, you can't log on to the computer, and with that card, you can be assured that the person's whose name is logged on is, in fact, the person to whom the card was issued because it requires biometric two source authentication.

It seems to be working. As with any large program -- already over two and a half million have been given the card. As with any large card, there are some initial start up problems, but it does seem promising, and we do need to ask whether or not security in general, including privacy, at government institutions could be enhanced by taking that kind of two authentication smart card and requiring it as a way of logging on to government systems, if you're a government employee, either at work or at if you're telecommuting.

Security also raises the issue of anonymity. So much of the security violations that have occurred on the Internet have occurred by people who are anonymous or who have spoofed their identity or who have stolen their identity, and it does seem to me that we need -- while we embrace privacy rights, we need to ask if there's a distinction between privacy and anonymity and whether everywhere on the Internet is a place where you

should go anonymously or whether there are large sections of the Internet where we need to prevent anonymity.

Certainly there are some places where it doesn't matter, but there are lots of places on the Internet where anonymity is a great risk to security and to privacy rights. I'm anonymous when I go to my county library and wander through the book stacks, and that's fine, but I shouldn't be anonymous if I go to the county hospital and wander through the medical records. That's not fine.

We need to make that distinction, and we need to find ways of ensuring that when you are on a web site or part of a network that has sensitive information and privacy information, that you are not anonymous or that you are not spoofing your identity.

There is another way in which security can affect all of us, and it's when we do business with a company or an institution that does not maintain security. How do we know that when we provide our information to a company or an institution, that it is living up to some set of good practices for IT security?

Typically we don't. If we do commerce online,

we may be able to see that the web site is using some sort of encryption. We always look for that little lock on the bottom of the web site before we put our credit card information down.

Of course, I'm told it's rather easy to have a little lock on the bottom of your web site whether or not it's a secure site, and sometimes we look for the name of a particular IT security company that is guaranteeing the security of the transaction, and with that we feel secure, and the transaction is secure, but after the data goes into the database, that may not be secure.

The information that you have seen on the web site says that your session, your linkage to the company is secure, but it doesn't tell you anything about what that company's IT security practices are. Online banking is a great thing, and you can tell frequently if the web site is secure, but you are, for the most part, unable to determine whether the bank has good security practices.

There are no disclosure requirements. There are no disclosure requirements about whether or not the bank or other institution with which you are dealing with online has been hacked. How often has it been hacked?

How badly has it been hacked? There are no disclosure requirements about what its IT security practices are. Who is the chief IT security officer of the company? How much money is being spent as a percentage of revenue or as a percentage of the IT budget on IT security?

When was the last time the organization, the company had an outside vulnerability assessment? Were the findings of that vulnerability assessment rectified? These are things that you might want to know.

When we dealt with institutions online prior to the Y2K roll over, we were able to find out whether or not the institution we were dealing with was Y2K compliant, and most of us, in our monthly bills, got long statements in small type face telling us something about Y2K compliance from our credit union or whatever institution it was we were dealing with, but you don't get that today with your monthly bill or your stock information if you happen to be an investor.

You are largely left in the dark as an investor or as a consumer about the security practices of the organizations with which you deal.

We all know that IT security is complex, but there must be some simple statement that can be made

about compliance with some set of best practices. I don't think the government should write those best practices. I think industry groups together with consumer groups should get together and establish some notion of what best practices are for certain kinds of companies.

But I do think somebody ought to provide some list, some criteria for evaluating, if I'm going to do business with a company, whether or not that company is, in fact, secure.

These are all issues that we intend to address in the national strategy. They're issues I hope you address today and tomorrow and on an ongoing basis as we develop the strategy, as we get it online and as we continue to modify it.

We look forward to these two days. We look forward to your input because it's vitally important to us as a country that the IT revolution continue, that we go into the next stage of that IT revolution, and that we realize all the economic and social benefits that will come when we move to the next step up the ladder of IT deployment across the country, but as John Chambers said in December, CEO of CISCO, we will not get to that next step on the ladder of IT deployment unless we can

achieve IT security.

Thank you very much.

(Applause.)

MR. EICHORN: We do have a few minutes for questions. If anyone has questions, you're welcome to come up to the mike.

MR. ABRAMS: My name is Marty Abrams. Do you have any thoughts about whether user IDs should be used on home computers to assure better authorization and authentication when dealing with sites?

MR. CLARKE: I think if you're dealing with a site online where you want to have high level security, not just on your end, but you want to know that the organization when it deals with other people are also secure. You know when you log on, but you're you, and therefore you think, Why do I need to have some sort of smart card to prove it.

It's not because you would abuse the system. It's because the next person that logs on and says it is a customer might abuse the system, so I would feel safer personally if I were doing business with a company online and it did ask me to use some sort of smart card because then I would know that no one else is going to be able to log in without having their identity in some way

verified.

I think that increases the chances that the overall system, the overall network that you're connected to, won't be compromised, and since you're probably providing that network with privacy information, with financial information, you want it secure all the time, even after your session is over.

MR. CLARKE: Hi. Drew Clark with National Journal's Tech Daily. When you talk with the tension between anonymity and security, are you saying something beyond the fact that individual businesses should be permitted to require smart cards and other type of things?

In other words, are you saying that there ought to be some societal set parameters for when people can be anonymous online and when people cannot be anonymous online?

MR. CLARKE: No, what I'm saying is that I think there are large sections of cyberspace where important information is transacted. It doesn't have to be consumer information. Sometimes it's consumer information. Sometimes it's merely business to business activity. Sometimes it's the management of the electric power grid. Sometimes it's the management of a major

rail system.

For all of the critical infrastructure functions and for most of the e-commerce sections, I think anonymity is a security risk to the individual. There are clearly large sections of the Internet where it doesn't matter.

Before coming over here, I thought I would try to find some jokes about consumer protection, and so I went online and found five sites with jokes about consumer protection. I think I ought to be able to do that anonymously.

MR. FOX: Jeff Fox, Consumer Reports. You mentioned before that we're going to be developing a national strategy, a national policy for information security. You mentioned that certain industries will develop a strategy with input from the industry.

Are we going to be developing a strategy for consumer's home computers, and will consumers be developing that strategy, and what kind of input will you get from consumers?

MR. CLARKE: Level one of the strategy is about the home user, and we are looking for ways to find groups, consumer groups to help us draft that strategy, and if you can give us ideas about that, we would

welcome it.

MR. LANE: Hi. I'm Terry Lane with Washington Internet Daily. The cyber security strategy, will there be any provisions to compel industry to adopt certain guidelines or regulations? How would that work as part of enforcement?

MR. CLARKE: I think in general having the government compel industry to do certain things with regard to cyberspace security is probably a bad idea. I say in general because the Congress has already passed the Gramm-Leach-Bliley Act on banking modernization which does include some cyber security regulation, and it's also passed HIPAA legislation on health care which also applies some regulation with regard to cyber security.

I think in general regulation is a pretty -- in the area of cyberspace security in general is likely to be pretty ham-handed. By the time that we were able to write, publish, get comment on and go into effect cyberspace security regulations, they would likely be outdated since the technology and the networks and the system so rapidly evolve.

So what we're trying to do instead is to stimulate the marketplace and to encourage codes of best

practices, sets of standards that are developed by the vendors and by consumers, by the critical infrastructures that use the technology and then to have those standards and those best practices clearly and publicly articulated.

The banking and finance community is on its own now developing a set of cyber security standards one by one. They started off with wireless security, which I always thought was an oxymoron, but in any event they are developing cyber security standards, and people will be able to see them and know whether or not their institutions are participating in these voluntary standards.

I think that probably given the technology aspect and the speed aspect is the best way of doing it, not compulsory government regulation.

MR. EICHORN: Dick, this will be the last question.

MS. FRAKER: Hi. I'm Mary Fraker from Powell Tate. I was wondering what kind of monitoring capability you have that enabled you to anticipate this enormous attack on White House.GOV, how you knew all these things were flowing out and waiting.

MR. CLARKE: We don't have a monitoring

capability, but the Internet service providers do. They monitor their own network, and what they were able to see was a rather large and unprecedented spike in network traffic, which led them to try to figure out what it was.

And then we received from NGOs like SANS, Alan Paller is here from SANS, from other organizations like CERT at Carnegie Mellon, we were told by these non governmental institutions that something was going on, and they then began to figure out what it was. Rich Pethia played a company role, back here in row five, over that weekend in figuring out what it was and telling the government what it was.

There is no Internet command post. The Internet is dispersed. There's no place in the government that monitors the Internet, so we rely heavily upon the cooperation of industry and NGOs like CERT and SANS to tell us when there's an anomaly, and then we have to work with them.

The government can't solve these things by themselves. When we talk about public private partnership, we talk about it so much that sometimes people get sick of hearing me say it, but the reason we talk about it so much is that this is a problem that

does risk our national infrastructure. It does risk our national economy. It does risk our national defense, depending upon who the actor is and what they're doing.

The government can't do it itself, the government can't defend this country's cyberspace itself. The FBI, the Army, the Navy, put them all together, they can't do it. Cyberspace has to be defended in cooperation with the government because we have some information and assistance and some capabilities that we can provide, but whether it's your home cyberspace or the cyberspace of the electric power grid or the cyberspace of the railroad industry, you really have to do it yourself.

MR. EICHORN: Thank you, Dick.

(Applause.)

"PANEL 1: Current State of Consumer Information Security"

MARK EICHORN, MODERATOR, FTC

MARY J. CULNAN, PH.D., Slade Professor of Management and Information, Bentley College

LAWRENCE DIETZ, Director of Market Intelligence Communications, Symantec Corp.

JEFF FOX, Senior Projects Editor, Consumer Reports

BRUCE HEIMAN, Executive Director, Americans for Computer Privacy

ROB LEATHERN, Analyst, Jupiter MediaMetrix

RICHARD PETHIA, Director, CERT Centers

MR. EICHORN: Panel 1 panelists, do you want to come on up?

Hi. Hello again. I'm Mark Eichorn. I didn't introduce myself earlier. I wanted to introduce Jessica

Rich and Ellen Finn and Laura Berger up here in front, we are together the team that's been responsible for putting this together, and Maureen Cooney, who will be doing the international panel.

Just ground rules for today for the panels, every one of our panelists has an illustrious history, and those are provided in your packets in the bios. We'll be making very brief introductions this afternoon and this morning.

Also for the panelists, I would like to remind all the panelists to stick more or less to the time limits that we've discussed earlier just so that we can keep on schedule.

Our first panel is the Current State of Consumer Information Security, and we're going to be talking about issues such as what the risks are and how the risks are changing and what the harms are and the impact on consumers, so if any of you have remarks on Dick Clarke's views, we may get to that as well.

At some point during this panel, we're going to take a break and then reconvene with the same panel, but we will basically go for the morning here.

Rich Pethia, I would like to start with you. Rich is the manager of the Network Systems Survivability

Program at the Software Engineering Institute, the director of CERT, and he's also active in the Internet Security Alliance.

Rich?

MR. PETHIA: Yes, what I wanted to do is just highlight some of the things that Dick Clarke mentioned, the first one being is that this is a problem that is here today. It's not one that we might see sometime in the future. It's not one that we have five years to get ready for.

We are one of about 160 different security incident response teams scattered around the planet, and every day we receive reports of intrusions in the systems. We receive reports of denial of service attacks. We receive reports of systems being compromised in one way or another, and in fact we get a lot of reports.

Last year we had over 52,000 separate incidents reported to us. Things like Code Red and the Nimda worm each count as one in that list, and so while there are some of these things that make the press occasionally as big news items, the real fact is these things happen every day, and the problem is growing.

Last year, as I said, we had 52,000 incidents

reported. The year before that it was about 20,000. Right now with the first quarter numbers in it looks like we're on track for almost a hundred thousand incidents reported this year.

The problem in terms of number of reports being generated is doubling every year, and that's just that data that we see at our center. That does not count the data that's being pulled at those 160 other organizations or in organizations like SANS that also receives reports from the outside community.

Another key point I think is that this is not a static problem. It's not like there are 16 things out there that we have to fix, and once we fix them the problem goes away. This problem changes every day. There are new threats that occur on a regular basis. The intruders, the bad guys, understand the technology. They learn more about it every day. They're getting better at finding flaws in the technology.

They share this information with one another. Especially over the last five years, since 1997, we've seen the widespread use of automated tools that are now available widely on the Internet. These tools have now literally brought us to the point where there's a point and click attack culture where people with very little

technical sophistication can successfully attack other machines connected with the Internet because the attack technology itself has evolved to the point where it's a very easy thing to do.

Another point is that the technology that we all rely on, the laptops, the PCs that we have in our homes, the servers that we have in our corporations, all of the products that are out there in some way or another have some significant number of security flaws.

Again in 2000, in the year 2000, we had about 2,500 security vulnerabilities that were reported to us. This year -- and by vulnerability I mean a flaw in the software that allows an intruder to take advantage of a flaw and somehow get better access or get access to the machine. This year at the current reporting rate, we're on track for almost 5,000 new vulnerabilities being reported.

So the attack technology continues to change. The technology that we're dependent on continues to be faulty in one way or another, and so whatever solutions you have in place today, you can be virtually assured that you're going to have to do something different tomorrow because the picture's going to change yet again.

So it's a problem that's here today. It's growing. It's changing. It is becoming more significant, and for the little bit of data that we all have on impact, and there are very few comprehensive surveys available, but the Computer Security Institute in collaboration with the FBI does an annual survey on the impact of some of these problems, and we see from that data on a year by year basis, as limited as it is, there are significant losses being incurred at financial organizations, and you can be assured that in one way or another as consumers those losses will be passed on to you.

So I think there's a lot of work to do. It's a problem that as I said we don't have time to get ready for. We have to start dealing with it now. I think there are lots of avenues available to us to attack the problem from improved technology, to more awareness, to more advocacy and activity on the part of consumer groups.

I think one of the things that's really missing right now in the world is a set of advocates for consumers who can help get this issue on the table, increase awareness and begin to bring pressure to bear against the technology producers and suppliers to

produce a better product that we all depend on.

And hopefully the next discussions over the next couple days will highlight more of these issues.

MR. EICHORN: Thank you, Rich. Rob Leathern, Rob is an analyst at Jupiter MediaMetrix covering online payments. His research focuses on using the Internet to enable and streamline financial transactions for consumers and businesses.

Rob?

MR. LEATHERN: Thanks. As some of you may know, Jupiter MediaMetrix is an online market research and analysis company. MediaMetrix is our audience measurement. We have a panel of over a hundred thousand U.S. users, and we can monitor what sites they visit and other aspects of their online behavior patterns.

Jupiter Research, which is the group I work for, does research into what consumer behavior and -- business behavior when they're dealing with consumers goes in to. I myself have been responsible for helping inform businesses how they should encourage consumers to interact with them through web based and wireless interfaces, specifically looking at transactional based businesses such as online retail and online financial services.

And I really agree with Mr. Clarke this morning that privacy and security really are two sides of the same coin. We find that overcoming security and privacy fears relating to credit card and personal information is the biggest thing holding back people from making online purchases.

In fact, of people who browse and look for product information online, that is people who have not yet made an online purchase, 51 percent say that better security for their credit card or personal information is what is required before they will consider making a purchase online.

We also find that there's kind of an incremental adoption pattern that consumers undergo. They will sign up for Internet access. They will be checking and receiving emails. They will then move on to things like online purchases, eventually moving over to conducting online banking and bill payment.

In fact, online bill payment is one of the greatest growing applications we've seen over the past two years, two to three years. So really that is something that is really growing and is threatened by some of these security concerns we see out there.

The trade-off between convenience and security

is one that continues to challenge businesses. There's also evidence that it's really been way too convenient for consumers up to now.

We did a survey in August last year where we asked consumers if they would be willing to undergo, to undertake certain additional activities to strengthen the security of credit card transactions online. What was interesting about the survey is we asked pretty much the same question for consumers about their online transaction experiences as we did about their offline transaction experiences.

24 percent of people say that they saw no need to increase credit card security offline, but only 14 percent of consumers saw no need to increase security online. It appeared that many consumers were willing to undertake additional activities in order to strengthen the security of their credit card information.

For example, 49 percent of people say they would be willing to type in an additional pin or password created or provided to them by the credit card company. As many of you may know, VISA is working on an initiative called Verified by VISA. You may have seen the T.V. commercials with Emmitt Smith.

What it basically is is when you conduct a

transaction, credit card transaction online, you get taken then to your bank card issuer site where you would be verified or you would be authenticated as the person you purport to be.

That's just an example of some additional security measures that make it a little more inconvenient for consumers to conduct transactions online, but frankly I think it's been a little too easy for consumers to date, and clearly the payoffs for businesses moving consumers online is great.

If you look at, for example, the financial services area in banking, processing a transaction at a branch costs perhaps five times as much as processing an online transaction. Communication, sending an email can cost a fraction of a penny versus 50 to 80 cents perhaps for sending an offline communication.

Recently we have see seen incidents, for example, Bank of America had a problem a few months ago where someone was sending out emails purporting to be Bank of America to customers. These are the types of things that can increase the costs of sending email communications, and perhaps maybe the cost of email communications should be higher because it's just way too easy to send emails to the list -- go visit Millions

of Addresses.COM and you will find that you can quite easily buy a CD Rom of 5 million email addresses and email people at will.

We believe at Jupiter that several trends are converging to increase possible security risks. Today of people we surveyed, over 60 percent of people would give their email address in exchange for a hundred dollars sweepstakes entry. 41 percent of people would type in a user name and password at a site that they hadn't done business with before in exchange for the self same sweepstakes entry.

If you add to that some brand new data that we actually haven't published yet but just came out a few weeks ago, that 53 percent of users use the same user name and password at all or most of the sites they visit, you can put these two numbers together and find out that if you have a really interesting sweepstakes offer, we all know it's pretty easy to brand yourself online, at least to look legitimate with graphics and other things, you can see that this is a big problem.

Sites quite easily gather -- appearing to be legitimate gather user names and passwords and then use those to compromise people's accounts, and we're not just talking anymore about someone going and buying a

$12 CD at Amazon.com. We are talking about people that increasingly have and are managing financial relationships, assets at brokerage accounts and banking institutions that can now be compromised by some of these aberrant password behaviors.

Consumer perceptions of the safety of their information are very apt to be influenced by widely publicized but infrequent events. You may have read the news a few days ago, Ford Credit I think they had, what was it, 13,000 credit reports compromised. Similar to some of the risk perceptions you get around driving your motor vehicle versus taking the airlines, obviously it appears when there's an incident in an airline context, it's much larger.

Obviously people have a much bigger fear of it, so you have this misperception of risk for one thing, so people need to be informed about they should be taking ongoing precautions, and the other problem you really see is that all companies are negatively affected by a lack of confidence in the online medium.

So even the practices of those companies who are doing a great job are negatively affected by those companies that are doing a poor job. There's a real need to better educate consumers, encourage and monitor

security best practices, and reward companies who are doing a good job of the above.

Unfortunately, one of the biggest, unresolved issues is who is going to pay for all of this. I've spoken in the last couple days to one of the top three banks in the United States, and they are totally on board with the idea of it, but unless really compelled to do so, they're not going to be extremely proactive and spend a lot of additional money in order to make this happen.

So I think that's the question I would leave off my prepared comments with is someone needs to figure out how we proactively encourage companies to spend money to help educate the consumer.

Thanks.

MR. EICHORN: Thank you.

Bruce Heiman, Bruce is the executive director of Americans for Computer Privacy and a partner at Preston Gates. He concentrates his law practice in the areas of IT, trade and transportation.

Bruce?

MR. HEIMAN: Thanks. Americans for Computer Privacy is a broad based coalition of more than a hundred companies, 40 trade associations and some 7,000

individuals. We really led the fight during the '90s to liberalize export controls on American encryption products. For the last two years, we've been working hard to ensure that our nation's critical information infrastructure is protected in the right way.

This morning I want to focus on consumer information security and make three points. First, I want to urge everyone to "gas" up in cyberspace. I want to make sure that everybody guards against strangers online.

Second, I want to offer a handful, really five specific, practical tools that consumers can use to protect themselves, and third I want to recommend three things that the government can and should do and two things that the government definitely should not do to help the consumer.

So why should we worry? Why should we "gas" up in cyberspace? When they asked Willy Sutton why he robbed banks, he said, Well, that's where the money is, so it shouldn't be surprising that in the information age, criminals are targeting information.

One important difference is Willy Sutton let people bring their money to the bank to a centralized location, but technology now allows for distributed

victims. With computers it's now possible and profitable for criminals to reach out and touch people where they are.

I would hope that the public understands that computer crime is real crime. It's not funny. It's not a joke. It's not cute, and anyway you look at it, as you've heard, the problem is clearly getting worse.

What's interesting is it's not only getting worse in absolute numbers but it seems to be getting worse relatively as well, that is, if you take the number of incidents and compare it to sort of any measure of online activity, whether it's number of computer users, number of computers, hosts, clients, in relative terms the problem is also getting worse.

So, what can consumers do about it? Plenty. The tools exist, and they are available for individuals and companies to protect themselves if they take the threat seriously. I want to emphasize this. Security can only be improved if users take advantage of the security tools that are available to them.

It's not rocket science. It's not even computer science. It's common sense so with that in mind, let me offer a handful of suggestions, five specifics that have been suggested by the Business Software Alliance and

others: Use strong passwords; change them frequently; use anti-virus software; install a home firewall; update your security features regularly; and encrypt your stored data.

Now, if everybody did this, we would be an incredible ways down the road to good security nationwide.

Finally, I want to talk about what the government itself should and should not do to help secure consumer information because there are definitely right ways and wrong ways for the government to get involved.

Three things the government should do: First, educate. Workshops like this are excellent. So too is the Administration's recent National Cyber Security Alliance. The government can play an important role in educating all of us about the importance of essentially practicing good security hygiene.

The government also can remind the public that cyber security is an ongoing responsibility. There is no silver bullet. There is no one time fix.

A second thing government can do is enforce the cyberspace laws. At this point the laws are basically on the books making computer hacking, theft and

destruction crimes. Now comes the hard part, investigating, prosecuting and punishing those who commit such crimes.

The government needs to make it a priority to devote adequate resources to the job and train law enforcement personnel.

The third thing government can do is remove barriers to information sharing about cyber problems and solutions. Right now companies are reluctant to share information because they fear it will be disclosed and used against them.

Pending legislation in the House and the Senate fixes this problem by offering limited protection for shared information.

Now, there are two things that government should definitely not do. First, do not mandate the use of particular security technologies, processes or products. The government should not be in the business of promulgating technology specific standards. Doing so will make the cyber security problem worse by stifling innovation, freezing development and artificially channeling R&D.

Cyber security is best accomplished through private sector solutions that are market driven and

industry led.

As you heard today, it's essential to remember that the private sector designed and deployed today's computer networks and products. The private sector owns and operates them, and they have really the knowledge and expertise to best develop cyber security solutions.

The other thing government should not do is weaken individual security. You might ask, Well, why would they do that or how could they do it? Well, first they shouldn't weaken the ability of individuals to protect themselves against cyber crime by limiting the ability of American industry to develop best products and services.

How could this happen? One good example were the efforts during the '90s to try to require that American companies install back doors into their encryption products or to require that an extra set of keys be given to the government.

Another example would be requiring ISPs to build their systems in such a way that permitted easy, immediate access to law enforcement. On the telecom side, this was the CALEA debate. This came up with respect to ISPs as part of the Council of Europe cyber crime convention, which unfortunately was not adopted.

Government should also not reduce our security under the guise of helping law enforcement, and a good example of this is a requirement that ISPs keep all communications for 90 days. That would be good, but you're also creating -- on the one hand you can go in and try to investigate. On the other hand, you're now creating a new repository of data that itself becomes an attractive target.

Also, as originally proposed, Fed.Net was a government-wide Internet -- it was a government proposal to have an Internet surveillance system. That has now been scaled back appropriately towards more of a management tool, a network administration tool for government networks itself.

So to review, we must guard against strangers online. We should take five actions to protect ourselves, and government should take three actions to help, and definitely not take two other actions.

Thank you.

MR. EICHORN: Thank you, Bruce. Mary Culnan, Mary is the Slade Professor of Management Information Technology at Bentley College in Waltham, Massachusetts, author of the Georgetown Internet Privacy Policy Survey, and coauthor of the Culnan-Milne survey.

Mary?

MS. CULNAN: Thank you very much, and I want to thank the FTC for organizing and hosting this workshop. It's really needed as we heard from Dick Clarke, and I hope that this will be the beginning of efforts that will do for security, particularly consumer and small business security, what their privacy workshops have done for privacy in terms of promoting the discussion.

I'm going to try and put a human face on security and follow up on some of the things that Dick Clarke talked about. Actually he gave my remarks minus one example, but I think one of the issues that I think is very important is that the vulnerabilities extend far beyond what people make experience in terms of loss of their own data or alteration of their own data on their home computer, that once you get broadband access and you're connected to the Internet, you're really connected to the world.

And therefore consumers that don't protect their home systems represent a threat to critical infrastructures, to our national security because that also includes their economic well-being, and as we heard their home computers can be used to launch denial of service attacks.

Just this year the National Academy of Sciences issued a report on cyber security called "Pay Now or Pay Later," and in it, it cites the use of unexpecting home computers to launch some of these attacks, and there's a real cost of these as we heard.

The CSI FBI survey reported that 10 percent of their respondents, granted that was a very small number, but they had experienced denial of service attacks, and the average cost to clean up one of these was $122,000, which if you add all of these up turns into real money.

So is this a real problem? And this is where I want to get into a couple examples. I had a student in a class last fall who came into class one night and reported she had a DSL line with no firewall, and she got hacked, and whoever attacked her came in and they hi-jacked her AOL account and used it to launch a SPAM attack.

The only reason she had any idea this had happened is because AOL had shut down her account temporarily because she had sent out too much email, and she was really in a panic. She didn't have any idea of what to do now, was there still stuff on her computer that was going to be a problem, had her system been compromised? And so this is only one example, but she's

clearly not the only one.

My own experience, I moved into the broadband early this year. I got a new computer that has Microsoft XP, and I installed a cable modem and installed a firewall, and within five minutes of installing the firewall started getting scanned because the firewall software would give you a pop up alert.

And over the past two or three days which is where I've been logging in, I've been getting 20 to 30 of these scans a day, and these are scans where somebody's actually looking at your computer to come in.

They're not legitimate interactions with known firms on the Internet, so this suggests that in fact this is a real problem, and it's going to get bigger, and while you have a firewall and you have good anti-virus software, you're not going to stop a really determined attacker who wants to do serious damage.

It wants to cut down on these sort of nuisance attacks. Just like putting a lock on your front door or a club on your car is going to send a burglar to look some place that's not secure.

So what should we do? Obviously there's a need for a lot of consumer education. I teach privacy and a

little bit of security at Bentley, and even with students who have been exposed to technology and should be relatively sophisticated, you don't get a good proportion of those that have broadband access having the appropriate software in place, and so there needs to be a lot of work on this.

I know Jeff Fox is going to talk about the Consumer Reports article that just came out. I think this is a terrific example of what needs to be done, not only talking about the problem but they rate software products and give people some tools that they can go out and either purchase or download immediately to put some protections in play.

And I also want to second Dick Clarke's call that the vendors and the ISPs should step up to the plate. I think this is irresponsible of them not to do so. Microsoft's XP comes with a basic firewall, which is an excellent first step because you really don't have to do anything except you do.

They don't turn it on or and they don't really provide you any kind of heads up when you install the software or start running it that in fact you should turn on the firewall. I found out about the firewall when I went to the computer store and went to buy a firewall

and asked if it would be compatible with XP and was told, You don't need a firewall, you already have one, so I went out and bought a box and was in business.

When you turn it on, it doesn't seem to affect your system at all so I don't see any reason why it shouldn't be on, and hopefully we'll hear from them.

I think the broadband vendors or the ISPs should also bundle security software with their services or make it easy for people to download it and have them turn it on as part of the installation process.

When I installed my -- got my cable modem installed, it was a third-party contractor who did the installation, and he didn't know anything about firewalls or should I have one them or whatever and so I found that kind of disappointing.

Finally, I think government can't solve this problem but it can certainly help. Chairman Muris, the FTC, and lots of other people in the government have the bully pulpit, and when they go and speak to the public, they can continue to encourage people to do better.

I also think that good security should be a requirement for any broadband funding expansion program, so if there's money given to telecom companies to go out and expand the reach of broadband to consumers, then

that should carry a requirement that they also provide appropriate security when they install these services.

MR. EICHORN: Jeff Fox is a senior projects editor for Consumer Reports. He's been covering technology, cyberspace and privacy for a dozen years now or so.

Jeff?

MR. FOX: Thanks, Mark. First of all, I would like to express my appreciation to the FTC for having this workshop and for timing it about ten days after the article on which I spent months working came out. Had it been before the article came out, it might be a little more difficult to speak about.

Also I want to mention to Rich that at least one major consumer organization is now on the case, and I would like to thank CERT for the help that they provided us in the investigation, and I just completed this lengthy investigation on essentially the subject of this workshop.

The information that was turned up is too much information for the few minutes that I have here, so I recommend to people to look at the June issue of Consumer Reports. If you need a copy or press kit, I can provide that for you. Thank you.

Also after these remarks, I'll be delivering a written report with a little more detail and analysis to the Commissioners, and if they want to put some of that -- including some graph charts and data, and if they want to put that up on their web site, they're free to do that.

I guess the center piece of the report was a survey that we did of about 8,000 of our online subscribers, and I'm required by our survey researchers to give a little caveat that these were online subscribers and not completely representative of the American public, although they characterized themselves as intermediate and advanced users, so we kind of expect that their experience would possibly be better than -- or they would be as well or better protected than the average person.

The subjects that we have focused on in the article were hackers and unprotected broadband home users and malware viruses and Trojans and the like.

The problem of unprotected broadband users, our survey showed about 35 percent of the figures that we surveyed did not have a firewall installed. This is the one piece of data that we've actually been able to back up with data about the general public. We've done

a subsequent survey that's not yet published that shows that this number is in the ball park, so that's one number that I mentioned today that can be generalized to the general public.

If you apply that to the number of online broadband users, you get at least several million users out there now that don't have a firewall who have high speed connections, and I would say that this is now -- I view this now as a cyberspace equivalent of Afghanistan. This is a breeding ground for criminals and terrorists. It's really just a time bomb waiting for the right person to set it off or people to set it off.

We didn't get a lot of data in our survey about hacking. We did get a small number of people that said they had been hacked, but the data was kind of skimpy. We got much more information about people's experiences with viruses and worms, and I'll just run through them quickly, but the data will be available in that report.

Of the people that we surveyed, nearly 60 percent have found the virus on their home computer at least once in the past two years. Nearly 20 percent have had that experience four or more times.

Ten percent of the respondents had experienced computer damage from a virus or other type of malware,

and other questions showed that in a significant number of cases, the damage could not be completely reversed. It was either partially -- they couldn't fully repair it. In some cases they couldn't repair it at all.

If you do try to project this to the hundred plus million U.S. online homes, you can certainly say nationally there are several million homes that have experienced damage, I would estimate conservatively hundreds of millions of dollars, if not billions of dollars in repair costs over the last couple of years, based on the cost estimates that people gave us. Also I would say that millions of homes have lost data permanently based on our survey.

As far as how these things get transmitted, email, 62 percent of the people said they came by email, but interestingly, almost 13 percent said it came from the web or download from the web which is about one in eight. That's kind of not as obvious a transmission.

User protection, 25 percent of the people had not protected themselves against virus, either because they didn't have anti-virus or they had manually updated anti-virus, and they had not updated in the past month, so that's a significant number of people that are not following good practice.

I think just in sort of in summary here of what the conclusions that I draw from some of this data is that there's been significant economic and personal damage already from viruses. Millions of consumers are now sitting ducks for both hackers and viruses, and what we see merely is that the federal and state governments, which are supposed to protect consumers from what essentially is crime, I don't think based on many surveys I've done have taken the problem seriously enough until this workshop.

For example, we had to do the survey because we really couldn't find any kind of government data. Most types of crimes now are tracked by the government, and I think that's extremely important. In addition, as Dick Clarke mentioned, ISPs being absent from the problem solving, I think the government certainly has to get involved at least to the extent of collecting data and tracking the problem. We can't be substituting for the government.

There's also -- despite that there are some cyber crime laws, I found for the average consumer that there's little meaningful law enforcement. If you're hacked, even though there's a law against hacking, it turns out if you're hacked in your home, if that

incident is not part of an interstate commerce or a government or financial institution computer it's just your home computer, basically the government does not want to talk to you.

So, in summary, on behalf of the millions of consumers, I think we can say that it's time for the government to begin doing its job of monitoring these crimes and protecting consumers.

MR. EICHORN: Thank you.

Larry Dietz, Larry is director of market intelligence for Symantec, an information security software and services provider. He's responsible for market analysis, competitive assessments and strategic directions and assists with business development.

Larry?

MR. DIETZ: It's always good to be like the seventh speaker because you need to have a lot of original material, and I'm mostly indebted to the FTC for insisting that none of us use PowerPoint.

The first remark I would like to make is that we need -- we must be very careful not to underestimate the magnitude of trying to train, educate and inform the average consumer of the problem.

I can recall several years ago when I was but a

young captain on assignment to teach communications security to a National Guard unit. Sergeants came back and said, Captain, we couldn't do our job. Why not, guys? Well, sir, if we teach them how to be communication secure, first we have to teach them how to turn on the radio. And so the implication is most consumers are not turning on the radio.

I'm also reminded, I worked for a company, we sold computers to car dealers, and I did have to explain to one of my customers that if you don't put chicken bones in the printer, it will work better, so don't underestimate the challenge.

First thing I point out is that the home is an extension of the enterprise and that every employee is also a consumer. As many of us work more than 40 hours a week, we end up doing work at home. Home computers get to be a target because they are an easier target, and of course we've learned so far today that anti-virus is not enough. I'm not going to repeat that.

I will mention the issue at home of multiple users on the same computer which has not been mentioned. Dick Clarke talked about the under three year old. It is I think pretty clear that most young folks are very technically inclined. Some of us still

have the double zeroes blinking on our video recorders.

So you have a class of users at home that I would refer to as authorized users, unauthorized users, and so individuals have to be cautioned as to who they allow to use their system and what protection they take.

Employers have a clear duty to protect all entry points to the information technology infrastructure. However, they're not necessarily sensitive to that, and new entry points crop up all the time, but there needs to be an awareness of the need to commute, to telework particularly in areas where the commute is very difficult.

I was at a Gardner conference last week in Chicago, and the figure they cited was that an employee who commutes an hour who's able to commute or to work at home, of that two hours, employer will gain two-thirds of that time in increased productivity, employee gets to keep a third, but there is more pressure to do that.

Next point I would make is that we're seeing a blended threat where there is a blurring of the difference between a hacker, a worm/virus, malicious code, and an exploitation of the vulnerabilities of the products or the configurations. It was already pointed out that a lot of opportunities

exist for hackers because products are not updated.

In terms of threat vectors, the hackers are doing port scanning. Some of you may find that there is a fair amount of technical mumbo jumbo in dealing with the Internet. Portology is one of my favorites. If you're ever at a cocktail party with a ponytail person and a baseball cap, you can say, Well, what about the Port 80 problem, don't you think that's really significant, and then take a sip of your drink because that will be a little while explaining that.

In terms of the home, Dick did elude to the point that the home is a target because it has a static IP address. I know all of you study IP addresses, but I think it's easier to say that it's harder to hit a moving target than a stationary target, and that because the home computers now have increased in power, they become a more viable target, and obviously those that are connected to broadband are paying $50 a month, which makes them even more of a target, and so there's a filtering out.

We've also seen complexity increases in viruses, new metamorphic viruses that change their patterns to avoid detection, as well as the number of viruses.

I would also suggest that some of the future

threat will be team attacks, groups of decentralized people, let's just keep pick a name at random, Al Qaeda, that have cells in different places, all charged with different acts, seemingly independent, unrelated, but all with a common purpose.

Lastly, we were asked to provide some data to the FTC in terms of things we found in the marketplace based on research we've done and surveys we've purchased. I can -- I agree very much with Jeff's numbers. We found, the most recent research we have, 70 percent of users have an anti-virus of one type or another, and only about 15 percent have a firewall.

In terms of how often do they update? It looks like about half of them update automatically. It's also done automatically over the Internet, 30 percent weekly, about 12 percent monthly, and then about 3 percent each for every few months after the virus, that's my personal favorite, and never.

So in sum, working with the consuming public, the small office, home office is going to be a difficult challenge, and we have a long road ahead.

Thank you.

MR. EICHORN: Thank you, panelists. I think this is a good time for a break this morning. Can

someone tell me what time it is according to that clock?

Why don't we get back together about five of, and this same panel will reconvene. Thank you very much.

(Break in the proceedings.)

MR. EICHORN: Let's get started again. I just wanted to remind everyone, once again, that if you want to pre order your lunch sandwich, there may still be time. I get a 10 percent cut from the cafeteria. actually I don't.

(Discussion off the record.)

MR. EICHORN: I want to take a step back at this point. We have a wide variety of attendees I guess, and I just want to jump back to some really basic questions for a moment, and I guess my first one would be: What are the threats to consumers? Anybody?

MR. DIETZ: Well, the threats, as I mentioned, are kind of a combination of hacks, which is an intentional hostile act by a third-party, viruses and worms, where code is received on somebody's machine, either actively on their own part or passively, and third, a vulnerability in the configuration of the end user's machine, either because the products they have

are defective or because they failed to configure them properly. Those are kind of the major buckets.

MR. EICHORN: Larry, can I ask you to describe -- we've heard the terms viruses and worms and Trojan horses is another one, and I'm wondering if you could sort of define out what the differences are between those -- or whether that distinction matters to consumers?

MR. DIETZ: Well, I think as a practical matter, the distinction doesn't matter. I had another one of my famous clients say to me, The reason I hired you is I don't know the difference between a megabyte and a dog bite, so I don't think many consumers and small businesses owners really care about what the problem is, but I will help you out there a little bit.

A virus is a piece of hostile code that will do something bad but must be activated by an act, and viruses are typically one machine at a time, so when we had the I Love You virus, it was a letter attachment to an email, and the user had to double click on it, so the user had to do something.

A worm, by definition, is self-replicating. That means kind of like the wire coat hangers in your closet, it makes more of itself, and you don't have to do anything else, and the worms are particularly

dangerous because they can replicate themselves several ways such as already has been mentioned, a download from a web site, email, file sharing, disk sharing. Those are all different ways that worms can self-replicate.

As far as a Trojan horse goes, everyone kind of remembers the story about the big toy horsey that came inside the gates, while on the outside it looked like a really good thing, although why you would want an 80 foot horse is kind of beyond me, but it was really dangerous on the inside. The payload in that case was soldiers from the enemy.

You heard Dick Clarke talk about Code Red this morning a little bit, and the nature of the payload was such to take over the victim machine, sometimes called a zombie in the jargon of the trade, and then use that as a jump off point to attack a target, so that's a Trojan horse.

MR. EICHORN: Thanks. Getting into sort of the meat here, how are these threats changing? All of you sort of mentioned this in some ways in your presentations, but what are the factors that are causing the risks to change? Rich?

MR. PETHIA: Let me go off on just a slightly different direction for a minute because sometimes I

think the technical terminology that we insist on inventing in this industry confuses some basic issues.

We all know about things like peeping toms and voyeurs and vandals and thieves and organized crime. Those aren't mysteries to us. We've heard about them. We've dealt with them for years.

What's happening to us in the Internet and the IP world is all those things are coming to cyberspace, just like they've been in the rest of our space for all of our lives, and one of the differences is they can come with less risk because in order for a thief to steal the money out of my house, he has to be physically present, but for a thief to steal account information from my PC, he could be sitting in Singapore just as well as he could be sitting in my living room.

So distance begins to disappear when we get to cyberspace. Time begins to get compressed. It takes virtually no more time to access my system from Singapore than it does from the house down the street.

So now all of a sudden you have to think about not so much what are the technical threats, but what is it that I have in my machine that someone might profit from and therefore want to steal, or what is it that my machine can do that someone might take advantage of?

For instance, we have reports from people who have become unwittingly -- unwitting distributors of child pornography because the bad guys found a server on the Internet that was unattended and decided they wanted to use it to distribute illicit information rather than their own machines.

And then at the same time you have to think about for all the people I do transactions with over the Internet, what information have I given to them that they have to protect, and what might the bad guys do if they get their hands on that information?

So, for example, the thief who wants to steal credit card numbers and information in order to illicitly use those credit cards or sell them on a black market, and there is a big black market right now for that kind of information, is more likely to go to some Internet provider of goods and services who has a big collection of credit cards than he is likely to come to me where I might find one credit card on my machine.

So I think when we think about threats it's important to understand the technical nuances of how these things happen, but I think it's more important to recognize that this is crime. These are bad people doing bad things for profit, and if you can think about

it in that way, it might help take some of the mystique out of this and let people know that unfortunately we've got to deal with criminals now in cyberspace just like we've had to deal with them in the rest of our lives.

MR. LEATHERN: I think I would add to that that I think we see people, the bad guys are going to be going where the money is, and increasingly people are accessing and having financial information available to them.

The convenience factor is great. I can access and conduct online banking transactions from my desktop at work, from home, from on the road as I am now. That's all great. However, there's a couple dangers that exist and we're seeing.

One, a lot of compromises are happening if a lot of systems are being attacked, if people's financial information is being stolen or accessed without their knowledge. This creates costs, costs not only to the consumers themselves who are affected, but also costs to companies. They will have to spend a lot more money on security, and so they may not end up implementing online access to their accounts. Consumers I believe to access these convenient features will go away.

The other thing is you're also going to see

services be available but just not responded to so, for example, if my email in box is stuffed with 150 SPAM messages and a message from Citibank that my account statement is now available online, it's increasingly likely that I'm going to miss and have to pay that $29 late fee because I didn't know that my billing statement was there, so we're going to see something like that.

We're also already seeing a lot of social engineering going on where people that create a virus or a SPAM mail are employing technology to try to make it look more -- look emails look more legitimate. This makes it even more likely that the legitimate emails are going to be confused or not responded to.

I don't know if any of you have received any credit card solicitations recently, anyone? But things like something that looks like a Fed Ex package, clearly I'm going to open that because it looks important. I've seen ones recently where some more poor schmo at whatever the credit card company is signing their name to make it look legitimate.

Those are the types of things we're seeing online, and because the cost of sending email for example online are so low and because you can get 10 million email addresses for 59.95 online, these things

are going to become increasingly more prevalent.

Our numbers indicate the average user received about 500 SPAM messages last year. That number is going to more than triple in the next four to five years, and I think even that I think is a conservative number.

MR. EICHORN: Jeff?

MR. FOX: In the area of hacking, I think a big change is the deployment of high bandwidth connections with large numbers of ordinary home users, and that has now -- because I think that hackers are after the bandwidth, and the servers and corporate networks that were targets were -- at least they had an IT staff.

Home users now have similar kind of bandwidth. They don't have anywhere near the sophistication that corporate networks do, and there are millions of them. So it's like a million targets with no expertise with a similar bandwidth.

And in the area of I guess viruses and malware, when I was a software developer before I came a journalist there was a slogan or saying that all software proceeds until it's 90 percent complete, and then remains 90 percent complete forever.

That's an essential problem we're going to have to deal with, even with a lot of the problems we're

seeing, the bugs, I'm trying to think of the word that's used for the flaws in the software, but the system software, the operating systems, the Internet and client software, they're not going to disappear.

They can tighten it up to a certain extent, but given the proliferation of Internet applications and the richness of applications, operating systems, powerful processors, you're always going to see large complex pieces of software, and I don't think you're ever going to see -- I've never seen bugs disappear in 30 years of using computers.

MR. EICHORN: Mary?

MS. CULNAN: One other thing that was mentioned earlier but it's worth repeating here is it's easier and easier for people to launch sort of unsophisticated attacks because of the scripts and tools, and so you don't look at the threat as being a monolithic thing, but there are different kind of bad actors out there.

And certainly it's easier to deter the people that are just sort of looking for somebody to hit and want to use a pre scripted program to do it. Someone who is a determined terrorist that really wants to get at something in particular, that's going to take a different set of tools, so I think that's also important

in thinking about threats as sort of break them into who's interested in getting to what.

MR. HEIMAN: I think it's important to follow up this idea of creating analogies to sort of the physical world. I mean, you wouldn't buy a car, you wouldn't buy a new car and then park it somewhere on, with the keys in it, running and walk away. You sort of just wouldn't do it, but in essence that's what you're doing when you have a high speed connection. You're just leaving it on all the time.

You wouldn't even buy the new car, leave it parked and open and walk away. I bet you if we take a poll right here, how many people, when they park their car, lock it? Let's have a show of hands. Right? Everybody does it.

Now, how many people have some sort of car alarm that gets turned on? See, a lot but fewer. How many people use The Club? See, there it is, and the numbers go down.

I think we need to create sort of the virtual analogies to sort of the physical world to really educate people and really get it through, and much as you have to take your car in every 3,000 miles to get new oil or it just isn't going to work right, you have

to periodically get those updates on your security features as well.

COMMISSIONER SWINDLE: Can I pose a question, Jeff and Mary could perhaps deal with it and, Jeff, you talked about it. It's slightly apart from this, but it's all a part of securities and vulnerabilities, talking about the software systems that come out, and there's one big company in our world that recently came out with a new product that Mary has, and it was criticized by many.

And I'm concerned about -- we all know there's no perfection in this. It's always revolving, searching out bugs, making it better, and yet we have another element now since the privacy debate has gotten so big, and certainly the security debate is going to be big, so we have a litigious environment now. We're going to sue people, the developers, for bringing this on without it being perfect because it has vulnerability.

Where is that taking us in this effort to improve security or privacy? Is it going to be an impediment or is it going to be an inspiration?

MS. CULNAN: Good question. You've obviously let both of us speechless about this.

MR. FOX: You mean the litigiousness?

COMMISSIONER SWINDLE: It seems to me that all the best minds and from every parameter that we can imagine, countervailing forces, the civil society, the industry, the public and so forth, we need to work together as opposed to trying to take advantage of others' fallacies, and obviously I don't think anyone in the industry is seriously trying to create something that's bad.

MR. FOX: But software companies need an incentive. Until now obviously that incentive has not been there.

MR. DIETZ: Let me just -- I'm licensed to talk out of both sides of my mouth by the great state of California. The products liability issue is a big issue, but the products liability issue is, A computer and its piece of software, is it like a gun? Guns don't kill people, people kill people? Is it if I put a seat belt on the car and you don't use the seat belt, is that my problem as the manufacturer?

Mary pointed out she bought XP. She didn't know it came with a firewall like capability, and it was switched in an off position. Now, should the vendor be made to ship product with an on position? Don't know.

MS. CULNAN: I think part of this is whether

we're speaking to sort of our individual interest as either consumers or companies or to our collective interests as a society, which is what Dick Clarke talked about and try to find some ground where if it's clearly in the national interest for companies to develop software and tools and provide those easily to people so that there is some form of protection, I think that's a good idea, especially at sort of a rudimentary level where maybe there can be some balance between something that runs well versus something that doesn't and is going to create an interest in people to sue.

COMMISSIONER SWINDLE: You harken back just a few years, and let's speak of Microsoft, all the problems that Microsoft had, although it's bringing all these wondrous things that we now know as the Internet and so forth and marvelous computing, and let's give credit to Apple first because they came up with the various and sundry means today that Microsoft uses, but we joked about it.

Today lawsuits are being filed about it. Are we elevating that aspect of this information technology world to the point where it's becoming a detriment?

MR. DIETZ: Well, I think the litigation with Microsoft is mostly about their trade practices, not

about the defects of the product.

COMMISSIONER SWINDLE: I am not talking about the thing over here at the Justice Department. I'm talking about current things, that it has vulnerabilities.

MR. FOX: I just want to speak as a former software developer who's developed code. I don't think the issue is so much whether people turn on a feature or use a software. There's a question of the quality of the software creation itself. The product, is it a defective product, is it a quality product.

And when I developed software in the 80s, the idea of a buffer overflow, which is one of the major flows that have shown up in Microsoft software, we didn't do that then. I honestly think that software quality control is not what it was back then.

I think in the race -- first of all, software has gotten bigger and more complex obviously, but good coding practice in which you check for things like that really honestly should have been in the Microsoft software development methodology all along, and I don't know why it wasn't.

Apparently now it is, but it took these problems to get them to do that, but there's a question of whether they are following good software practices, and

I think if a customer has shown not to have followed good software practices, they've created a defective product, and maybe there is a ground for legal action there.

MR. PETHIA: I think the pendulum needs to swing for awhile. There is probably as much new software in my new truck as there is in my laptop, and yet I don't have to stick my finger in that software every other day to correct some flaw. Granted, it's not plugged into a DSL connection, but there are literally millions of lines of software and many products, and we know as an industry how to produce those products with high quality, high reliability, to ensure high availability and good service.

So the question is: Do the quality features of the product -- are they adequate for the marketplace where the product's being sold? And I think today I can't think of any vendor who could justifiably make a statement that they don't understand the threat environment of the Internet. People like SANS and CERT and others have been publishing tons of data on what the threats are, what the vulnerabilities are, what the impacts of with all of these things are with respect to secure, safe operation of computers so the vendors today

need to make a decision. Are they going to build products that are fit for that marketplace or not?

I contend that a lot of products today aren't released. They escape. They get out into the field long before an adequate job is done of quality control and testing and quality assurance, and that's something I think we all need to make noise about, not necessarily from a litigious standpoint, but we have to send a signal to the vendors that says --

COMMISSIONER SWINDLE: That's my point.

MR. PETHIA: -- the quality of these products today is just not acceptable given the threat environment they're now expected to operate in.

MR. EICHORN: Can I jump in and just say we're actually going to be discussing these issues a little bit in a later panel that will actually be tomorrow so we'll have more time to discuss this.

COMMISSIONER SWINDLE: Who says staff can't put Commissioners in their place? Thank you for the interruption.

MR. EICHORN: Could anyone on the panel comment about other sort of issues out there like wireless and file sharing? Larry mentioned a little bit, like Spyware and Kazaa and all of these kind of things that are

out there and Instant Messaging as well, how are those operating?

MR. DIETZ: There should be like a bell. If you answer a lot of questions, we should get some money.

MR. LEATHERN: There is a lot of -- there are a lot of applications out there. Some of them you refer to Spyware. I think in most cases that refers to something that's installed without your knowledge when you're installing some other kind of application which has legitimate purposes.

Also, I mean, there's a lot of -- there are many applications out there that I say once they're on the desktop, they may later be used for other purposes. It also creates the ability to track what sites users are visiting. For example, an example of this is Gator. I don't know if many of you are familiar with Gator, but it's actually really useful. It helps you remember passwords at sites. All the information is stored on your own computer.

However, obviously the way they make money is they sell advertising so what they do is they'll pop up windows every now and then that have an advertising message, and if you're willing to put up with that and occasionally click so that their advertisers stay happy,

you also get this application which lets you remember different passwords at different sites.

The issue there is you have an application that's on your system. It's sending information back to the home base every now and then. Microsoft, when you install XP, it's extremely hard not to sign up for a Passport account if you don't have one, and they also use it with the Windows Messenger product to keep sending information back.

If you run Microsoft Word and it crashes, it appears as though the problem is with your application, click here to send a product, a message about the error back to Microsoft, so there obviously is a lot more information being traded by different applications. It's not just your web browser that's accessing the Internet. It's these other applications as well.

And once you, through your firewall, say, It's okay for this application to access the Internet, it then has kind of the ability to do so. Sometimes, however, of course the good firewall products will tell you if the program has changed since it last accessed the Internet, so those are some of the things that can help consumers here, but clearly the proliferation of other products on the desktop clearly does make the

situation much more complicated.

MR. DIETZ: I have a couple of notes here. First is wireless, anybody who uses wireless should have no expectation of having security or privacy, period, end of story, and particularly organizations with sensitive data, and they don't have to be big ones, let's take law firms. Law firms, we have a lot of egos crammed in a small space, and they don't want to be bothered. Wires are yucky things, how can you see my $5 million desk, I want a wireless LAN.

So opposing counsel perhaps hires some nefarious dirt bag or dirt baggette to sit outside in a truck and just kind of listen to what's going on, so wireless, no expectation of privacy.

Spyware, first question is who's the spy and what for? The flip side of the workshop is privacy. There is more than a little interest in the notion of employers monitoring email. There's more than a little interest of employers restricting what web sites, URLs, universal record locators, employees can go to. Should employers do that? Do employers have a duty to other employees to monitor what their employees are doing? So you have to look at who's the spier and what for.

The other thing is: Is it an advertiser that's

gratuitously sending up. Get a web cam. Is that a problem, is that the spier, and was I one of these brilliant individuals that gave my email address, my IP address, my blood type, all for the chance at a $25 raffle as we heard about earlier today. So who's the supplier, what's the deal?

And last, but not least, Instant Messaging in my view, and I would be interested in the view from CERT, Instant Messaging is kind of like a VPN. It can be a way that a secure facade such as an enterprise with its firewall and so on, intrusion detection, is breached because I'm Instant Messaging my sister on what we're going to do for Aunt Ruthie's birthday, and that becomes a way in for a potential attacker.

So all of these technologies have to be looked at in context, and it's the duty of the business owner. It's the duty of the parent to take the precautions to implement whatever policies they want to set for their resources.

MR. EICHORN: Jeff?

MR. FOX: I would like -- with all the looking at technology, I want to comment on again the importance of looking at what some people are calling live ware which are the human beings because you, the human being, is the key. The user is the whole key here.

In one case talking about the file sharing and Instant Messaging, I visited the Sub 7 site. That's a site that actually distributes a Trojan called Sub 7, and probably if you want to visit it should turn your firewall and AV up to max I was warned, but there was explicit instruction there on what's called social engineering, which was actually ploys and cons that you could use when doing Instant Messaging with people, chatting with people as to how to persuade them to accept a Sub 7 Trojan that you would be giving them.

It was -- actually the person had written in there kind of in their poorly written English, I found lying works, and then gave actually arguments they could tell people this was a video, this was a that. They were actually coaching people on how to con people.

And the other aspect of live ware, about three days ago, I received an email that I would call sort of a human powered virus that would never be called by any AV software or firewall. It was an email without an attachment. I don't know if anybody else has received it.

UNIDENTIFIED SPEAKER: Was it called deleting and dealing and --

MR. FOX: It was very plausible. Consumer explain what it was.

MR. FOX: The one I got had been forwarded by about 50 different people, but the last person was somebody I knew. Presumably they got it from someone they knew so it was trusted and said that there was this new virus floating around and gave instructions for deleting this virus and that the virus software couldn't catch it and that you were instructed to go actually gave instructions, go to your start menu -- it actually go into a certain place, delete the file, told you exactly what the file name would look like.

I was sent this by a friend of mine who had actually deleted this file blindly following -- you're laughing, but you don't realize this is the level most people are at, and I recognized it as a hoax immediately, but this is more than a hoax for these people who had actually followed this, besides propagating it. They don't need to use the Outlook address book.

They're getting the person to do the file deletion, no need for a script kiddy anymore, and this turned out to have been a minor Windows utility thing that I don't think was important, but had that been a company system file, you could have had essentially a human powered virus that didn't require any scripts or

any kind of programming at all, and this is something -- cons have been with us since human beings began, and this is not something that is a technological problem.

MR. EICHORN: When you look over the threats out there and the trends, is there any trend out there that's sort of in the right direction, that's making security easier in any way?

MR. DIETZ: Well, I think when you buy a computer, you get at least one AV program on there, and you're free to choose either one or two or three or however many. I think most new computers are shipped with it. I think that's probably a good thing.

MS. CULNAN: As long as it's --

MR. DIETZ: It's different than the operating system.

MS. CULNAN: I still want to argue that shipping the software with the computer is a terrific idea, but it's either got to be turned on or it has to be really easy for people to it turn it on, and I'll give another real world analogy. It's as if you bought a car, it came with seat belts but the seat belts were hidden in a secret compartment in the truck, and the only way you could find out how to get them out and hook them up would be to read the entire user's manual.

It shouldn't be that hard. It should be easy,

and also people also need to know that they need to do this, and that's even the harder task I think.

MR. HEIMAN: I'll say on the encryption front, a lot of communications now are encrypted. When you're shopping online, you look down and you'll see the little lock, and SSL is being used. For folks using Blackberries, the communications link is at least encrypted using triple disk. There's lots of products out there that can encrypt your stored data, but again it's up to users to choose to employ those products.

MR. DIETZ: On one hand I think it's probably a good thing that schools are starting to teach computer skills as a part of growing up as early as the fourth grade.

On the other hand, I can't be comfortable that they're going to teach all the other things, adjust your mirrors, fasten your seat belt, because most schools tend to be pretty rushed, and I'm not convinced that before all the little tykes go on the computers, they'll hit their live update button or make sure that the anti-virus is on, and I'm just a little concerned about that personally.

MR. LEATHERN: I think a trend moving in the right direction is I think recently we see a lot of

companies who when consumers are doing online transactions, they're asking for additional information, for example, asking for the card on the verification field. It's that extra number on your credit card. Recently I went to the gas station and I used my credit card at the gas station. They asked me for my Zip Code. That was something new that I had never seen before.

So as you can -- as the technology improves, and these databases are more available, they have access to them in real time, they can do the -- they can match your address to your credit card number. They can check against a database that can detect if you're shipping something to a known fraudulent or suspicious address. If you try to make 15 different transactions in the last 30 minutes, they can look at your IP address and see if your ordering something to be shipped to Florida when you're actually accessing from Slovenia.

So technology is improving, helping on some of these issues that I think especially in the transactional area where money is definitely at stake, there's a lot more investment going into that.

I think one of the areas where there's not as much is just every day password practices and so on. I

think there's still a need for consumers to become the bread and butter of how they think about interacting with customers -- with companies, and I think the psychology there is still -- it's still very different.

People see the Internet still as different, not just another extension of the company they're doing business with, and I think there needs to be an evolution there as well.

MS. CULNAN: I think one thing where education is also needed is that people just as they don't realize that their broadband connected computer can easily be scanned by someone looking for a place to attack, is that there are password cracking programs that also run, and if you have a password that's in the dictionary or is too simple, basically you're putting yourself at risk, and people don't know that so that's something else along with adjusting the mirrors that needs to be taught.

That's another thing when I poll my students periodically, and too many people raise their hands and say, yes, their password is just letters or it's a word that somebody could easily find instead of having numbers and upper case and lower case and some scrambled characters.

MR. FOX: I think that broadband enabled

computers, when they're sold, there either should be an option to get a firewall or an option to turn the firewall on. I don't know if computer manufacturers are permitted by the antitrust settlement to reconfigure Windows in that way, Windows XP. If they are and they're selling the computer broadband enabled, then they probably should turn it on by default, maybe not for dial up users but certainly for people that have a broadband computer.

Otherwise at least offer people the option of getting a firewall with the computer.

MR. EICHORN: Mary just mentioned passwords. Can you all opine on consumers' use of passwords and how they do it?

MR. LEATHERN: I'll jump in because we did the recent survey I mentioned earlier. Our survey done in April found that 53 percent of users use the same user name and password at substantially all or most of the sites they visit. 25 percent of users write down their password on this piece of paper that they keep right next to the computer.

If you think about it, it isn't necessarily that bad. If it's in your home, then it becomes pretty much as secure as your home does, so depending on that. We

found about 7 or 8 percent of people use password helper applications, either something like Gator, which is you dial into your machine, all the information is stored locally, or Passport -- Microsoft.NET Passport -- that with participating partners all the information is stored on servers ostensibly in Redmond, Washington, where you can log -- you could for example log on to eBay using a Passport account.

You wouldn't have to set up a separate eBay or you would have to set up an eBay account but you can then log on to it with Passport information.

So clearly there are people using the same user names and passwords everywhere. Some sites have moved away from letting you choose a user name so M. Smith, obviously M. Smith will probably be taken so you're going to have to go through a couple iterations until you get to M. Smith 961 that works.

But then since I mentioned before many sites, many consumers will willingly give out a user name and password, register to receive access to a site so they can get a $100 sweepstakes, that's a problem because if I'm using the same user name and password at the Citibank site, I could set up a site to gather this information and try to use it elsewhere on the web.

It's like having a door that everyone can stand outside of for as long as they want and keep trying different -- the 10,000 different combinations of the typical house door key until they find one that works.

MR. DIETZ: I guess, once again both sides of my mouth here. I think the notion of passwords is surely important. Whether the user who uses the same one is always at risk, I'm not willing to say. Password synchronization can be a way for a user to use the same password, presumably a difficult one.

I took an anti hacker class, perhaps the oldest living graduate of said class, and we were told a really good example is 100 percent milk. 100 percent sign M I L K because it had numbers and it had one of the characters and so and so forth, so users have to make the decision on passwords that they can remember easily and they have also have to manage them.

I've given up counting how many accounts and things that I can't remember them, if someone is trying to attack me, God bless them, if they gave me the list, I would probably be happy about that.

I think you have to put things into perspective and recognize the order of magnitude of the threat and what's a common sense practice to defeat the threat.

MR. EICHORN: To what extent -- let's assume that consumers are less sophisticated than businesses are. To what extent does that affect how well they can secure their own systems?

MR. PETHIA: This is a pet peeve of mine so let me start with this one. We talked about quality issues, and I think in addition to quality issues we need to look at fitness for use from the perspective of matching the product to the characteristics of the person who is going to use it.

Today's laptop, desktops, the things we have in our homes are very sophisticated electronic software devices. Unfortunately, however, they're instructed in such a way that the user has to have a lot of technical sophistication to get both the power, but also the security that's inherent in the products.

For years now we've talked about things -- we've talked about, we haven't produced, we talked about things called Internet appliances, things that are built for the skill set of the people who are going to use them. I think that's one of the big problems the industry has to face over the next ten years.

If we ever want this big expansion and more electronic commerce, if we ever want the trust of the

broad consumer base, the industry is going to have to step up and build products whose characteristics are matched to the characteristics of the people using them.

It starts very simple, from simple, easy to put together, take out of the box, default configurations and moves all the way up through things like configuration management and worrying about whether or not you have patches installed and getting virus updates, all of that has to become two orders of magnitude more automatic than it is today.

MR. FOX: I would like to mention a few things. I interviewed a number of consumers in doing the article. Not all of them made it into the article. Once person I spoke to who had experienced some damage on his computer from a virus and then had updated to the new version of the anti-virus that he was using, this is a question of lack of sophistication, is that at that point he was bragging to me it was like perfectly safe now to click on attachments and everything.

This is a guy who actually had experienced a virus loss and even after having that happen, because of his sort of total faith in the promotion of the product, which told him how great it was, he now believed the new version of course was perfect, and he didn't have to

worry about good practices anymore.

And although as a journalist, I'm just supposed to ask questions, I couldn't help but give the guy a little advice and say, Please, don't drop your guard just because you have the new version, don't take it so literally, but people trust this information, and they have no way of knowing things like that.

MR. LEATHERN: I think one point I just wanted to mention is it's hard to figure out whose responsibility it is to educate the consumer in the case of, when you're accessing your Citibank account on line, knows the person who makes the browser, well it's probably the same person who makes the operating system, right, so is it Microsoft's job? Is it Hewlett-Packard who made -- perhaps they made the PC. Is it the software manufacturer that could have made the anti-virus software. Is it Citibank itself?

A lot of things need to come together for this to change, and the clients and the companies that I talk to, it seems like everyone is waiting for someone else to pick up the ball and run with it, and that's just the thing that I see every day when I talk to companies about these issues. It's great if VISA is spending money or someone else is spending. I don't want to

necessarily be spending my own money in this environment to educate the consumer.

MR. HEIMAN: It's everybody's responsibility. I mean, I think it starts with parents and at the home. You teach your kids to lock up when they leave the house, and you teach your kids not to talk to strangers on the street. You just have to incorporate that. The school point was interesting, and I hadn't really thought about that, but it's true.

Kids clearly are getting educated about computer use at school, and I doubt they're incorporating any security education as part of that, and that needs to change.

Businesses are, need to, are doing more in terms of educating consumers about the security features that they are building into the products. So I think it's really -- the short answer is everybody has to do more.

MS. CULNAN: I would agree with that, and you need to educate the teachers that they need to educate the students. It's fine to say, We need to teach the students but if the teachers don't understand, and so I think there's some real good opportunities to develop some packages or summer institutes or other kinds of things to get the word out there, and again if you start

young, then you don't have to worry about it so much as people get older.

MR. EICHORN: From a practical side, this might be best addressed to Jeff or Mary, but what happens to consumers when you find a virus on your system? Where do they go? What's involved in cleaning up?

MR. FOX: The first advice we give to people is to disconnect from the net, and also don't do anything immediately, I mean, because if you start to do things or you try to delete it yourself or repair it yourself, you're just going to get in more trouble.

These things are complex pieces of software and many people naively assume if they just delete a file, they've cleaned it or they may not even know if it's actually a virus, but you want to run an AV scan as quickly as possible, even if you have to go out and buy it.

MR. EICHORN: We heard from Dick Clarke about several interests of consumers. One is the role that consumers play in denial of service attacks, and I guess there are arguments that consumers have an interest in protecting the network partly based on patriotism and altruism and things like that.

But how do you think that consumers can be sort

of educated about the importance of security. Is that -- so that there's a market for security?

MS. CULNAN: One way is it's in their own self interest so they don't have to clean up after a virus or some kind of a problem or worry about their identity being hi-jacked, but the other issue I think is people need to be made to feel, and maybe I'm being made to be naive that this is going to be easy, but basically you don't want to be the one that helped launch a terrorist attack or created higher prices for everybody because there were so many denial of service attacks that in fact the costs do get passed on.

I don't know if there's some way to trace this back to individuals. A few stories in the media perhaps might get people's attention that ultimately you are responsible, even if you don't get hauled into court or go to jail, but basically it was your fault, but I don't know. I think that's a hard issue, and we have to sell that or it's not going to work.

MR. DIETZ: I think it's a difficult issue because who is the consumer? Is it the person -- I sound like the little red hen. Is it the person that bought the computer? Is it the person that uses the computer the most? Is it the person that's the default

computer support person, the person that's turned to in the household when the computer goes cafluey? Just who is the consumer?

MR. FOX: I would say anybody that uses email or got on the net. I spoke to a woman who had a home network and her son's computer which was on the home network had been hacked by what she called hacker vigilantes. These were people who actually found him cheating on an online game, and they hacked in, deleted this game which he had paid for, and so clearly everybody in the household -- your kid is using sharing files, downloading music and stuff like that.

If you think you're the user because you open an Internet account, anyone using the Internet is a consumer.

MS. CULNAN: It's sort of the same thing as everybody who leaves the house should lock the door, so I would agree it's everybody's responsibility.

MR. EICHORN: Several of you mentioned data on how often consumers actually use like anti-virus, for example. Does anybody have data on patching, how often people patch?

MR. PETHIA: We probably have a lot of data on how people don't patch, and we know that 80 to 90

percent of the security break-ins that we see could have been prevented if people had upgraded their software to include patches, and we also know most of those patches are not for serious design flaws. They're for silly implementation errors like buffer overflows.

So we've got lots of data that says the great majority of incidents come from software that's not up to date. The flip side of that though is it's really hard when you have 5,000 new vulnerabilities being discovered every year to make sure that your software is up to date with the most recent hackers that were probably produced three minutes ago.

MR. EICHORN: This might be a good time to turn to questions from the audience. Just go ahead and move up to the mike.

MR. LEATHERN: I just wanted to mention that anyone that is interested in any of the data during any of the comments I mentioned, just leave your business card with me, and I'll email you a presentation that has all of those numbers in there because I know a lot of numbers are flowing around.

MR. EICHORN: If you do ask questions for the mike, the court reporter has asked that you provide your name. I'm going to leave that up to you.

MR. PALLER: Alan Paller from SANS. I was taken with the discussion that Rich and Mary and Jeff and Bruce had. Bruce's position seemed to be that users should learn to do it themselves, but Rich said it's like the seat belt's in a locked door, in the trunk, and it can't be found.

And then Mary said it's outrageous that the vendors would make it that hard, and, Jeff, you were talking about incentives. What's the right incentive? It's clearly not litigation. It might be litigation, but it sounds awful to do it with litigation.

If it's not litigation, what will cause the vendors to get it out of the trunk and make it absolutely simple for Grandma to have a system that isn't automatically attacked?

MR. FOX: Well, I think if things get so bad that there's a ground swell of outrage and demand by consumers, but I think we're still pretty far from that I think, the market will always do it.

MS. CULNAN: Public humiliation I think.

MR. LEATHERN: I think it's ironic talking about litigation. It seems people often get rewarded for stupidity, spilling coffee on you or whatever. I don't want to get into that whole issue, but to be perfectly

frank, people are -- you don't need to be -- you get rewarded for that, and I think we're talking here about people having -- being highlighted for doing silly things when there's really -- there's an externality to your actions.

You're not just allowing your own financial information to be compromised or denial of service attacks can influence everyone. I think it's a very hard thing to do. I don't see an easy answer.

I think education and starting at an early age are a good first step toward that, but the real answer, should it be something like seat belts where everyone is required to have certain software on their computers or things configured in a certain way. I don't think that's necessarily the answer. It's difficult to answer that.

MR. HEIMAN: I think it's important to recognize not only the severity of the problem but the complexity of the problem too. I mean, what, at last count there's some 50,000 viruses sort of on record now? You're talking about 5,000 new vulnerabilities developed each year to really acknowledge how complex these software programs are.

So I don't think you can simply mandate certain

things. I think, in fact American industry is doing a pretty good job of coming up with solutions and fixes to things.

Now, I do think there is consumer responsibility to use some of those tools, and if they use some of the tools that are available today, then a lot of the problem gets rectified.

MR. FOX: I want to say the biggest problem is the lack of information about the number of, magnitude of losses. When there used to be 50,000 people dying in cars every year, that gave rise to Ralph Nader and the consumer movement and movements to make improved car safety.

And I think the reason that we don't see, as Rich said before, yet a vigorous consumer advocacy here is because we don't have the information. If people knew hundreds of millions or billions of dollars per year were being spent -- if people saw the numbers, there would certainly be people then rising to the occasion and then beginning to make the public case.

But in the complete absence of information about what's happening, everyone knows what's happening on their own little computer.

MR. HENNESSEY: Joe Hennessey with a

technology question. All of the threats that you described, the viruses, the worms, et cetera, do they all require the consumer, the end user to activate code either by downloading it or double clicking it and executing code?

MR. DIETZ: No. A number of the worms don't require that at all. All the end user has to do is go to a web site that has been compromised and poof, you're hit.

MR. HENNESSEY: Are any of these worms activated simply by opening an email?

MR. DIETZ: Viruses can be. Worms can be, yes. Although I must say, any attorney who opens an "I love you" message probably knew that was a mistake.

MR. KOENIG: This is Jim Koenig from ePrivacy Group. As an attorney I have a question, but it's actually for Rob and Jeff.

Rob and Jeff, in the data that you talked about and discussed earlier, and I know there's a panel later on about business models with respect to security, but I want to ask a consumer perspective.

If in a general sense, whether it's confusion or consumers don't know the difference or the market hasn't pushed the companies to put it in the products yet, in

asking the question, who's interested in privacy, who wants privacy, who wants security safeguards in place, everyone will raise their hand.

If you ask the question, who wants the security and is willing to pay an incremental amount more and balance the two together, I think that's an operative question, and that comes back to the market determinations.

Companies see it's a differentiating factor. It's a brand issue. If it doesn't tag them on their brand, it doesn't affect the bottom line, then they're less interested.

So what type of data did you see there that would help companies then be motivated to say, This is an increasingly important financial issue for me that it affects my bottom line, not just the interesting public issue.

The second one is -- second question is on consumer education, and so right now if consumers are confused and don't know where to go and what to do, I think we all have raised our hands and said that consumer education sounds good. Who puts it together, who finances it, who distributes it?

MR. LEATHERN: Your first question, I recently completed a report about online privacy, and one of the

things I think always is a challenge to do is get away from the abstract. For example, if you ask consumers what's going to make them buy more stuff online, one of the responses is better prices. Big surprise, 75 percent of people want better prices.

When you ask similarly about privacy and security, I think you're always going to get a high response rate if you say, I'm worried about my privacy. I mean, in fact 70 percent of the people we surveyed are concerned and they worry that their privacy is at risk on the Internet.

However, the flip side of that is only 30 percent of people actually ever read privacy statements online, so what I think the challenge is is to quantify the trade-offs that are made.

Are you willing to undergo something a little more inconvenient, maybe spend another 30 seconds signing up for a web site or providing a card number or something like that to get the product or service that you're looking for online?

I think businesses need to spend more time doing that. We've been in a stage where in the last three or four years we've seen companies throw traditional business models out the window in order to try to get

consumers to buy things online or sign up for some online account.

A lot of sanity has returned to the marketplace, thankfully, so I think we see companies who have been around the block and have been in business for 50 years starting to try to get consumers to sign up for online services, and that needs to be there.

Brand needs to be there. Trusted company -- companies with trusted brands are going to be able to get consumers to sign up for their services. They're going to be in a position to provide these services, but they also need to ensure that through their privacy and security policies they are retaining that trusted position.

One thing I think is interesting that came out of the report I just wrote is that I think companies are doing a good job, need to take more credit for what they're doing as well. They need to really -- I think to call it marketing of their privacy policies, it seems like kind of like an oxymoron, right, but they need to take credit for things that they're doing well.

And I think by doing so, by going above and beyond it, being within the spirit of laws and practices and adopting best practices, that's the way we'll move

forward in this area.

MR. FOX: I want to say something about consumer education. I was going to save this for tomorrow's panel VII, but I don't know how many of you are staying in hotels here. I found this in my hotel room, brought it with me.

This is the campaign with that little dog on it that you probably have seen in hotel rooms, the traveler safety tips. I've seen this wherever I've traveled in the country. This is a campaign, a crime prevention campaign for travelers, people staying in hotels. I don't know if it's a government/industry effort, but clearly this is reaching people where it matters.

I just wanted to comment on the campaign that was launched, the government/ industry campaign that was launched during the winter which I thought was a great idea, was launched with a lot of fanfare in February. One of their things that they said they were going to do was having twice a year when people turn their clocks ahead and back, this was going to be like a check your computer security thing.

The weekend of April 7 there was nothing. Just to make sure I didn't miss anything I did a Nexis search, and I found virtually no coverage since that

great launch in February, and so it looks to me at this point that this campaign has not yet followed through on its promise.

And it's not even a question of putting a site up there and saying, We've got the site there, people will go there. Ordinary people, people I know are not hunting down sites like that.

You need something like this. You need something where people are when they sign up for an account or when they are getting their bills or whatever. You need a place prominently all the time to get in front of people's faces. That's the kind of campaign you need.

MS. CULNAN: Also there's no such thing as a giant consumer education program. This has to got to be in chunks. I'm a big believer in small wins. I think we can look at some other areas where there have been some good efforts to educate consumers about problems.

Identity theft is one where the FTC and others have done a terrific job being some place and pulling out some of those postcards that you see when you go to bars and restaurants and whatever. Then there was the "don't let someone steal your good name" postcard from the FTC, and I'm thinking this is really great.

So I think everybody needs to do their part, but I think clearly one need is again to develop some programs that get rolled out into the classrooms at all levels K to 12. College, there needs to be curricula developed that people can choose to use if they like it or they can modify it.

And then everybody that's interested and companies who have a little money and marketing insights can step up to the plate and do their part.

MR. KOENIG: Just before I go, Rob and Jeff, was there any specific data on consumer specific willingness to pay more? I know Commissioner Swindle had the incentive of litigation or possibly moving something, but was there anything specific about something

MR. PETHIA: Although I have to jump on that one too. We don't expect to pay more for tires where the tread doesn't separate from the tire body. We shouldn't expect to pay more for software products where teenagers or children can break in to them versus those being very secure.

I think this is a basic question of, Are these products fit for use in the marketplace in which they're in, and I think today the answer in many cases is no, and consumers shouldn't be expected to pay more for products that are clearly advertised to work in that

domain.

MR. EICHORN: Last question.

MR. RONKEY: Bob Ronkey from Privacy Council, and I'll tell you right up front that this question is going to sound like I'm a heretic, but there's been a lot of talk here that there's a huge problem and that there are multiple components to that problem, whoever developed the machine, whoever developed the software, who sold it, who services it, and then us as users of it.

What I'm wondering about is, I've heard an awful lot of talk how solutions exist, we just don't use them so there's a motivation issue under that, that it sounds like there's a lot of activity to try to motivate builders of the software to make it better or the sellers of the computer to make it easier.

So what the heretical question I'll ask is: What motivates me as a consumer to take part in any of your educational programs? I get an awful lot of documentation with my software, but I go to the quick start little sheet because I want to get going with it right now, and I want to partake in the good stuff that comes with getting online, but it will never raise to a priority for me to truly understand some of the security issues that are available to me.

So you've used car analogies a lot. If I go out on the road and drive too fast, I get fined. If I don't wear my seat belts in Illinois where I live, I get fined. In the little town where I live 38 miles west of Chicago, everybody locks their doors in my community, but if I go another 38 miles west, there's a little town where they don't because nobody goes there and they feel secure so what's the motivation?

Should the solution -- Bruce said government doesn't need to pass more laws, they exist. He said we shouldn't mandate a specific solution because there are multiple solutions, one of which might be better than the other, but how do we activate the consumer? Should there be the speeding fine or "you didn't use your security" fine? I would be interested in what your impressions are on that.

MS. CULNAN: Well, for one thing if we focus on people who are younger than those of us in the room, you basically have a captive audience, so they may choose not to do it, but at least they're going to hear the message because it's part of the curriculum and they're required to listen. The older consumers, it's a harder sell I think.

MR. FOX: I do object to putting the onus on

the consumer, even though the consumer has responsibility. I think that just simply saying it's up to consumers to protect themselves, it's dealing with street crimes by saying, Okay, everyone is going to wear Kevlar vests.

You have to deal with the roots of the crime. You have to deal with -- the essential problem is the Internet's infrastructure was not built for the kind of activity that's going on now, and ultimately it's the Internet's own mechanism, they're going to have to create traceability, accountability and better security, control the Internet itself because that's why you can't track down the people that hack into your computer.

That's a long-term problem. We're dealing even with AVs and firewalls with really short term issues of to wear the Kevlar vest while the bullets are still flying, but long-term we have to find some way to stop those bullets from flying.

MR. HEIMAN: Well, I wear seat belts because when I took driver's ed way back when, they showed you gruesome photos of people who didn't. My kids wear seat belts because if they don't click up, we don't leave the driveway. I think that sort of the captive audience point is the right one.

I think you sort of answered the question. In your town everyone looks their door because they perceive a threat, and 38 miles away people don't because they don't, and I think what we need to -- so it comes back down to the education point which is those people in that other town where they don't lock their front doors, if they get online, they have to feel threatened.

They have to know that there's a risk out there, and so I really do think it begins with sort of basic education and it begins with the family and parents.

MS. CULNAN: Jeff's point about if there were more data available about what can actually happen to you in a tangible way if you don't implement, sort of the gory picture kind of thing, that might help too. I think people don't perceive there's a problem, a lot of people don't.

MR. LEATHERN: I think another captive audience that you can have is companies, if a company -- we've talked a little bit about how it is good practice for a company to tell its employees about these things, and you can start there again. I mean, I spoke with Hewlett-Packard, and they have a web based training system that tells their employees how they should be

treating customer information, how they should be respecting their customer's privacy.

That's a great place to start if you start with big companies and give them encouragement, maybe money or there's obviously a number of different ways it could work. But it's a great place to start, and I think we need to start there as well as start with the younger consumers, the consumers who -- it was funny, about a year ago we did a survey. We asked teens and their parents who thought they knew more about the Internet, and 97 percent of teens said they knew more about the Internet than their parents did, so clearly that's a great place to start.

MR. EICHORN: Well, can I -- oh, I was going to cut it off. Rich, you want to make a quick point?

MR. PETHIA: One other quick one. I'm very happy to see the June issue of Consumers Reports because those of us in the security business have been talking to each other for years, and we have to get this message out to people in vehicles that they already relate to.

And the more we can do with Consumers Reports and other kinds of consumer publications, events, to get this message to an audience in a vehicle that they're accustomed to dealing with, the sooner I think we build

that awareness that causes people to want to take some action.

MR. EICHORN: We've been running about 15 minutes late all this morning, and I want to continue running 15 minutes late so we don't cut into the lunch break, so why don't we start after lunch at 1:15.

There's a list of restaurants that are nearby in your packets, and I really want to thank the panelists from coming from all over.

(Applause.)

(Whereupon, a lunch recess was taken at 12:00 noon.)

AFTERNOON SESSION

(Resumed at 1:15 p.m.)

PANEL II: What steps can consumers take now to secure their information? What are businesses doing to education consumers about these steps?

MODERATOR: LAURA BERGER, Attorney, FTC

PANELISTS:

TATIANA GAU, Vice President, Integrity Assurance, America Online, Inc.

STEPHEN C. JORDAN, Vice President and Executive Director, Center for Corporate Citizenship, U.S. Chamber of Commerce

SHANNON KELLOGG, Vice President, Information Security Program, Information Technology Association of America

CHENGI JIMMY KUO, Network Associates, Inc.

BERNHARD MEISTER, Systems Architect, Security Architecture, Development and Implementation, Verizon Communications

MS. BERGER: Good afternoon. I would like to ask everyone to please take your seats so we can begin the first afternoon panel.

I'm Laura Berger. I'm an attorney at the Federal Trade Commission, and this panel is about consumer information security education and what steps consumers can take now to secure their computers. We heard some about that this morning. I think the discussions naturally blend together that way.

This panel is only 45 minutes, and we're going to allow ten minutes towards the end for questions. And because of the brevity of the panel, I've asked each of the panelists to just be prepared to do a dialogue about this topic, so I'm going to quickly introduce the panel, and then we'll start talking.

Immediately to my left is Tatiana Gau, senior vice president for integrity assurance at AOL.

Continuing down the line we have Stephen Jordan, vice president and executive director, The Center for Corporate Citizenship at the U.S. Chamber of Commerce.

To his left we have Shannon Kellogg, vice president, information security program, Information Technology Association of America.

We have to his left Jimmy Kuo of Network Associates, Incorporated.

And on the far left, my far left we have Bernhard Meister, systems architect, security architecture, at Verizon Communications.

So to start our discussion of what consumers can do now to secure their own computers, let's talk for a minute about the top ten tips. We heard a little bit this morning about what are the top five things or some of the important things people consumers can do to

secure their computers.

What are the most important, the top ten things that consumers can do? This is on a volunteer basis.

MS. GAU: I'll jump in. I'm going to try to not be redundant on some of the points that have already been covered earlier today, and I'm going to go down to the basic level of talking about the average consumer out there and not the user who is already on broadband and has a certain higher degree of sophistication I'll call it.

We recently did an Internet study which actually was part of the launching pad for the Stay Safe Online campaign that was launched in February as was referenced earlier today, and we interviewed Internet users at large from the most novice level to a higher degree of sophistication.

And we clearly found that people just are not taking the proper precautions that they should be. 77 percent of users indicated that they did not update their anti-virus software on any kind of regular basis. They are not using strong passwords such as alpha numeric combinations or passwords of a length of six or more characters, so it really was kind of a level set there that I wanted to establish with respect to the

type of consumer that I would like to talk about today.

In that context, the top five tips that I would throw out is: Number 1, and this is something that we reinforce through various means on the AOL service by communicating with our members through messaging that we provide online, alerts that we provide to our users when they sign up, sign online for a session, specific areas on the AOL service that we promote and push members into, help areas and things of that sort.

The first number 1 tip that we push right now is to have a strong password, right from the outset create a password with a combination of alphanumeric and make it at least six characters long or more preferably, but those are the guidelines that we put out for passwords.

Second item, make sure you have anti-virus software and keep it up to date, obviously emphasizing the latter point as we've already seen and discussed today.

The third tip that we always give to our users is to notify AOL, and this really serves as a central point for the flow of communication and understanding of the issues that are impacting our users because by our members notifying us of problems that they encounter online, scams that they are seeing happen online,

viruses that they may have received, it allows us to take steps on the back end from the technology perspective as a business, where we protect our network and protect our consumers before the problems even land in their mailbox.

It also provides a way for consumers to reach out and get help in certain situations, and we have Notify AOL Buttons scattered all over the AOL service in the mail read form, in the Instant Message form, on the AOL web site areas, in the chat rooms, on the message boards so that wherever something could possibly happen, members have a quick and easy way to notify us about it.

Going on down the line, I would put using firewalls to protect yourself if you're on a high speed connection and also to make sure you download security patches, of for a more slightly sophisticated user unfortunately.

In the same survey that I referenced just a moment ago, we found that less than 30 percent of the respondents of this survey said that they downloaded security patches on a regular basis, and remember, this is obviously self attestations so the number is probably actually lower than that.

But another question in the survey asked how

they learn of security issues, how did they learn of patches being released or how did they learn of new viruses or things of that sort, and overwhelmingly people said that they got their information from television, and most interestingly, of the respondents that had seen some message relating to security, the vast majority of them recalled a virus alert of some kind, and that really was the message that they were getting most often.

Finally, the tip that I would put out here is the tip that we always give to consumers no matter what age they are, whether they're adults or whether they're children, don't give out information gratuitously.

For children, it's obviously important for parents to teach their kids not to talk to strangers, don't give out personal information, things of that sort, but the same rule applies to adults, and we find that a lot of consumers have a false sense of security in some ways in their homes.

Their door is locked. They're comfortable. They're in comfortable clothing. They're sitting at their computer. And caution just doesn't seem to play the same role that it would play in some other setting than when they're at home, and with that I'll turn it

over to somebody else.

MR. KELLOGG: One thing that I would add there, and those are all excellent steps to take as a consumer and for small and medium sized businesses, remember I think from the outset that we need to reiterate probably what we said this morning, that this is a continuous process.

So any of these actions that Tatiana is recommending for consumers or small businesses has to be done on a regular basis, or ultimately you're not going to get the results that I think we're all looking for.

Another thing in, this area of broadband and hopefully as we go forward with more broadband deployment, remember to disconnect from the Internet when it's not in use. That's also something important to remember as far as specific actions.

And then kind of looking again sort of at a more general level, we at ITAA work a lot with our larger corporate members and also a lot of our security vendors. We've got 140 companies that are involved in our information security, many alone, and we do a lot in trying to get the issue of information security up at the board level and making sure that businesses look at it as a business continuity issue, not a business

survivability issue.

It's the same message to small and medium sized businesses and an important part of our audience for today as well as the average consumer in that we want to make sure that they look at this and understand information security as a business continuity issue, if not a business survivability issue.

And therefore there are a number of things which Tatiana has already gone over that you can do that are free, that don't cost a lot of money because we understand whether you're a home user or if you're a small or medium sized business, that you can't necessarily invest a lot in this area, but there are things that you can take, are steps that you can take that are basic and are forward looking and can start at the consumer with this.

MR. KUO: First of all, if you didn't pick up this thing this morning, there's a whole stack of them outside. This is my paper that was written for Stay Safe Online campaign and as the anti-virus presentation for that campaign.

But one more thing that businesses can do is that when they have service online, they should find or realize what those machines are there to do and limit

the machine down to only those services, so if you're not supporting FTP, turn all those things off.

If you're not supporting Telco on that machine, turn all those things off, and it's a matter of education, but it's much safer to only allow those things that that machine is going to do to only allow those services.

MS. BERGER: I want to interject for one second. You mentioned something that businesses could do. Is that something you would advocate for consumers as well just to set their computers for how they're going to be used?

MR. KUO: For home users, generally they should have a firewall, a personal firewall, and if they don't turn off their machines and get off the Internet when they're not using it, they should at least turn that firewall to the high setting so that when they're not using it, all the ports are closed.

MR. MEISTER: I would just like to amplify on the comments made certainly so far in that what we're seeing is the redeployment of computers in the household more in the aspect of data centers. If everybody were to regard their laptop, their home computer more in the form of this is my family, this is -- within this

machine is my family's jewels, my bank account information, my resume, my -- all these very sensitive family documents, we have to start to separate.

That's one thing I would advocate people to do would be to separate family data away from the devices within the home that will be going on to the Internet on a frequent basis. I know in my house, my son, he has his desktop machine.

I make sure all our family's information is on our secured server we have in our living room, it's a mess in there, but this is the concept though. We have to take it to the next level, be able to say, Okay, a firewall is an essential. I would say firewalls today, even if you are on a dial up connection, I'm starting to see people talking about -- actually I've seen personally scans coming through dial up connections.

So the broadband issue will only exacerbate the vulnerability to the home environment, but unfortunately, we have a home environment where the parents are very busy, very frustrated about all this new technology. Their children are developing skills which they don't understand, and it's a very tough call for the parent, so my message really is to not only

focus on the PC and your home computing environment, it's no longer just a PC.

You have PDAs, you have wireless, you have infrared, all these elements can combine together, but I would also emphasize that we have to do better as an industry in demystifying how these things work.

I think too often we throw up our hands and say, Oh, I don't know how this works so you don't do anything. That's really running away from that issue. And I would like to see demystification become part of our dialogue between our consumers and those who provide the technology.

MR. JORDAN: You know, when you originally asked the question, it was about the top five security tips.

MS. BERGER: Actually it was the top ten, but it's gotten narrowed down as we've again down the line.

MR. JORDAN: I think what we need to do is we need to make a distinction between behaviors and tools, and a lot of folks talk about tools, firewalls, software, anti-virus packages, things like that.

And I think that one of the things that Shannon was getting at is behaviors are just as important for this, and one of the things about this too is the tools and techniques are probably going to change and evolve

and are going to be very dynamic, and I think that sites like Stay Safe Online and things -- and other web sites and other tools that keep track of the tools are going to be very dynamic on the tools part.

But I think that the basic behaviors need to be filtered out as well, and then those need to be disseminated, and that doesn't necessarily have to be that evolutionary. I think that basically talking about applying your elements that you apply for physical safety to your cyber safety posture is something that maybe we can educate a mass audience about and probably they can make their connection very quickly too.

MS. BERGER: So we're starting to talk about this in terms of getting consumers to understand the process. I just want to follow up on something Bernhard was telling, if other people want to comment on this, about getting consumers to understand what of their data is sensitive and to target that data and protect it.

I wondered if other of the panelists had thoughts on that.

MR. KUO: Another comment about what small businesses can do, one of the biggest problems on the web is when you give the credit card to the company that you're doing business with and you find out later that

it's been kept on an unsecured server and that whole database was just compromised, and that's one of the things a business can do is to take that credit card database off of that web computer and put it on simply another computer that's not on the Internet.

And that computer is the one that does all the billing and is only dialing out to do the billing, but if you looked at what are the crown jewels of the business, and that set of credit card numbers is really critical, just take that off and move it off to the side or to a more secured server.

MS. GAU: I'll try to take a stab at your question, Laura, in terms of what can consumers do with respect to data that they have on their computer in their home.

One of the tips that again is part of the National Cyber Security Alliance's efforts is to make a back up of your computer data, and there is certain advice that's provided in terms of how often you do that and how far away you should store that from the computer so it's not right next to it.

But I think that that is something definitely that consumers are not doing on a regular basis. It doesn't protect the data obviously if the data gets

stolen, but it addresses a situation such as a virus infection where important files get deleted.

To the issue of actual protections for people's data on their computer, I'm going to actually echo my colleague's comments with respect to behavior. I think that there are tools out there that consumers could use if they wanted to, to encrypt their data on their computer or, for example, use firewalls and things of that sort.

But ultimately it is about behaviors and making sure that consumers understand the need to do this, and interestingly enough, one of the approaches that we took earlier this year with this alliance was to call upon -- we actually called it the Call to Action.

As a citizen of the United States it is your duty to do your part in trying to protect the nation's infrastructure. Yes, there's other elements that need to play a role in protecting our nation's infrastructure, but you as a consumer need to make sure that you don't unwittingly become the mechanism through which an organized group or a disorganized group could, in fact, attack a government web site or some other system in our country by having your computer become a robot simply because you had a password that was too

easy to guess.

And we found that really using that kind of approach as a call to action just as we need your help to be on the outlook -- to be on the look out for things happening in your neighborhood, and currently of course with the latest terrorist threats that have come out, to be vigilant for what is going on in your apartment building, for example, are these people coming and going, what is going on.

The same thing applies to the online world, and it's a message that hasn't really come across that strongly at this point, and it's one of the things that I think may well be a driving force to getting more people to pay attention.

MS. BERGER: Just -- go ahead.

MR. KELLOGG: I was going to say, that's what I like about Stay Safe Online, if I may just be blunt, is it boils things down so everyone can understand what we're talking about, and it also pulls a lot of different resources together.

Sometimes these can be very complicated issues but some of the steps you can take are very simple. Stay Safe Online does that. It packages things very easily so you can understand it, and what it does and

what we're all talking about here is it sort of addresses this issue of establishing a culture of security which our friend Commissioner Swindle talks a lot about, developing a culture of security.

Now, you want to do that in your home. You want to do that in your small business. You want to do that in your corporation. You want to do that in your organization. You want to do that in government, and it's key that we have this mentality.

This is our responsibility to do that, whether we're at home or in small businesses or in corporations, and again Stay Safe Online pulls that all together. I think that's more important, and we should be supportive in industry as well as in the public sector and of consumers or from the consumer standpoint of initiatives like this and get aware, understand what's out there already, and so we're not reinventing the wheel, and most importantly we're not making things more complicated than they already are.

MR. JORDAN: I think there's a part of this that we should also look at, which is while there are fundamental base line behaviors that would apply to all consumers, that not all consumers are monolithic, that you don't have -- you might have some fundamental

things, and then each category of consumer is also going to have specific needs that should be tailored to their particular interest.

Under Stay Safe Online right now, what we're seeing is that we're getting predominantly to new users and to heads of households and to small business owners, and --

MS. BERGER: Stephen, I'm going to pause you right there, because before we get into -- this is a very important discussion we're starting to have about alerts for consumers and Stay Safe Online and how you can tailor education efforts to the appropriate consumers, but there are just a couple more areas of tips to consumers that I want to hit first before we move on and pick up with that discussion.

And one is an implication of something that Tatiana has just raised, which is maybe getting consumers to recognize when someone has or is attempting to interfere with their systems. I would like to know if the panelists think that that's also an area for consumer education, getting consumers to recognize when something has gone wrong with their system so that they can repair it or intervene and fix it.

MR. MEISTER: Is this microphone working? This

morning it wasn't working quite that well. I just want to take your point because it is important to see that part of that process is to understand, and I'll give you an example.

We have a home network. My son was chatting online, and I personally find as a parent I don't like him talking to strangers. Who was he talking to? Well, I'm lucky I do have some knowledge of the security realm, so I put on a packet sniffer, and I began sniffing packets. Now, the illustration here is not that I spy on my son. I trust him implicitly.

COMMISSIONER SWINDLE: Verify, right.

MR. MEISTER: But I wanted him to see categorically how easy it is to sniff this information and how non anonymous it truly is, so it's through these small illustrations, these small lessons, if you like, I also did the same technique with my own management. I showed how VPNs worked by throwing something going across in the clear, including budget information which was of course fictitious, we have no budgets, money, terrible.

But to see important information in the clear being deciphered out of this wire to me is a very important lesson in understanding, and this is why

perhaps I feel like a broken record here, but when we talk about firewalls, my firewall goes off continuously because I see people trying to do stuff.

Some of it is very innocent. Some of it maybe isn't, but the next generation firewall hopefully will be able to combine some of these aspects.

MS. BERGER: So you're suggesting one of the ways that consumers can be alert as to something that might be going wrong with their system is through firewalls that give them notifications.

MR. MEISTER: Absolutely.

MS. BERGER: I just want to see, are there other important ways that consumers can be educated about how to recognize if something has gone wrong that they need to remedy to people.

MR. KUO: Go ahead.

MS. GAU: Are you sure?

MR. KUO: Go ahead.

MS. GAU: One of the things we try to do at AOL to help our consumers recognize problems, particularly in the variety of malicious web sites or viruses, Trojan horses and scams for that example is actually put up examples of what these things look like online.

We have an area called the Neighborhood Watch

where we post alerts about the latest virus that is going around and what the email looks like when you get that virus. Normally when a virus first hits oftentimes it's appearing as the same email. Of course that doesn't last very long because then it starts mutating, that is, the email that is carrying the virus has an attached file, but also with web sites, fake store fronts so to speak.

There's a big problem right now with bad guys creating look alike web sites for top named companies on the Internet, sending an email saying, You have won this that or the other and you'll get 25 percent off your shipping to come here, log in, boom they've got your password. In some cases they get your credit card too.

So we will put up examples of those kinds of sites online, and we give the step that always navigate to a place where you're going to be giving personal information by typing in the URL. Don't go to that web site by clicking on a hyperlink in a piece of email that you don't know where it came from and you don't know whether or not that email is authentic. The safest way to make sure you are at a legitimate web site and giving out the right information is simply to manually have typed in the URL.

MS. BERGER: Because this is a short panel to begin with, I'll go ahead and let you all move into giving the highlights of the important consumer education efforts that are out there, and if you want to address at the same time what you have found through your experience the level of consumer awareness to be, feel free to comment on that as well.

We've already talked a little about Stay Safe Online. I don't know if people want to pick up with discussion of that.

MR. JORDAN: I was just going to go through and say that we are finding that there are very different user sets on the Stay Safe Online set, and it basically breaks down into about six categories. The first of course are the new users who -- their kind of feedback is, I believe somebody is trying to scam me, how do I report them, I really appreciate your site, but I'm having trouble getting out of it, can you send me email with information about it, but you know early adopters -- I mean, early to the process and are really trying to figure out the stepping stones of how this works.

The second group, the parental group, is very traumatized by pornography and by viruses and by scams,

and they're really looking for information about access issues.

The third group are the functional users, the small business owners. The kind of questions that they have for us are -- it's like a little bit of a higher level of education, and they're really looking for vendor education, for determining preferences. They would like to know, for example, what firewall works better than another or is there such a thing as a spaminator or things like that. That was a cute quote.

But anyway, then another group are the truly technological users, and what's interesting about their behaviors is that they seem to divide into three different subsets. One subset is rather complacent actually, and they feel like they've got all of the tech tools. They know what's going on. They don't think that they're really vulnerable, and they don't see what all the fuss is about.

The second subset that we're seeing are the true believers, the folks that have one set of hardware or software solutions that they think is better than another, and they've got a set of preconceptions, and I think, Jimmy, you can talk a little bit to the religious force there a little bit later.

And then the third set are the activists. They're the folks that know about the threats, know about the vulnerabilities and want to see action done, and they actually want more information about the process behind security, so these are some of the things that we're really seeing in terms of the customer profiles or consumer profiles.

MS. BERGER: Given the segmentation that you're describing, what are the ways, the best approaches to educating consumers? They're using the Internet for different things and they have different levels of expertise. How do you tailor education to accommodate that?

MR. KELLOGG: I think that's one of the driving reasons behind this National Cyber Safety Alliance and Stay Safe Online is that it brought together industry and government to tackle a lot of these issues, some of which were behavioral, but mostly what can we do to collectively reach out and educate small businesses and consumers about what they can do to harden systems.

But, for example, on the behavioral side, you have links to a variety of organizations there that focus specifically on this, like the Cyber Safety Citizenship Initiative, Stay Safe Online.com, which is

actually a Microsoft initiative. You have a number of other programs that are available on Stay Safe Online that you can link to that cater to a younger group as well as parents and educating them on what they can do to proactively address some of these issues.

So I don't want to beat the horse to death, but sometimes there are solutions right in front of us, and it's not all about the technology and the tools. It's also about this is an ongoing continuous process, and having one stop where you can get a lot of this information if you're a consumer or you're a small business or a medium sized business is helpful, and that's one of the driving reasons behind Stay Safe Online and that campaign and why we formed the alliance in the first place.

MR. KUO: Earlier this morning we were talking about how consumers don't get enough education about this. Yet at the same time we're saying that 40 percent of people that were surveyed had received viruses and, 20 percent of them had evidence of, received it four or more times. That's saying 40 percent is actually getting educated and 20 percent are often getting educated quite often, but we're still in the stage where this education still needs to be tackled by educating

the educators. We can't get out to all those people that quickly.

. During the Code Red crisis, I did some calculations, and during the crisis period, 60 to 90 percent of the servers that were infected at the beginning were no longer infected by the end of another week, so we were getting the message out during a crisis period, and without the pain of crisis, people just don't pay attention, so back to what I was saying.

40 percent of the paper are now getting educated because they have firsthand experience so unfortunately they're learning it the hard way, and the rest of the population are either going to learn it the hard way or they're going to wait for somebody close by to suffer before they learn it.

But if we can teach enough of the teachers to get out there, we may be able to I guess shorten the number of degrees of separation so that there are other people that feel the pain of the neighbor as it were a pain for themselves.

MS. BERGER: In just a minute or two, we're going to be moving to Q&A, but now that we've been discussing the importance of these broadband campaigns and of educating the educators about how to reach people

through these more broadband campaigns, I'm wondering if anybody wants to highlight particular things that individual businesses might be doing to reach consumers who use their sites, something like what Tatiana has mentioned about telling a consumer "continue to type the URL" at a time when it might be especially pertinent to the consumer.

MR. JORDAN: I have actually a pretty good case study on that, but before I go into that, I want to build on something Jimmy said. We have to think about this in terms of market adoption. You have 60 million households in the United States that have adopted in some form or another of technologies, but that doesn't mean -- of computer technologies. That does not mean they've adopted the same computer technologies, all of them.

So you have these waves of adoption that are currently taking place, and some people are up to say like Windows 95 and others are up to 2000 and others are up to NT, so we're dealing with a plethora of adoption sets, and I think that that's one of the reasons why you have to break it down between behaviors versus tools.

Because of the fact that the rate of technological change is proceeding like this, I think

that you're always going to see a lag in technical adoption or adoption of technological techniques.

That being said, segue very badly, this is a $10 million direct sales company in Florida that is putting information about scandals and scans on the back sheet of their -- of just their basic newsletter. What we're seeing is that companies like the National Companies, the National Company are really trying to educate their own consumers because they see it as a unique selling tool for themselves.

So we see this ranging from the very small $10 million type company to the hundred million to the billion dollar folks, and again it ranges from folks that care about their consumers to folks that are caring about their employees to folks that are caring about their marketplaces.

MS. BERGER: I'm going to allow just one more comment from Tatiana, and the people that have Q&A, you can go ahead and approach the microphone because we're going to move to that immediately afterwards if there are any questions from the audience.

MS. GAU: You asked for other examples of ways in which messages are getting across to consumers. I'm going to point to the Code Red example where the

national infrastructure protection center of the FBI actually held a press conference. It hit the headlines of all of the major newspapers. It was on the TV. It was on the local news. It was on the national news.

It was something that really got the attention by using the mass broadcast media, which as I indicated before, we found that in the survey we did respondents were getting their information from TV still, and that's the average consumer that that's where they're hearing about problems.

Incidentally I would like to say that that survey is on the Stay Safe Online.info web site. You can link to it from the web site.

MS. FRAKER: Hi. My name is Mary Faker. I'm from Powell Tate, and I have quick questions for Tatiana and I'm sorry, is it Bernhard?

MR. MEISTER: Yes.

MS. FRAKER: Tatiana, and I apologize I don't have AOL and I also don't have broadband so that may be the cause for my ignorance.

My question for Tatiana is someone this morning mentioned that there's some aspect to Instant Messaging that can somehow make the recipient of the Instant Message more vulnerable. Is there anyone in here that

can say that better? I'm not sure if it breaches a firewall or what, but apparently there's some --

MR. FOX: There's file exchange options in Instant Messaging.

MS. FRAKER: Thank you. I was wondering if this is a potential with AOL Instant Messaging and if so, is that one of the sort of warnings or advisories or whatever that you make available?

MS. GAU: The file sharing functionality on Instant Messaging is actually something that is optional. It is not automatic. Somebody earlier mentioned the tip of turning things off if you don't use them. That's one approach to it.

With AOL's Instant Messaging system, we actually have a series of permission windows that will alert the user as to what exactly is about to happen, that somebody wants to share a file with them or wants to get a file from their computers asking for a file from them where there is no way that that consumer can just by accidentally hitting the return key cause that to happen, that we make sure that they are fully aware with messaging, with pop ups that interrupt their screen, so to speak, to tell them this person is asking to send you a file or is asking for a file from you.

So to that extent, we try to prevent the situation from ever getting into a problem situation, but to the extent that the person ignores the messages and just willy nilly agrees to accept files from strangers, they are going to be at risk.

MS. FRAKER: Is there some kind of a warning? Is it a yes no thing, or is this some kind of warning, You may not want to do this because?

MS. GAU: There is a warning.

MS. FRAKER: My question for you, sir, is we've gotten a million calls from people offering us Verizon DSL. Does Verizon DSL have a firewall or at least in the process of becoming a Verizon DSL subscriber, would I be advised of the need for a firewall?

MR. MEISTER: That's not my part of Verizon personally, so I won't try to tell what's going on there, but I know for a fact that there are lots of discussions and lots of activities in this arena because we also use this technology extensively. We have many home commuters who take the opportunity to dial from home, and many of those people dial from home using broadband connections.

So we as a large corporation are moving actively in this sort of arena to protect our customers, and I

would imagine that the Verizon online folks are working to protect the online DSL users as well.

MS. LEVIN: Hi. My name is Toby Levin with The Privacy Council, and I have a question regarding the technology skill gap. Consumers have been given the blessing of computers in their home, but with that there's a major technology skills gap unlike the car where consumers can just take drivers ed.

They can take classes, learn how to drive a car and they're off. When there are security or issues regarding safety, they pretty much can rely on various sources for information to address those concerns.

Well, with regard to computers, here's the technology that is probably at least as sophisticated as automobiles, if not more so, but yet consumers aren't equipped to really handle all the security repairs and safety issues involved. How do you address the fact that -- is this a short-term problem or a long-term problem?

Will consumers with the education that you're suggesting that's underway, is that enough to really address the security issues given the sophistication of the tools that they now have at their disposal?

MR. JORDAN: I know you're going to hate this as

an answer but it depends. I think that right now actually we're in the stage of a thousand flowers are blooming, whether it's in terms of policy, whether it's in terms of threats, whether it's in terms of vulnerabilities, whether it's in terms of different product lines, I think there are a plethora of web sites and available tools that are out there.

The problem that you have is that because there is a wide range of tools out there doesn't necessarily mean that there's been a shake out of what the best ones are for the particular groups. I think that a market idea that there may be a market solution for this, whether it's the establishment of businesses that they come and check your security for your home every month or something like that or some kind of outsourced business administrator, things like that will start to evolve.

And just as you have your pest control exterminator come once a month, you'll have your virus and online pest control exterminator come once a month. Who knows what the long-term solutions to that will be, but I think that right now we're in the growth stage before kind of the shake out of consolidation.

These are not mature industries. We're talking

about industries that are what, a decade, two decades, three decades old at the most? This is a process that's still evolving and rapidly.

MR. KELLOGG: But, Steve, when you also think about the tools available out there and you look at tools two years ago versus now, the fact is they are a lot easier to use than they were, and they're getting easier to use. The technology is moving very quickly.

Always when we talk about this point, I always think about an older family relative of mine who started using a computer several years ago. He is of the greatest generation and so he came into computers late, and then he started using them and get interested and do a lot of things with them.

But it took him awhile to understand that with that came responsibilities, and then when he understood that, gee, this is really -- these things are just hard to use, well when he actually started to try to update his system on a monthly basis and then on a weekly basis, he then found out that they weren't so hard to use.

So it gets back to what we were talking about, increasing awareness and getting over that barrier, sort of the lack of education out there, whether it's among

consumers, small businesses or medium businesses, there's just a lot of fear there, and it's going to take time to overcome that, and it takes a real effort, and that's again what we're trying to do in this industry and what I think we're seeing in government as well in partnering with us.

So it's important to remember that this is going to take time, and it's nothing we can immediately overcome.

MS. BERGER: On that note, I can take one parting remark from a panelist, and I see two of you leaning forward to grab it. I think I happened to see Tatiana first, and then we'll have to close this panel and move immediately into the next one hour segment. There will be a break after the next one hour segment.

Tatiana?

MS. GAU: Actually in summarizing your comments, I agree with everything you said, but I think that the consumer is never going to be inclined to learn all the details about what's going on in the computer. It's like in the car. I mean, I know I have an air bag system, but I don't care to know about the technology behind the sensors that's going to set those air bags

off.

I just want to know those air bags work, and I base my decision on the company from whom I buy the car and the assurances they make because I trust them as a brand and as a company that they'll do the right thing.

There is a lot that companies in the Internet space and the technology space right now can and could be doing on the back end to help protect consumers. We do a lot of that, and as I mentioned already, we rely on customers to tell us what problems they're experiencing in order for to us respond to it, but there's more that could be done in that area, and I think that is what is key, combined with education as to really simple, easy to remember tips for the consumer.

We can't overload them with heavy technical detail at this point. We've got to take some responsibility through our online industry associations, other kinds of trade associations, partnerships with government and things of that sort to really get the word out.

MS. BERGER: I would like to thank each of our panelists for participating this afternoon. Thank you.

(Applause.)

PANEL III: WHAT EXISTING BUSINESS MODELS HELP CONSUMERS MAINTAIN SECURITY?

MODERATOR: LAURA BERGER

PANEL MEMBERS:

SCOTT CHARNEY, Chief Security Officer, Microsoft Corp.

STEPHEN COBB, Senior Vice President, Research & Education, ePrivacy Group

SIMSON GARFINKEL, Chief Technology Officer, Sandstorm Enterprises

JAMES C. PLUMMER, JR., Coordinator, National Consumer Coalition Privacy Group, Consumer Alert.

MS. BERGER: We're going to move ahead in just a minute here to begin our next panel.

I'm Laura Berger. I'm going to continue as your moderator for the next panel and introduce the panelists. Well, this panel is going to -- in the last panel, we were talking about what consumers' need to know and how to get them to know about it, to educate them, and now we're going to talk about business models

that businesses can use to get consumers to start doing them, to get consumers to start using security products and incorporating security into what they do.

And immediately to my left we have Scott Charney. He's chief security officer for Microsoft Corporation, and on his left we have Stephen Cobb, senior vice president for research and education for ePrivacy Group.

Going down the line again to the left we have Simson Garfinkel, chief technology officer, Sandstorm, and an author of among other things Web Security, Privacy and Commerce and also of Database Nation.

And on the far left we have James Plummer, Junior, coordinator of the National Consumer Coalition Privacy Group for Consumer Alert. So I would like to welcome you all, and as with the last panelist, I probably won't have to cut people off as I did on the next panel, but we're going to go with the same format of just discussing with questions what we've been talking about.

So just as a segue from the last panel, to start with, what is the role of education in getting consumers to use security products?

MR. CHARNEY: I can certainly start. Education

is the key. I've been in the security space for 12 years. Threats aren't really -- or the risk of having something is very small and at PricewaterhouseCoopers, we talked to enterprise customers or even home users, especially those with broadband because we're seeing broadband home access for the first time, and you say, Look, you have to really be concerned about your security and they go, why.

And you can show them specific cases that we've worked over the years of serious hacking. You can show them surveys by the American Society of Industrial Security, the Computer Security Institute.

The statistics are there, yet people still continue to say, I think the likelihood of me being attacked is very small, and they'll go somewhere else, and this isn't a real threat, and because of that they don't deploy security.

So the first step has to be education. People have to recognize that these threats are real, that there are practical steps they can use to mitigate their risk, and then they have to implement those steps, and I think -- then I'll turn it over to other panelists, but I think part of the problem is that this information technology threat is not very intuitive.

Life is all about risk management. You can walk out of this proceeding and get hit by a car and killed. It's unfortunate, but it happens every day to somebody, so you go to the corner, wait until the light is green, and you look both ways before your cross.

You exercise risk management, but that's intuitive. When you're talking about technology, it's not intuitive, and therefore far more education is necessary.

MR. COBB: I'm going to pick up on the automotive analogy because they seem to have been running as a theme through today, and I was struck by the earlier comment about only one in ten DSL vendors providing a firewall.

It was like selling a car without seat belts and airbags, but I think the education analogy is closer to the ad you see for the kid in the car who's going, I don't know how many miles an hour, and he's shifting gears, and you see the tachometer, and this car looks great, and every kid wants to buy one.

There's a little message down at the bottom that says, Professional driver on closed circuit, do not attempt, and I think vendors in this space have a problem, a dilemma, if you will, in that we want to say,

hey, dude, you're getting a Dell, but we don't necessarily want to say, Hey, dude, you're getting a virus.

And you have a dilemma as a vendor, which I sympathize with in terms of pushing forward the technology, and the advantages of the technology, at the same time making people aware of the risks of the technology, and so I agree certainly with Scott that there is this problem of perception of the risk.

We were talking about this at lunch, about putting numbers on what it costs you, even as a family to have a virus problem, and I again spent many, many years in the business and numbers upon numbers each year, and we do get better numbers I think now than we used to.

But quantifying the risk in terms of numbers may not necessarily be the way to go for consumers. I think if you had video of people stressed out over losing their information that might be close to what I see on the consumer end of things, but certainly a way of getting across to people, I think someone in an earlier panel mentioned the seat belt analogy and the gruesome pictures, possibly the video of the stressed out user who's lost all their information due to a virus, is that

analogy, carries that over.

But the problem -- and in approaching the panel I was thinking about the question of the business model, I'm not quite sure who is going to pay for the education that's really going to say, well, there are down sides to the technology, so I think that's possibly a role for independent parties. There are industry associations, organizations like TRUSTe who play kind of an intermediate role in the technology to step forward and explain that side of it.

I don't necessarily think it's even fair to ask inventors to go too far down the road of saying, Well, what we're selling you is dangerous because if it is used properly, it need not be dangerous.

MS. BERGER: Does anybody want to chime in with any examples there might be of businesses educating consumers about risks associated with products? Simson, did you want to speak to that point?

MR. GARFINKEL: I'm sorry, I was going to finish.

MS. BERGER: Go ahead. I can raise that again.

MR. GARFINKEL: Thank you. I wanted to say that throughout all of today, we've had a real "blame the user approach" in this conference, this workshop, and clearly

it's the user's fault so they should be blamed, but I'm not sure that that's entirely fair.

Earlier the questions like why don't the people selling DSL connections supply a firewall with the modem, and that's a good question but a better one would be, Why don't they program their routers so that firewalls are not needed? Why don't they program their email system so that they're doing virus scanning so virus scanning isn't needed on the desktop?

Making a business case for increased security services was mentioned earlier. One problem that we have with the increased security services for the users is that the companies that are trying to make money selling Internet services are systematically sabotaging attempts to have increased security and privacy.

You may remember that back in the 90s we had a huge public education campaign about the importance of digital certificates and the little lock at the bottom, but Microsoft and Netscape both refused to modify their browser so that the certificate name, the CN, would be displayed.

And now most of the companies that are doing secured web sites don't do their own credit card processing, so the HCPS is going to a third-party.

One of the earlier panelists said that a huge problem that we have is web sites going up, looking like they're from IBM but really being from like somebody in Korea. The whole digital certificate infrastructure was supposed to prevent that, but the way that the web has been commercialized has defeated those security measures.

So you asked how education and how business models can bring back -- give us better security, and I think that in one part we're blaming the wrong people. I think blaming the user is a lot of fun, but I think that the real business is going to be made off of bringing back the security that we knew how to build in in the beginning and that we haven't built in for reasons of misguided attempts at usability or trying to make quick money off of users instead of doing the hard work and developing these services.

MS. BERGER: Okay. So we're starting to frame this discussion a little bit more in -- wherein Simson's remarks are trying to frame it a little bit more or try to keep framing it in terms of business models for doing this, for getting consumers to expect safer products or being able to through your business deliver safer products that consumers will be interested in adopting

and will, for example, be willing to pay more.

As someone suggested this morning consumers might be willing to pay more for a safer ISP. What are the sort of ways that businesses can bring these products to consumers and consumers will be interested in selecting safer products?

MR. PLUMMER: If I could get in the initial questions about education. I think what businesses should look at is why consumers are on the Internet, and consumers are on the Internet for two reasons. One is for convenience, especially for consuming and actually buying products, and to gather more information, information on things that interest them or entertain them, and unfortunately many consumers just aren't that interested or entertained by treatises on 32 bit encryption security.

So you have to try to get -- take advantage of the consumers' need for convenience but yet acknowledge their reluctance to get deep into technical details and add both of those in you're thinking when you're trying to get consumers to harness security and more security education.

For instance, the Dell came up earlier. I just got a new Dell laptop and that came with demo-ware of

Norton anti-virus, and that was free to me, and any consumer who has not had an anti-virus program before, they get this free run for 90 days. They will, as has been mentioned before, get an education on exactly how many viruses might come into their email, provided the number.

So I think that one way is to do it is if you're selling security products is to just show -- show what your product can do, and you can do that for free by demonstration ware or take another model, for instance, some alarm firewalls and probably other firewalls have a home use option that it's free, and that way the consumer gets free use of the security software, but if he's the kind of person that makes decisions or is influenced on the decisions for his business which is what they're hoping by giving away the free software, you have to take that knowledge to the office and maybe use that same product at work.

So that's just a couple initial ideas on education.

MS. BERGER: Okay. Scott wants to follow up on that.

MR. CHARNEY: Well, yeah, I think as a practical matter, there are a lot of people who go out and shop

for other things like cars that may not know what a fuel injected engine is or may not understand automobile engineering but will buy a Volvo because they perceive it safe based on a safety campaign and maybe even independent tests.

So I think as a practical matter for vendors of products, the key is once consumers are educated that they actually do need to take security seriously and that they should be investing in security products, how are they going to go out and buy those products?

Well, they're going to do it like they other do other things. They're going to look at brand and business integrity, and certain brands have a certain level of trust. They're going to look at ease of use of the product and how easy it is to install and manage.

And they're going to look at independent testing, to the extent groups test different products and write magazine articles or do some consumer reports on security products, they're going to go and look at those and say, Which ones have the red circles, which ones have the black circles for ease of use, the number of threats that are covered, how easy they are to maintain and the like.

And I think we sometimes got bogged in saying

consumers have to understand all the nuances of the technology but I'm not quite sure that's true. I'm not sure they understand all the nuances of how automobiles work, but there are still metrics that consumers use when they go to the market, and I think we should look at that in this space as well.

MS. BERGER: Okay. Simson?

MR. GARFINKEL: One of the problems is there isn't a good alignment between where the money is being made and where the security is. The people who are selling the most insecure products are making the most amount of money in this consumer space.

The Microsoft products are the least secure, and people are making the most money selling them. The Apple products are more secure, and it's a much smaller market segment, and the Unix products, Linux, the free software ones are even more secure, and there's even less money being made there.

So there's a whole problem trying to use the market, except for like the tort system, to reform us. It's much closer to how do you regulate the tobacco industry than how do you regulate the car industry.

MS. BERGER: There's going to be a separate panel on legal standards and standards for regulation,

so just if we can stay focused on the business models for this panel.

MR. COBB: That's the difference between Scott and Simson. I mean, I hear what Simson's saying. I think -- I mentioned for somebody who spent 15 years looking at all of the things that can go wrong with these things, I'm actually quite optimistic because what I've seen over the years in security is that it's all about timing.

And you could have had a great idea for a security product five years ago, and nobody would have bought it because there wasn't sufficient critical mass in terms of understanding what the problem was, and although we've been really sort of drowning in the woes and the problems which are certainly real at the moment, I do sense a rising tide of understanding in the marketplace amongst the consumers.

And I do think the pressure that really led for say, for example, Volvo to succeed with the idea of a safer car, I think that may well arise, and that market pressure I think will have an effect, and I think we would have to acknowledge that Bill Gates did send this memo around at Microsoft saying, We have to focus more on security than features, and I don't think he did that

out of a sense of patriotism.

I think there's clearly a business model in which or an economical model in which people's dissatisfaction with things reaches the point where they stop spending money, and I think a smart business model for some company might be to fund an independent third-party to put out ads about all the terrible things that can happen to your computers and some of the steps you can take to solve them while at the same time marketing a product which they stress the security of.

Not to be cynical about it, but I think, yeah, one way or another there's going to be an increased consumer pressure for better, safer products in the space and companies are going to respond. I do see waiting in the wings legislators and regulators that are concerned that the consumer is perhaps getting the raw deal.

MS. BERGER: Scott?

MR. CHARNEY: I think it's important to note two things. People don't buy products just for any one feature, not just for security, so even people who buy cars who might want a safe car wouldn't buy a car that has a great safety rating but breaks down every two months, so consumers are actually more complex than

that.

But I would say we see a synergy of two different things happening, that I completely agree that I'm very optimistic about the future and the synergy is this: On the one hand, you finally have markets demanding security, and if the Justice Department kept going out and telling people that cyber crime was a huge problem, they kept saying, no. Now you don't hear that anymore.

And to the extent consumers and enterprises demands security, then the market builds security, but the second thing which is also very real is the threat model is changing. If on September 10 you said to me, What are the odds of four planes being high-jacked, three of them hitting buildings and two World Trade Centers collapsing, I would say the threat of that is almost zero.

And then this happened, and as a result of that and Code Red and NIMDA and a bunch of stuff, people are reassessing the threat model. We're throwing out what we assumed were givens and we're reassessing, and the result of that is a lot of companies -- I mean, there's no question that Microsoft sees a market in security.

But Microsoft has actually been working on

critical infrastructure protection systems for quite a long time, and we are now escalating that a great deal, and let's face it, I'm a cost center to the company, but we're doing a lot of stuff, and a part of it is not just markets but public and social responsibility.

We have to protect these infrastructures or we're not going to have the society we aspire to and you're not going to protect these infrastructures without insecurity, so we have to get it right for a host of reasons, and that now a combination of markets, threat models, critical infrastructure protection, there's a lot of reasons to think that everyone at every level is going to take this seriously, and we are going to start moving much faster down a path in the right direction.

MS. BERGER: Yes?

MR. PLUMMER: If I can follow up on a couple things that people said. I think a lot of things that everyone said make sense when seen together. The importance of brand names was mentioned, and that's very true, and Microsoft has indeed got a reputation for security over the last three years, which is why Bill Gates is having this big push to increase security.

So Simson definitely had a point there, and it is true that consumers are complex, not just looking for

security but for other features, and part of the reason why Microsoft has been more vulnerable is that's what almost everyone uses so that's what most of the viruses are written for.

They're written -- I have Windows myself but I don't use the Outlook email system. I use Eudora because many of the viruses are written -- they'll go off easier if you have Outlook.

So that's another thing that as far as brand names go, first of all, it's a good idea for consumers to diversify where possible on their home computers, and if everything is linked and one thing goes down, then it all goes down, but companies like Qualcomm who have that advantage, they should advertise it.

If companies think their product is more secure and they honestly believe that, they should advertise that. Earthlink should advertise the fact that they're a lot less likely than say AOL to just turn over all your information to the first guy with a badge that shows up at your door, so these are all very important things to talk about.

MS. BERGER: I want to turn the discussion a little bit. We've been focusing on security that's embedded in software and saying consumers don't just buy

a product for security it can offer them.

What about business models where you actually just sell supplemental security products, are those an advantage for consumers?

Simson?

MR. GARFINKEL: I have a real problem where you're selling a product, and then there's an additional product that you need to buy to make it secure.

MS. BERGER: Assume there's a separate vendor.

MR. GARFINKEL: If it's the same vendor or separate vendor, I think that's anti-consumer, and I think that products should be delivered that are secure. I also think that in the field of computer security, it's very difficult to advertise that one company is more secure than another, and I didn't mean to attack Microsoft earlier. I only meant to attack their software.

The problem is that all the software that's out there has security vulnerabilities, and if you advertise that your product is more secure and then a vulnerability is found as invariably an -- as invariably the vulnerability will be found, you look like you are a liar or a cheat, and this is really difficult for the companies.

MR. COBB: But I think -- I don't know that it's necessarily reasonable to expect every threat to be anticipated by a vendor. If you look at the development of say anti-virus software, neither the hardware companies nor the application companies or the operating system companies sold anti-virus software in the early days because there were hardly any viruses.

Then as viruses became more prevalent, people gave out the anti-viruses to fight them, and some of those companies are still around selling that as an add-on. In fact Microsoft introduced a form of anti-virus in DOS 6.something, and it didn't stay in there very long.

So I would say that there is a valid market for an add-on product. It is addressing a threat that hasn't yet been internalized by the software, but on the other hand, I would agree that there is a base level of security that consumers should be able to expect from their hardware, software and applications that right now we're not seeing.

MR. GARFINKEL: See, what I would like to see instead is more emphasis on services. Now, the anti-virus people are actually doing that, and they have largely migrated what they offer from being a program

that you buy to an update service, and I would like to see more kinds of services like that. The single biggest problem that consumers have with their computers is that they do not back them up, and there should be better emphasis on back up services and back up products like that.

A second huge problem is data sanitization. A few years ago I bought some used computers, and let me tell you what I found. One of them had been used by a law firm, and there was a lot of confidential client attorney privileged information on it, and another had been used by an organization that delivered mental health services, and there was a list of names and diagnoses.

Those machines when they were sold to me, they should have been sanitized. There is one or two companies that actually are doing this for a business, but there is very, very few of them, and there's very little information out there for consumers on how to properly dispose of a computer. There's a lot of erroneous information such as you can't ever erase all the information, which is just not true.

MS. BERGER: So what's a -- framing this again in terms of business models, how would a business be

able to encourage a consumer to take steps when disposing of a computer to make sure that it's sanitized?

MR. CHARNEY: Part of what I'm hearing, it comes back to your first question about an education problem. There's been file wiping utilities on the market for a long time, and I agree that people need to use them, and there have been well reported cases of companies sending machines to surplus or put on the secondary market that haven't been appropriately wiped.

I think Washington Mutual was one of them, and there have been others, but the utilities exist to do that, and it's interesting that in my days at PricewaterhouseCoopers when I was doing security consulting how we kind of assume that at the enterprise level, the IT staff is just incredibly competent. They can get everything done, and the reality is that's just not true.

This technology exploded far faster than our educational institutions could train people to do this technology, and I'll give you a real life case in point. In 1991 when I became chief of the computer crime unit, I went to Johns Hopkins with a colleague to take a course on networking in computer security because

I now had this new tasking, and he and I are in this classroom which was taught by an instructor from the Defense Department, and we were there with 12 women, all roughly 22 to 24.

And the instructor wanted to go around and say why were you taking this course, and my colleague and I explained that we were now prosecuting this stuff and needed to get a handle on what we were doing, and as they went to everyone else it was, I was a secretary in the medical department, I was really good formatting documents, they've now told me I'm the LAN administrator.

Each one came from a different division at Johns Hopkins, so one of the problems is sometimes the tools are there, but the people are not appropriately trained to handle this, and of course it gets even more difficult at the consumer level.

We don't have a unified user base. It's not monolithic, so when my mom went on email that was great. When she started thinking about broadband and I tried to explain firewalls, the conversation went downhill pretty fast, and so even at the enterprise level very often the people -- the tools are out there in the marketplace but the business processes are not in

place to do it right.

People aren't educated enough to do it right and they don't audit the processes even when they're supposed to be doing it to make sure it's actually being done right. So there's a lot of things at the enterprise level that businesses have to do.

On the consumer level my view is that vendors and service providers have to do more because I don't think -- we can educate consumers on the threats. They can go into the marketplace, but this technology, we do not yet have what I call security usability. Security is just not that simple to use yet. We have to get it there.

You know, you buy a hair dryer. In the old days you bought it, you look for that little UL label on the cord because you didn't want to electrocute yourself, and that UL label said it was safe, and you went home and plugged it in the wall. Now you go out, you buy a hair dryer, you plug it in the wall, you don't think about it.

We all know electricity is safe. We all know hair dryers are safe. Nobody thinks about it. That's where we need to be with computer technology. We are not there yet. We will not be there for some time, but

we have to work in that direction.

MS. BERGER: We are going to move to Q&A in just a minute here, but I wanted to talk about just one more type of business model or product to get consumers to secure their own computers. We have talked a little bit about supplemental security products and what role they might play and in improving security and security that's included in software.

What about transaction based security products, what kind of role do those have in getting consumers to set up their computer?

MR. COBB: You mean securing transaction as they occur?

MS. BERGER: That consumers might conduct, yes.

MR. COBB: I think if you're talking about increasing the level of security, some of the speakers this morning talked about two factor and three factor authentication, moving to that level.

I think it's interesting to see what's happened in the marketplace where we've had initiatives like the blue card from American Express which is a smart chip which as far as I know isn't actually being used as a smart card at this point, and I have a sympathy for vendors that have pushed them.

I had an account with the Royal Bank of Scotland which is one of the first to push out digital certificates to use. This was a number of years ago. Unfortunately, it was very, very complicated, and if your computer sort of died for some reason, then it was a whole series of phone calls to get it back.

And yet you had to admire them for going that extra mile. I think it's a difficult one because if you're going to push security to the point where it involves another layer of inconvenience and it's conceived as that by the consumer, then you've got resistance. I think possibly industry wide initiatives to kind of raise the threshold might be in order.

MS. BERGER: So there's some tension there for consumers because businesses have some hesitation to implement the extra steps, but at the same time you want consumers to have an incentive to look for those kind of guarantees.

MR. GARFINKEL: The real problem is that we've traditionally framed security and ease of use in opposition to each other, and the very best security is security that actually improves ease of use rather than makes it harder. There are ways to do this in the electronic transaction era.

For instance, your ISP could offer some sort of enhanced security service that works with the merchant that you're buying from and like feeds off quality ID or feeds off their radius server or something, but that's really hard to get working, and nobody's even thinking about that right now.

I do feel that there is a future out there that Scott's talking about where the systems are more secure and where they're easier to use and people are making money off of this and nobody can do any bad things any more, but I think it's going to be much harder to get there.

In the meantime I think that we need to hold the people providing the software more responsible. For instance, there have been file wiping utilities, but I should be able to tell the operating system that I'm selling the machine now, please self destruct and it doesn't have any system for doing that.

MS. BERGER: Okay. I'm going to have Scott comment on my question, I think he was ready to, and then we have a line of questioners waiting.

MR. CHARNEY: I think to some extent it depends on the transparency of the user. You can compare, for example, SSL to protect credit card numbers in transit,

and there has yet to be a documented case that I know of where a credit card has been stolen in transmission because of SSL, the consumer has to do nothing at all compared to the AMEX blue card where I talked to AMEX years ago and they said, Well, the problem is if you get the AMEX blue card, you can call us up and we will send you a free credit card reader, and then we get calls from consumers saying "it says plug into parallel port, what's a parallel port."

These are the same consumers who when CDs came out they called the vendors up because they couldn't get the cup holder to retract, so a lot of it depends on the way in which this stuff is implemented and to what extent consumers can use it easily or specifically without even thinking about it like SSL or to what extent do consumers have some role to play in implementing the technology.

And if it's a technology that needs to be implemented like two factor authentication, there's a big difference between building it into the keyboard, a card slot, and giving them a third piece of hardware which has to come out of a box, be connected or driver installed.

This is not the same thing so we have to focus

on making security usable.

MS. BERGER: Thank you very much. Questions?

UNIDENTIFIED SPEAKER: In terms of speaking of business models, as a consumer. I have a problem with business models. Everyone has focused on a lot on Microsoft, not to beat up on your company too much, but in the bundling of the services, I loaded a firewall from a completely or at least I think it was a completely independent service provider.

And one of the things I was disturbed about was not only how many times my computer -- people sought to access my computers but how many times Microsoft XP products would automatically access the Internet to report on God knows about my computer from jukebox to you keep going down the list of the products that I have to keep having to say no, no, no, no.

And I wanted to see if the panelists could comment on kind of the conflict of interest that can exist between companies that are configuring their computers to report back on what the user is doing and their providing a firewall to prevent access to the consumer's computer.

MR. PLUMMER: If I can say, that kind of goes back to the thing I said earlier about trying to

diversify and not put all your eggs in one basket. As a consumer I have a non Microsoft firewall and it's already telling me about my Windows media player and other things that are trying to tell Microsoft something, and I always hit no.

So the consumer should definitely be aware if they're getting everything from one place to know what they're doing. I think Simson was advocating earlier that broadband ISPs should provide more security features. That might work for some people, but I think for more sophisticated users, they don't necessarily want that.

They want to have -- they don't want the ISP. For one thing it can be inconvenient when it's running everyone's mail through three different filters, but I think kind of dividing what you're using among -- diversify is my point.

MR. GARFINKEL: I think it's important to pick the right battles, and one of the problems with these firewall home products is they cry wolf because they want people to think they're doing a very good job. All the times that Microsoft products check for feature updates are treated like attacks, and in fact you want the Microsoft products to check for updates because

frequently those updates are to deal with security problems.

And Microsoft is doing the right thing by having its products checked for updates' use, so it's important -- there is so much misinformation out there that I'm very troubled about.

MR. COBB: I let my machine talk about Microsoft in the XP instance because quite frankly I don't think of them as the evil empire, and I think it's a question of trust, and I think that that's probably one of the key elements to building the new economy is the aspect of trust.

I think if I trust that they're doing this for legitimate reasons, and I really don't think they're scanning my hard drive for credit card numbers because last I heard they had 40 billion in cash on hand. But as Simson says, it's a question of education, and this is one of the things we're going to have to watch as we move down that road in consumer education.

And one of the things my CTO was pointing out to me before I came down here was that the traditional model in security back in the corporate days often as far as selling was fear, insecurity and doubt. You tried to scare up business, and I wouldn't want us

to go down that road in terms of over selling the product to consumers.

It's a question of making them aware of what are legitimate issues and helping them distinguish between something that shouldn't be coming out of your computer and something which is legitimate.

MS. BERGER: Next question.

MR. KRAUTHAMER: My name is Michael Krauthamer, and my question is with regard to transactions and the potential use of biometrics for authentication. If a credit card number which is currently stored on file for the purpose of comparing with the number that the user submits to make sure it's legitimate, what happens when or is there a problem with biometric information being stored on a server for use of comparison with what the user submits?

MR. COBB: If I could leap right in on that one.

MR. GARFINKEL: Are you going to raise up your credit card with a biometric on it?

MR. COBB: No, that's a picture on my credit card which I though was cheap, free, simple, easy working for them, works for me. I didn't have to have this on my credit card. They took the picture at the

bank, put it on there, and when the Royal Bank of Scotland put pictures on their credit card, fraud dropped 70 percent.

There wasn't any need for Bank of Scotland to store the pictures on a server somewhere, and I do want to make the point on biometrics that it isn't necessary for a central server to store stuff in order for biometrics to work. I could have my fingerprints stored on there, and nobody else would have it. You would just check that it hadn't been changed since it was put on the card.

And I would really like to get out the message that biometrics isn't necessarily a big brother assembling all this personal data about it. For example, fingerprint biometrics is not the same thing as the FBI stores when it takes your fingerprints, so again it's a question of education.

I think there's been a real problem selling the public on biometrics because this specter of having your identity stolen even more arises. If it's done properly it doesn't have to be a threat.

MR. GARFINKEL: The other thing about biometrics is that they are, maybe people do -- every biometric system has a back door. They all fail. They're all probabilistic systems that tell you how close the match

is, and the company then is using a test to make a decision about what sort of thresholds or tolerances they want to accept or not accept.

So we see a lot of -- the other thing about biometrics is that they're not democratic. Some people will not print with the system. Some people, the live scan fingerprint readers just don't work or the iris scan readers just don't work.

So when we deploy these biometrics systems, we have to be sure they're backups or ways of doing the transaction without the biometric. There is so little understanding about the use of biometrics, even among biometric practitioners out there and there are so many people trying to make money selling their particular biometric system, I'm very hesitant to see something deployed for 300 million people.

MR. PLUMMER: Just to follow up, Simson is right about the back door vulnerability. All these systems are vulnerable. I do think at least for the foreseeable future, the security responsibilities on the -- it's the onus of the vendor really, not the guy sitting at home trying to buy something.

The SSL system seems reasonably secure with credit card numbers and transmissions. I read a report

this morning that fingerprints are basically easier to crack than good user names or passwords, and I don't think most consumers are going to be happy about getting their eye scanned to buy a book off of Amazon. I think it seems quite ridiculous.

MS. CLAY: Hi, Alicia Clay from NIST. I have just a quick comment about biometrics going to the last question. One of the things I think that we need to be aware of is that outside of the computer security world, people are starting to use biometrics in places that are completely unnecessary. I should not have to give up my fingerprints or to cash a check or to rent a U-Haul truck, so --

MR. GARFINKEL: That's to protect your bank and to protect U-Haul.

MS. CLAY: So I realize that if I don't return that truck, they can dust the entire world for my fingerprints and try to track me down.

MR. GARFINKEL: We want to prove it was you when you don't return the truck.

MS. CLAY: Not that they have my fingerprints already, so that they still can tie that thumb print to Alicia.

MR. CHARNEY: You need to be careful too because

a lot of these technologies, it's not capturing the actual print. It does a mathematical -- it's not like leaving a print on a table, right. It's a little bit different, so depending on the implementation, your print may not be nowhere at all.

In the example you gave where you compare it to a credit card for example, the print's not in a centralized database. It's compared locally for you, no one else has it so we have to be careful of that too. We make sure we understand how the technologies work of course.

MR. GARFINKEL: What the banks are doing though which I kind of liked was when somebody went to cash the check who didn't have an account at the bank, they put the person's fingerprint on the back of the check itself. That was like with ink, and then if there actually was fraud, if I say I didn't write a check to that person, my checking account was stolen, then they have the fingerprint, the video surveillance and the next time that person comes in with the stolen checkbook they can nab them.

If you actually put an ink print on the U-Haul contract and then the truck is not returned and they call you up and they say, Someone using your name rented

a truck and never came in, then you can give your thumb print and show that it's a different thumb print, so it's to protect you.

MS. CLAY: I want to talk to you more about that off the record.

MR. PLUMMER: I wasn't aware U-Haul started requiring fingerprints.

MS. CLAY: In certain neighborhoods.

MR. PLUMMER: The ultimate thing I can say consumers can do is go to Ryder trucks, just go with your money.

MS. CLAY: That's what I did but my actual question I have for Scott really. Scott, one of the things you mentioned was it would be good to have a UL label for secure computer use. That's something that we should be working towards.

MR. CHARNEY: I did not say that. I said that in the early days for consumers when they were trying -- we were trying to get them to use new products, right, we had the UL label on electric cords to tell them it was safe.

Whether in this environment, I mean, there are a lot of independent entities that can assess computers and computer products and all that, so I'm not

suggesting it would be one centralized thing, but I think consumers do look for independent evaluation of products as part of their purchase of choice, and I think that's healthy.

MR. GARFINKEL: We did the UL label, we did the orange book. You can come and buy an A-1 computer to surf the Internet with, and the problem with that is that the very secure systems are extraordinarily expensive to produce and they're not very functional, and you can't load new software on them.

So we could build -- the 30 of us in this room, we could build a consumer computer that would be absolutely secure, that would do the email and do the web and would never be able to take a new virus but they couldn't load any new software on to it, and that's the computer that's going to be sold in five to ten years once we have the feature set nailed down.

MS. BERGER: I think we have time for just one more question.

MS. FISHER: My name is Vicky Fisher, and I'm going to go back to the car analogy because I work for a car company, but when we're evaluating one car against another, we have a certain set of standards we use, how fast does it go from zero to 60, what kind of miles per

gallon does it get, and that gives us the criteria that we say, well, gas mileage is very important to me, so this car is going to meet my needs better.

Do we have anything like that that can tell us about what kind of firewall protection we're going to want for my life-style? Do we have any kind of standards that we can agree on so we can rate things against each other?

MR. COBB: I think if you look at a slightly more specialized computer press going beyond PC Magazine to something like Secure Computing or Information Security Magazine, there are product reviews and testing is done. I wanted to make the point on, for example, anti-virus software, what used to be the NCSA which I have to say at one point I used to work for used to test and ICA still tests anti-virus to a standard that's a published standard.

And I think when they introduced that, that certainly made a big difference to the market. I can remember it was a big instance where IBM started insisting that vendors be certified to that standard.

It's a little more difficult, I was involved in the formation of something called the Firewall Product Vendors Consortium, and Marcus Raynum, one of the early

firewall pioneers, did draw up a standard language for describing firewalls.

That got very, very complicated actually but I think there are publications out there that are testing products and giving you a product with ratings and so on and helping consumers judge, Is this the right level for me, do I need a $2000 box or a $50 Zone Alarm license.

It's not standardized though to the level that cars are, and that's never going to be the case, that it's just a much more than a vehicle.

MS. BERGER: I would like to thank each of our panelists in afternoon, and we'll begin the next panel at about five after three.

(Applause.)

(Break in the proceedings.)

PANEL IV: WHAT STEPS CAN BUSINESSES THAT MAINTAIN CONSUMER INFORMATION TAKE TO IMPROVE THEIR OWN SECURITY?

MODERATOR: ALICIA CLAY, NIST

PANELISTS:

MARTIN E. ABRAMS, Hunton & Williams

LYNN GOODENDORF, Six Continents Hotels
FRANKLIN G. REEDER, Center for Internet Security
VINCE SOLLITTO, PayPal, Inc.
VIC WINKLER, Sun Microsystems, Inc.
MARC ZWILLINGER, Kirkland & Ellis

MR. EICHORN: Hello, everyone. Our last panel today will be moderated by Alicia Clay of the computer security division at NIST, the National Institute of Standards and Technology. She's on the U.S. delegation to the ISO/ISC subcommittees responsible for developing international standards on information security, and one of her roles at NIST is to handle regional workshops around the country, especially for small businesses about security and security awareness, so Alicia?

MS. CLAY: Thanks, Mark. Good afternoon. I was very excited when Mark asked me about facilitating this panel discussion because it does fit very closely with what I'm doing at NIST. Basically we are reaching out to small business owners, trying to teach them about information security.

As many of you probably know, the computer security division at NIST puts out a host of documents each year on information security, and about three years

ago we decided to see what could we do to help use some of that to help strengthen the information systems of small business, so that's what we're doing with this outreach program.

And we're doing that in cosponsorship with the Small Business Administration and with the National Infrastructure Protection Center, but in any case, coming here today gives me a great opportunity to be on the question asking end, so I get a chance to play devil's advocate, and I'm totally excited about that.

Now, by way of introduction, I'm going to give just sort of a one or two liner on each of the panelists here. You have their bios, I believe, in your packets, and we'll give each of them an opportunity to give us about five minutes worth of theirs view on security for business systems that are holding consumer information.

So first we have Marty Abrams. Marty leads the center for information policy leadership at Hunton & Williams. He is a senior policy advisor to the firm's privacy and information management practice.

Marty?

MR. ABRAMS: Super. Thank you very much. I should give a disclosure that even though I'm with a law firm, I'm an anthropologist and not a lawyer. I have

spent 23 years doing consumer policy, probably the last 13 or 14 doing information policy, most of that in the world of privacy, and I have long been interested in the interaction between security and privacy.

And when I was with TRW back in the days when they had a big information business, we used to talk a lot with the folks in the information security side of the shop, and those are the folks who do information security for the government and big large organizations, and we talked about the language and the objectives.

And one of the things that became crystal clear is that security is typically focused inward while the work we did on privacy was focused outward, that security was based on this concept of protecting assets of securing the organization, and in the world that I now work in, we're talking about pushing and helping consumers to serve themselves more than we serve them.

So I go and book my own airplane reservations at American Airlines. I book my own hotel reservations. I deal with all sorts of issues today over the Internet that I used to deal with people who would deal with that, so the whole question of consumer facing security has become a lot more important both to the organization and the business as well as to the consumer.

And one of the reasons that we migrate to serving ourselves rather than letting individuals serve us is because of the convenience, and convenience is the driver of the marketplace as we have seen it change over the last 30 years.

I often joke about the first time I applied for credit back in 1972. It took me three days to be turned down. Today we would not tolerate waiting three days to be turned down. Today we would like to be turned down in five minutes at the most, and we'll walk away from a vendor who doesn't allow us to do it.

So that when question think about the risks to us as consumers it's increasingly that in these interactions there's not just risk to the organization, but there's risk to us as well.

Very high quality consumer research that's really been unpublished said that there are three drivers of consumer angst, and the first is I want to be secure and I don't feel that way, and it had nothing to do with any of the things that we were talking about this morning.

It was talking about the whole world of identity theft and the driver of the consumer angst as it relates to security is ID theft. The issues that we're talking

about this morning are very far from where the consumer's mind is at, but what is real clear is that if we're going to revolutionize the way we interact with consumers so that the networks and infrastructures are more secure, it's got to be done in a way that does not interfere with convenience and is easy to use, incredibly easy to use.

It's got to be something that doesn't require an interaction on the part of the individual but rather it is like a tool that is an intuitive tool.

If we ask the consumer to act on their own behalf, both to keep themselves more secure and to make the network more secure, we will probably not succeed in doing that. A great example is my wife, and this is a privacy example, she is very privacy sensitive. She tells me that all the time.

And so I took our home computer and it's XP and I ratcheted up the whole question of the privacy setting, and two days later my wife, who is very competent and could do these things herself, said, You've got to get on the computer and change whatever it is that you changed and change it back. She says, I can't live with this constant interaction with the computer, clicking through and clicking through. The security devices that

we have to come up with have to be easy to use.

I think it was very telling on the part of Dick Clarke this morning when he was saying that security in the Defense Department is now a matter of putting a token into a machine, and that same token is the token that opens the door of the building, lets you get in to works. The computer can't work without that type of security.

It's easy to use. We're asking the Defense Department people to use something that is easy to use. If we're going to make security work for us and if we have a challenge in protecting the network and we have a challenge in terms of protecting the interaction between the consumer and business, whatever devices we have to do have to be from thinking outside the box to reinvent the way we think about security.

It can't be focused on our own assets. It's got to be focused on the needs and the habits and the liveability of the consumer.

Thank you.

MS. CLAY: Thanks, Marty. Next we have Lynn Goodendorf. Lynn has 26 years of experience in the technology profession with expertise in telecommunications and data networks. Ms. Goodendorf

assumed executive leadership of information security at Six Continents Hotels in 1999 and recently added responsibility for data privacy to her role.

Lynn is actually unique on our panel here in that she is completely on the user end of security and privacy products and services.

MS. GOODENDORF: Thanks, Alicia. I don't know if Six Continents Hotels is a familiar name to everyone because we changed our name about a year ago, and we own and manage and franchise Holiday Inns, Inter Continental Hotels and Crown Plaza Hotels.

All together we have about 3,200 hotels that are distributed across 100 countries, and all of those hotels with just a few exceptions are connected with data networks into our reservation system.

That same reservation system is then connected to our web sites. It's connected to travel agency networks. It's connected to a number of mechanisms or call centers, all for the purpose of making it very easy for consumers to inquire about a hotel room, to ask about a price and to book the reservation.

We also have a very successful customer loyalty program called Priority Club. We have over 12 million people enrolled in that club, and so we take the privacy

and the security of our customers very seriously.

A few years ago we made a tremendous investment in the physical safety of our guests in that we required all of our hotels to change their key door locks to the electronic locks, and so we have a history and a culture of being concerned about our guests' safety, and we're very committed to information security.

MS. CLAY: Thanks, Lynn.

Next we have Frank Reeder. Frank formed the Reeder Group after a career of more than 35 years in public service. Frank is chairman of the nonprofit Center for Internet Security and also chairs the National Computer Systems Security and Privacy Advisory Board of the National Institute of Standards and technology.

Frank?

MR. REEDER: Let the record show that's a pro bono, and the taxpayers are getting their money's worth. I'm not sure how to take that back.

But I would like to parse the problem a little bit differently because we've been distinguishing between businesses and consumers, and as I had listened to some of the previous panels, there's a scaling problem, and certainly the challenges that face

Microsoft are slightly different or the capacity to meet the challenges facing Microsoft are slightly different from those facing the small business.

And I would really like to focus my remarks on the small business and consumer because I think their problems are probably more similar.

The nature of the problems they face in this -- at the risk of repeating what you've already heard -- comes from several perspectives, first and foremost from within, from acts of vandalism or acts of inadvertence that run the risk of damaging security, security being defined as the availability, integrity and confidentiality of information, and also secondarily and obviously non trivially protecting themselves against acts of malice from people outside, hackers, a polite term for people who are a combination of thieves, vandals and thugs.

The consequences also are fairly obvious. One, financial loss, that is you can lose your money or your merchandise. In the case of a Six Continents, it might be you would lose your ability to sell rooms which is ultimately what they're in the business of doing, interruption of service, a business unable to operate and ultimately loss of confidence by your customers and

your ability to continue to deliver reliable service.

And here I risk -- I think the automobile metaphor is extraordinarily useful in several respects. We're dealing with a technology like any new technology that has the potential to deliver enormous value and good, we needn't belabor that, but with some unintended consequences and some potential risks that can cause and inflict great pain and loss.

To prevent that, we need to do a couple of things. Obviously we need smart people out there who can help us protect ourselves, but as several of the speakers have reminded us, there probably aren't enough smart people out there to populate every organization, certainly not when we start talking about our parents and grandparents' computers or mom and pop store computers.

So something else has to happen in this marketplace to assure that those folks don't become the victim of the technology that they're attempting to use for their benefit, so what can you do?

One we've already talked about, beat up on Microsoft and get it to build safer products. The reason we beat up on Microsoft is because they're the biggest and by definition, if you were going to hack a

product, you might as well hack Microsoft Exchange rather than something obscure.

It isn't obvious that their products are inherently weaker, they're just inherently more attractive to people who want to break into them.

In any event it's reasonable of us to expect the kind of commitment we're beginning to see from the people who sell us technology to deliver safer products but let's assume that away.

Let's assume for a moment that tomorrow we had the equivalent of airbag equipped, antilock brake equipped vehicles riding the information super highway. We would still be left with two other very large problems, one again as was discussed in the panel this morning, the problem of user education.

The UL metaphor is wonderful. Even if you buy the hair dryer that has a UL label on it, you need to know not to toss it into the bathtub while you're in it.

So it is possible to do harm with safe products and so the notion that delivering a safe product guarantees safety is I think a trifle naive and probably didn't bear belaboring.

Initiatives like say Stay Safe Online for

example are terribly important. We need to continue to push user education. We need to continue to -- and the safe computing metaphor I think is a very interesting and helpful one, but finally we also need -- and here the automotive metaphor I think is important, a series of things that deal with one, the problem of latent defects.

Even the safest product, especially in a field as dynamic as information technology today is likely to be rendered unsafe tomorrow by virtue of the uncovering of defects that we weren't aware of at the time it was delivered or by virtue of the manner in which the user applies that technology, and so you need to do a set of things that even if you were delivering the safest product assures that those products continue to be safe.

In the automobile space, we do periodic safety inspections, and we have product recalls when deficiencies are uncovered that are deemed to be of sufficient magnitude to warrant that kind of action. We place a responsibility back on the vendors. We place the responsibility back on the distribution system to correct those defects.

And the inspection metaphor I think is also

important from another perspective, and that is information technology systems are by their nature inherently complex, and it is imminently possible in the course of doing business to undue the safety measures that may already be installed in the system, and so periodic checking becomes very important.

As to what's available out there, there's a range of capabilities that already exist with respect to what we're starting to refer to as minimum standards of good practice. NIST is an important source, and in fact in our conversation prior to this one of the things we agreed upon as a panel was that we would provide, each of us, to the Commission a list of resources that we were aware of that it might -- that the Commission might put on its web site, without endorsing it, as resources that are potentially available.

At the risk of being accused of acting in self interest, I would like to mention just one of them just as an illustration of the kind of thing that can be done. About 18 months ago a few of us in a dark room across town conceived the notion of something called the Center for Internet Security.

The notion of the Center for Internet Security is very simple. That is that there is a set of -- that

most of the vulnerabilities that are being exploited in the Internet are very well known as are the remedies for those vulnerabilities, and that one of the things that we can do to contribute to the level of safety on the Internet is simply sharing through an open mechanism what is perceived to be the consensus on good practice.

Not at the level of generality that most of us understand, change your password periodically and back up your files, but at a level of great specificity, that is these are the minimum settings you ought to have in your X operating system or on your Y router.

We'll put the URL for the center on this list. This is not a solicitation for support. The center provides its products and its tools free.

The final point I would want to make, and here again I come back to the automotive metaphor, and I think it again echoes things that were mentioned earlier. We've got to start thinking about more passive restraints.

We have to, as other speakers have already indicated, start to use the technology intelligently so as not to require that every individual or every small business that operates technology systems needs to have expertise. We see folks in a -- I'm not doing this to

pander to AOL, I don't make any money from them. AOL has figured out how to push software out to you without your having to do anything. You don't have to be a systems administrator to update your version of AOL because AOL understands to do that.

The virus packages that I used Friday told me that Microsoft had three patches out for its browser and showed me where to go to download this with a simple click. It didn't require me to do anything except to respond to a notice that I already got because I'm not prepared yet to allow my virus software to download automatically.

Those kinds of things, that kind of technology exists. We've got to make it easier for folks to protect themselves without having to become technical experts.

MS. CLAY: Thanks, Frank. Next we have Vince Sollitto. Vince is vice president of corporate communications and external affairs at PayPal. There he oversees public, investor and government relations.

MR. SOLLITTO: Good afternoon. I think I must be sitting in the assigned industry seat which is why Simson must have removed my microphone for this segment. Hopefully you can all hear me. Much better.

Great.

I'm here probably as a quick example of a company that can provide some context about what we have to do for security because of the vulnerabilities that we as a small business online face and also a quick possible solution for some very small businesses that have begun to take advantage of the security we provide.

Just before I get any further, I would like to ask a quick question. How many folks have actually bought something online in this room? How many folks are familiar with eBay in here and PayPal, anyone familiar? And how many had the delicious barbecue beef sandwich and will be asleep in about three more minutes?

Real quick, PayPal is an online payment service that allows people to send money in a sense by email to anyone else with an Internet connection and an email address. Part of what we do is we allow the consumer to give us their financial information and data and not to the recipient, particularly if it's someone they don't know. That's part of the appeal of the system to a consumer.

As such PayPal is a repository of financial

information and private information for consumers and for the small businesses that get paid through our system. So PayPal is a relatively new service launched about two and a half years ago. We currently have over 16 million members using the system. It's kind of shocking for someone who just joined the company when there was only about 30,000 customers, but about $3 and a half billion was sent through the network last year.

Currently about 300,000 transactions are done every single day. About $17 million goes through the network each day. People conducting transactions with other people they don't know instantly and securely and part of that reason is our security. So as Willy Sutton said, why did he rob banks, because that's where the money is.

That's one of the reasons why we have to be ultra secure because we are where people go to place their information so they don't have to share with others, and in fact we have 16 million accounts with credit card data, bank account information and a whole host of other financial data.

Are we at risk? We are certainly a target. As Frank said Microsoft may not be any less secure than anyone else. They're just a very attractive target

because they're huge. We're very large, we have a lot of information out there, so we take security very seriously.

Fortunately one of our founders is a cryptography expert and actually built the entire system in-house so we don't rely on any outside stuff, and a large part of that is many of our solutions are customized and they work for us.

What are some of the important things that we do? Well, all our transactions occur on secure servers using SSL and that's something folks, consumers can look for when they shop on line, is this site I'm on actually a secure site, does it say HTTPS, or just HTTP, and a lot of e-commerce sites don't necessarily take advantage of that, figuring their consumers may not have the ability to access those sites with the best technology or they just don't want to go that route.

All the information that comes to our site is entered via SSL, HTTPS, URL, and then what happens to the information after we have it? It sits in our secure servers which are surrounded by firewalls and we use 128 bit encryption which is military grade. As a matter of fact our CTO is from Russia so in America it takes two keys to launch a nuclear missile, but in Russia it

takes three people or at least three keys to do that or actually it did until they began to become a little more flexible.

As a result, whenever we have to restart our database, we have to get three people out of eight together in a room, and they all have to enter in a 128 character password which they all have committed to memory so it's obviously a pretty secure system.

One other thing we do is we don't connect our servers to the Internet directly. All the information is stored offline in a sense and housed in a number of facilities in California underground, with biometrics by the way, so what does this mean? We still get probed constantly. We get about 500 attacks a day.

Now, some of them we pay for. We try and get professionals to try to break in constantly but many others we don't. They're from all over the world Russia, Indonesia and beyond.

So security is obviously critical to us. We're very fortunate that we've got some great people doing some great things with it.

One of the interesting things about being in our business is we often learn of hacks of other sites before perhaps the victims do themselves because PayPal

is a place where people who may have gone and stolen credit card data from other less secure web sites might come in an attempt to use those stolen credit cards and monetize them in a sense, go open up an account with somebody else's credit card, try and send money to someone you know or perhaps even yourself and withdraw it.

And in fact we frequently work with the authorities on identifying large bin numbers of credit cards that might have been hacked or compromised, so in a nutshell what that says basically is PayPal is a huge target because we're a huge database. We take inordinate steps to provide security for that information.

Small businesses are faced with this same task and yet we're specialists. They're probably not. They're generalists. For a small business the most important thing they focus on is your business, how to convince you to pay them, not how to convince themselves that the security they have for their web site is the best it can possibly be.

A lot of people on this panel are going to explain ways and steps business can take to protect their web site and consumers can take to protect their

information on their web site.

I offer out there as one example of a solution that both consumers and small businesses have come to is that in a sense why not out source that concern to a specialist, and in fact that's what our 16 million members do.

Consumers use our system as almost a secure online wallet where they just give only one web site their financial information, credit card, bank account and such, ours, and then transact through us so as to be more secure because they don't have to worry about whether or not Frank's web site, although I'm sure it is, secure so to speak.

Same thing with small businesses. They're not really interested in using that information. They don't want it. They don't want the risk or the liability. They just want your money, and so by using our service they don't have to worry about whether or not they've held that information secure.

Obviously there are many steps they can do to do so. I'm sure we'll hear more about them. I'm just trying to explain the steps we have to take to secure that data. I know how difficult that is and also to indicate there are other options out there if folks

don't feel frankly up to the task.

MS. CLAY: Thanks, Vince.

Next we have Vic Winkler. Vic is the principal architect for security at Sun Micro Systems public sector. There he's been responsible for enabling customer security architecture decisions, authoring security white papers and writing the security policy for the government of Malaysia.

MR. WINKLER: A disreputable place sometimes, Malaysia, that is.

I'm not sure what I should say to you except for run for the doors. I think security has collided with marketing, really good marketing in the recent past and for a number of years. It's on the one hand extraordinarily difficult to achieve a comfortable level of security. On the other hand it can be relatively easy to achieve appropriate security.

And there were a number of examples today using cars and other objects that can kill bugs, but I think that it is a great challenge to both the consumer and to a small business, even to a medium or a large sized business to impose functioning solutions, manage them day-to-day and have a degree of trust that they'll do what you think they'll do when those solutions are

comprised out of components that are unbelievably complex, and that are designed really not to inter operate very well together.

In fact sometimes the individual components are designed not to inter operate with other vendor's technologies so at the point where we are today, and by the way, where we are today is a snapshot in time, and we really shouldn't feel too good or too bad about where we are at a particular point in time, right?

So if we look back at an archeological record we'll find mainframes which were the scenes of much control and tyranny if you had an application you wanted to run on them, and then enterprises managed to wrestle away certain modest amount of funds from their financial officers and bought mini computers where they could then run applications without the constant attention to detail that one had in the main frame world, and then all hell broke loose.

PCs appeared. This was the cause of much chaos and much confusion trying to move from one PC to another to just do your damn work, right? Then after that the network slowly caught up with PCs, and we found we could move things around, and since then it's been a blur.

I'm not sure where we are today, except that

things seem to be moving up into the network and away from all of these little computers that we have sitting at our desks. These are just -- they seem to be, and these little devices that can communicate with the network seem to be just little port holes into the network for information and applications.

That kind of a world seems to me to be far easier to manage from the standpoint of controlling enterprises and what individuals can do than does the world where applications and data all reside on individual platforms. Where all the data and all the applications really have to reside on individual producer platforms, that's untenable. That can't be managed.

The amount of code that can't be proven for correctness and authenticity, that you can't perform that on each of those platforms. We're not at that point. Theoretically it's very far off, so the model where we have centralized control over applications and data but where users can have exactly the same rich computing experience that they have today but without all the hassles, and you might not want to ask yourself where you want to go today but rather what you want to do today.

And if what you want to do today involves fixing bugs, patching, fighting viruses, fighting hostile things over the Internet, I don't want to play that game. I want to play the game where the computer resources I use are tools that allow me to do my work, and that's the same for a consumer as it is for a business.

It's sheer lunacy to expand the tens of millions of dollars that the Veterans Administration said they spent last year fighting two viruses. That's a phenomenal amount of human effort, amount of resources in the economy that are being poured in one direction. It's a tremendous waste of human effort, and computers really have the potential just like television once upon a time did of enriching our lives.

And we're at the same point today I think where television was a number of years ago when Madison Avenue got a hold of it. It became something that was marketed to the point where your television viewing experience without Tivo is a terrible thing, and that's the convergence of computing and TV.

Now I want to see the convergence of reasonable behavior and reasonable architectural choices with computing, and I think that's all I want to say right

now.

MS. CLAY: Thank you, Vic.

Last but not least on the panel we have Marc Zwillinger. Marc is a partner in the Washington office of Kirkland & Ellis, a cyber law and information security practice group, and he's a member of the firm's technology committee.

MR. ZWILLINGER: Thank you. The panel is book ended by lawyers. I guess I have to start with the reverse disclaimer, which is that I am a lawyer, and I know nothing about anthropology.

As a lawyer, what I do is I help my clients handle computer incidents, that is I help them prevent and minimize and recover losses for when a computer incident occurs, and I deal with relatively sophisticated clients.

And where I find that they have the most problems in preventing computer losses or recovery losses is in incident response, that is in handling an incident after it's occurred and recognizing it and responding to it.

And the panel that we're talking about is entitled "what steps can businesses that maintain consumer information take to improve their own

security?" So talking about incident responses doesn't seem to make that much sense because already there's been a problem, but we know there's going to be a problem because no preventative measures are 100 percent effective, and if we look at the Security Institute and FBI study this past May, last year 80 to 90 percent of the companies that responded reported some kind of security breach.

So my perspective on that is that a proper response can help reduce losses both for the business and for the consumer, that is for the business, the response to an incident may be more significant than the incident itself.

That is you take the CD Universe case for an example. Credit card data was lost and had the company wanted to make good on all the credit card transactions that occurred as a result of the stolen data, they could have done that without even affecting available cash, but because the incident was so well publicized, because they didn't handle it as well as they could have, because the marketplace stigma that got attached to it led to the demise of the company, the handling of the incident resulted in the demise, not the actual penetration.

From a consumer point of view it's the same thing, that is if a company recognizes signs of attack right away and responds appropriately, what could have been a simple penetration or trespass defense can be stopped there. If there's no proper response it can result in full theft of credit card data, trade secret loss for the company, consumers with out of pocket losses and a near catastrophe.

So since the ticket to this debate seems to be being able to make automotive analogies, I have to say what I'm talking about is like Lojack, that is your car is taken, and you limit your losses and you get your car back by being able to handle the incident, call the police, track the car and get it back to you, assuming some percentage of automobiles losses are going to happen, your car is going to get stolen no matter what security you put in place.

When we talk about incident reports, I want to focus on the two aspects of it, which is recognition and reaction, and I think it was Laura Berger in moderating the last panel that asked the panelists to talk about the problems of recognition from a consumer point of view, and there are problems in recognition from a business point of view as well. That is, it's difficult

to separate the incident from the background noise.

You have to have a lot of experience with a system like PayPal to know that it's normal to get 500 attacks a day and what those attacks look like and what bandwidth they consume, so when you're seeing one day 1,500 attacks that all seem to be coming back to a country where you're not used to seeing that amount of traffic, that something is going on and to react appropriately right then.

The problem is we have a difficult culture even in businesses with users recognizing these problems, that is we've lived in a situation, and I'll bash Microsoft for a moment, where we blame our problems on a computer system with Microsoft's operating system so we say, Well the computer crashed but that's Microsoft. It doesn't occur to you, your first instinct, that the reason your computer crashed is you just suffered a denial of service attack. You just try to reboot and only after a couple days of a problem that the staff can't fix, then you start to think about other causes.

The network is slow today. Sometimes that happens. The network is slow. Also the network can be slow because your bandwidth is being consumed by people that are taking over your computer systems and are using

it to launch denial of service attacks.

So getting businesses to train their own employees when an attack is taking place is often difficult and requires planning and thought.

The most famous example is Cliff Stohle for the people that read the Cuckoo's Egg. He noticed this infiltration into the computer systems there by noticing a 75 cent discrepancy in the accounting system, realized somebody had created an account. On one computer that wasn't on another which resulted in a 75 cent discrepancy, and when he found out why that account had been created it was a hacker who had broken in and got administrative privileges, and the whole investigation started from that simple discrepancy.

That's what we need in our corporate environment. That's what we need for businesses to protect themselves and to protect the consumers.

And again the analogy doesn't always work and here it breaks down because when your car is stolen, you tend to know it. You walk out of the mall and you utter those words that have been made into a movie this year, Dude, where's my car, right, but you don't do that in a computer environment.

You don't know that your system has been penetrated and you don't what's been taken which is why

the next phase I want to talk about briefly, reaction, is so important.

That is without a plan in place, a plan that requires the assembling of a multi disciplinary response team, you're never going to be able to respond to an incident quickly. You don't want to be making introductions, and I'm not going to beat up on PayPal, but I'll use them as an example.

Vince doesn't want to meet all the people both inside and outside who are going to be needed to respond to an incident after the incident occurs. He wants to have worked with them and planned with them and set out a strategy and protocol well before he experiences a system penetration.

You hire a law firm to respond, you can't even clear conflicts in the first 24 hours much less get a retainer on file, right? So you want to be putting your teams together in advance.

The other aspect of the team is involving outsiders. Nobody wants to spend a lot of money responding to incidents, and your plan or protocol will tell you when you need to kick it into high gear.

If we go back to the Computer Security Institute and FBI study last year 150 million dollars of losses

were caused to 200 companies from insider theft or insider abuse. So when you detect your incident, is your first call going to be to the insiders who are going to investigate and tell you what happened, or are they going to be to an outside consultant who's going to come in and do an analysis.

These are all questions you want to think about. What types of incidents do you want to respond to in one way, what types do you want to respond to in another way because only by getting that done before an incident occurs will you be able to respond effectively and cut your losses.

The only other thing I want to mention at the beginning is the problem of attribution. That is, companies tend to respond to a computer incident of any type with a make it stop approach, that is I don't know where it's coming from but let's just make it stop, and making it stop often amounts to closing your eyes. That is you want to know before you make a decision on responding to an incident whether this is a competitor or a malicious hacker, whether this is a teenager, and even the government has trouble with attribution.

I've been involved in a couple of cases, excuse me -- I'm trying to give the stenographer a run for her

money. I've been involved with a couple cases in the government where in the first 24 hours after an attack, there was a conclusion reached, tentative conclusion reached that this was an organized attack, this was a nation state trying to break in to the computer systems, when several days later this same attack was properly attributed to teenagers in California.

I've been on the other side as well, that is an entity didn't respond quickly and said it's just kids when it was in fact organized criminal activity, and if you don't think about how you're going to solve your attribution problem, you're going to end up in a situation where you have losses and you have to explain those losses to somebody, to your customers, to your vendors, to Congress, as to why you didn't respond quickly because you thought it was just kids and it wasn't that important.

You need an attribution strategy as part of your incident response plan, and all of that together gives you a way, whether you're a small business or a large business, to minimize your losses. If it's two people in the company, your plan could be when do you call the other person, when do you call your outside provider, your ISP to say, Help us, but you need to have thought

about that in advance as a way to minimize losses.

MS. CLAY: Thank you, Marc.

Marty, you look like you're itching to say something before we go on with the questioning.

MR. ABRAMS: I am. I've spent many years trying to arbitrate disputes between marketing departments and security departments in organizations, and one of the things I mentioned before that security can't get in the way of immediacy, and in the world in which we live, often there is a disconnect between the concepts of security as we have we mapped them out and the concepts of reacting to a marketplace where people buy because of quality, price, quickness, all of those attributes.

And part of that conversation, part of this whole question of reinventing the way we think about talking about security and where we place security I think was mentioned by the gentleman from Sun Micro Systems, that we need to find ways so that it's not about stopping the process. It's not about slowing down commerce.

It's about building the infrastructure that allows us to have security work without people having to work AT security.

MR. WINKLER: Yes, and I would like to follow up

and say that our architectures, the Internet, large businesses, these architectures have grown organically without very much planning in advance. They've been kind of added on to and so forth, and what we need to do is step back and rethink what these architectures are really supposed to do for us, not how we can best serve them by buying more products that fit in here and there to try to better protect things that are inherently defective or ways of doing things that are inherently defective or counterproductive.

MS. CLAY: Your introductory statements have been a great lead in to this afternoon's discussion. One of our goals is to close out this session with a clear understanding of the real issues that businesses are facing and some ideas or even examples of how they can address those issues, and a lot of that or at least some of that has come out already.

So with the first question, let's say that we've been asked to start a list of processes that businesses should implement to secure consumer information. As a base line, what would you put on that list? What would you include?

MS. GOODENDORF: I'll start out that one of the processes that is so critical for businesses, very

basic, is a risk assessment, and every business, every industry is going to be a little bit different, and when you do a good job on risk assessment, then you really know where to focus your security energy and where you should spend your money and what you should spend it on.

That's just one process but I will start with that.

MR. REEDER: In the interest of provoking a little bit of controversy, let me disagree, and it's a partial disagreement because certainly risk assessment is not -- is an important tool of security management, but I would start in a very different place, and that is there is a set of base line practices that irrespective of the risk that one is assuming, obviously if you're a bank you're in a slightly different place than if you're a public library, but everybody needs to worry about availability.

And so there is a set of things that every organization needs to do. I'll diverge from cars to medicine. We all know that we ought to wash our hands, that medical practitioners probably ought to wash their hands between patients. It doesn't guarantee that infection won't be transmitted, but there's a level of

risk that none of us need to assume even assuming that nobody that we're dealing with that day happens to be infected because we simply don't know.

So I would start in a slightly different place, and we could all construct our own list. We all need to do things like back up. We all need to do things like making sure that our software is up to date. I would argue that you ought to look for the Center of Internet Security benchmarks which are designed as minimums.

What I fear and I don't think -- and I'm putting words in to Lynn's mouth that I don't think are necessarily hers. What I fear is if we walk out saying you ought to do a risk assessment, everybody feels comfortable, now, I can wait six moments until the consultant's report comes back and I have an idea what my risk is.

There's a shared risk that we all have by virtue of living on the Internet and a set of things we ought to be doing while we get the consultant in that says to us -- and beyond that because you are who you are and because your business is so heavily dependent on availability, there is a set of things you need to do.

MS. GOODENDORF: I don't disagree, but I would say that a lot of companies have comforted themselves by

spending a lot of money on security, but if they spent it -- particularly buying a lot of tools and doing this and that, and they're thinking that they're doing a great job, and some companies will benchmark themselves on how much money they're spending on security, but they're not necessarily spending it on the right things.

And I think that's the whole point of really just thinking through where your risks are and where your vulnerabilities are.

MR. WINKLER: I think the problem with risk assessments is that it doesn't much matter whose assessment you read. It probably will apply to your environment, and that the risk assessment industry is -- while there are some very capable practitioners, it's going to make a lot of money doing very little except changing words with some boilerplate.

So I think the point about best practices is probably the one I would lean more towards, if I can change what you said and call it best practices, a base line of accepted ways of doing things. And I think that we would all do better with more attention to that.

MR. ABRAMS: Again part of where I'm getting uncomfortable in the discussion is we're separating what we're trying to do as an organization from the whole

question of how we're safe as an organization, and in the area of helping organizations think through their information policy, we say you should catalog your risks along -- in four bundles, okay?

And the first bundle is compliance risk, and let's put that aside. The second is reputational risks. What are the things that if they go wrong will put you in a position of losing your brand, your ability to work with the outside world?

The third is investment risk, and that goes to the whole question of if you have a problem, how will that affect the payoff on your business going forward, and the last is reticence risk. What are the things that if you're reluctant to make decisions will make it difficult for you to do business with the folks that you need to do business of going forward?

In my interaction with the whole question of security, typically we never get to this question of reticence risk, and what happens in organizations that if the security tool is too hard to use or gets in the way of that interface with the consumer, if the consumer has to wait too long when they come to the Inter Continental site to do whatever it is they want to do, then what happens is that the security stuff gets

turned off, and then you actually end up with more risk, which is sort of why we need to think about the whole question of security as integrated into the business process and not something that is left to, quote, the specialists in information security.

MS. GOODENDORF: I think someone on the previous panel made a comment I strongly agreed with. He said the best security -- I don't remember his exact words but it really enables the business. It doesn't hinder it. It enables it, but I would just mention other base line processes that I think should be mentioned is prevention, which includes patch management.

And I was talking with someone a few weeks ago about the importance of patch updates which is a preventative measure and he said, Oh, that sounds kind of going like to the dentist. It's not glamorous. It's not jazzy. People in the technology industry aren't particularly attracted to that.

It's like maintenance, and yet most of the vulnerabilities, a lot of the security breaches that are happening are exploiting just known vulnerabilities that can be prevented with patch updates.

Detection I think is another base line process that is significant, and intrusion detection has come a

long way in its capabilities, particularly in the past year, and there's both network intrusion detection and host intrusion detection, both of which address -- I can't remember who mentioned it, but companies not even realizing that something has happened.

Those are probably the most insidious security breaches are the ones that you don't even know that are going on, and I think that's really the value of detection of recognizing when something's abnormal and attacking it and then also I agree about response plans too, I consider that another category of base line processes.

MR. ZWILLINGER: If I might, and my comments are always going to be in this vein of sort of thinking about security from both the technological and the policy or legal point of view. I think it's very important to recognize that when you deploy technology of any sort, you need to do it with policies, that is, three basic policies are external facing policies, your terms of service, your internal facing policy, what's an acceptable use of this technology on your networks, and your incident response policy, what are the base line policy processes and do they support your technology.

That is again to my point, you can put into

place whatever system you want. An insider can exploit it, but if you have an ability to monitor that insider's traffic, when they start to exploit it, you can detect it and stop it even though your IDS system doesn't necessarily go off or stop it itself so those are the three base line policies I would introduce into the process.

MS. CLAY: Would anyone like to make a comment on training before we move on to the next question, training with respect to a process that should be implemented for business security? Anyone? Anyone. I'll make a comment. This is one of the fun things about having the mike.

I think that this is one of the things that was mentioned earlier today is that we can have a lot of technology out there, a lot of processes in place, but if the people who are responsible for getting the job, the ultimate job which is making new sales, if they don't understand what they're using and why they're using it, then you can still have a huge security problem because there's always a way to work around that little thing that the security officer wants you to do, so just another thing to keep in mind.

The other thing I would like to mention is that

some of the topics that have come up just in this first question about risk analysis, risk management, contingency planning, security policies, you will have access to resources on how to start with some of those things.

That's one of the things that we'll provide to Mark to put on the FTC web site.

MR. REEDER: Alicia, if I may, I think it's important to distinguish between organizations of sufficient size that they can, for lack of a better term, attempt to create a security aware environment where security awareness training is built into the normal mechanisms.

But ultimately I'm not saying about our ability to take the small business person or our proverbial aging aunt or uncle who's gotten that $600 PC and is now email enabled and talk a lot about training.

I think we really have to think more about what I would call passive security, that is, doing things that -- and here the metaphor actually works. We build cars that are safe. We teach people, we try to teach people how to drive them safely, and we still expect them to run into other objects and so we do things so that when that occurs they don't hurt themselves as

badly as they otherwise might.

And we increasingly try to do that with side and front airbags or rather than even having them -- although we know we should use seat belts as well, relying on their willingness to always do that, and I think we have to think that while training is terribly important and certainly in enterprises of any size it's feasible, I think there's a limit of how much awareness and training can accomplish, and given the power we're putting in to the hands of folks who aren't going to worry about that.

MS. CLAY: Very good point, Frank, and I think that the closer we get to that point about passive protection, the better off and the more enabled we'll be. Very good point.

Are there any standard software or hardware elements that should be included in a good security program? If so, what are they?

MR. SOLLITTO: Well, at the risk of redirecting the question or sort of almost rebutting in a sense, I think one thing you folks should keep in mind is that, maybe this is the same conflict about whether you do a risk assessment or whether in fact there are basic standards that all folks should do, that at least in our

experience we found that what we do for security is what's right for us.

And I'm not sure that there is a general basic standard that is the best for each company, each customer, or just general use because as was talked about before down here, if somebody goes to this hotel site and can't log in because we've made it so secure that it's virtually unusable, then that company is going to be out of business.

And part of the reason our company has been so successful in our view is because we've struck a balance between convenience and security that works for us and our customers. For us it's a really high hurdle because we have to be really secure and still very convenient, and I think it's just important that folks realize that security is inseparable from the way a business operates and the business goals at hand, and that what works for some folks might not work for others, and that we've basically been forced to advise what works for us of separating unique situations.

For instance, I'll take one example. All the transactions that occur on our web site occur via SSL technology, secure socket. EBay does not do that. They have decided that the transactions that occur on their

site require less security than perhaps we might because of the financial nature of ours versus the pure commercial nature of theirs, that combined with the broader user base they may have or the inability of all of their customers' technology systems to interact ideally in that environment and therefore have chosen to go another way.

So I think while I would recommend SSL for all types of security, there are very many companies out there who decide that it's not going to be the best thing for them, so I'm sure there's some great answers here on this panel of what might would be the basic standards of security most companies would strive for.

I would throw out as a caveat in the beginning that many companies might find that what's best for them is best for their unique situation. I know we certainly have.

MS. CLAY: Vic Winkler?

MR. WINKLER: There are a number of things that I just heard mentioned that I might have comments on. The SSL issue is one where SSL was originally designed more to create -- allow for the creation of an encrypted link between a client and a server, but the real emphasis was on allowing the consumer at the client end

to trust the server, and this is a little bit different in an example like eBay where the trust issue is one of individuals doing business via third party eBay, and I'm not a big fan of eBay but I think there's a difference there.

I think the best in terms of standards today really is the common criteria which NIST I think has ownership over within the U.S. in conjunction with NIAT. The common criteria are a set of standards for looking at both the assurance and functionality of security within products, be they operating systems, firewalls, whatever.

And it is really up to the business community, the health care community, the consumer community to define what are called protection profiles, which operate against them.

So what really hasn't happened is that we haven't taken advantage of what the common criteria offers in terms of allowing us to define and then value pick products that are in compliance with what would be commonly accepted behaviors or functionalities for a particular domain such as a retail outlet with a web facing the front end.

So I think the common criteria really ought to

be given more emphasis. There is a lot that has been done in security, and we've really raked most of the hard questions over a lot of coals for many years and have seen that they have not been adopted for usually the wrong reasons, not because security is too encumbering.

MR. ABRAMS: In some ways we're talking about the apples of security and the oranges of security. There's certain issues --

MR. WINKLER: Can we refer to the apples and the suns of security and so forth?

MR. ABRAMS: How about the kumquats and the apricots? That gets us out of brands.

In terms of the apricots of security, that's some of the issues that have arisen because of the network world, and I have a great deal of confidence that we can come up with the solutions to those, and build in things like the firewalls that we talked about earlier today.

I'm not at all concerned that our ability to come up with technological answers that respond to those issues and our ability to come up with standards will indeed come to the forefront, that there's a will to solve the problem and then it will be solved.

I'm more concerned with some of the standard business facing -- consumer business facing security issues that are a lot harder to do with technology. The simple concept of if I don't know you today and I didn't know you yesterday, how do I know that you are who you say you are, and the whole question of how we do authentication authorization in our marketplace where we have lots of other countervailing issues, issues of privacy, issues of people's memories, issues of we don't have -- if we're not going to accept a chip embedded behind our ears, which I think none of us are willing to do, how are we going to build those solutions because it's not just technology based?

I think those are the more difficult solutions and the more difficult questions for that small business that truly is trying to safeguard the consumer, the real consumer, not the fake consumer, and the business from a continuous string of fraudulent transactions.

So I think in terms of talking about the business solutions we need, I think we have to separate the kumquats from the apricots and let's say, Yeah, we have one approach to the kumquats which is securing the network and securing the interaction with the network.

But I still think we have a huge challenge in

terms of the second set of issues, which are that we are really moving to an economy where the consumer spends more time serving themselves by interacting with the company directly and not interacting with an individual that says, Hmm, this patient just seems suspicious, and I think before moving forward we separate those two sides.

MS. GOODENDORF: I think there have been some common themes in the discussions today that I don't know if they're recognized as hardware and software standards, but it seems generally recognized that passwords have become a standard. Anti-virus has become somewhat of a standard and I think firewalls, and almost everything I see both in the consumer world and the business world, those are three very common themes.

MS. CLAY: Okay.

MR. ABRAMS: That's a great example. Let's look at passwords, and I'm 52 years old. I fully admit to being 52 years old. Probably the most used button when I go to a web site after I haven't been there for three weeks is have you forgotten your password, and then they ask me such a great question as, What was the first car that you owned.

Well, was that the first car that I really want

to forget when I was in college or the first car that parents gave me when I graduated from college or the first car I actually paid for? It's a question that for the life of me even if I think about it honestly and rack my brain I just can't answer.

Those are the types of things that we -- that we're getting to because things like passwords just aren't working very well today as people like myself get older and can't remember the 16,000 passwords that we're confronted with.

MS. CLAY: Marty, it feels like you want to make another statement around what might be an alternative maybe, software, hardware elements for a security program for authentication specifically?

MR. ABRAMS: Well, I think there were some suggestions today. I don't have a great answer, and I'm not a technologist, but I think that we have to move towards tools that we can possess, that we can use, that we need to build the utility into our machines.

I think the suggestion this morning from Dick Clarke at the Department of Defense, they've solved the problem of people not being able to remember their password by using a token. I think that we need to be thinking about those sorts of tools for the interaction

between consumers and smaller businesses.

MR. WINKLER: Actually with the Common Access Card, the user still needs to know the pin to unlock the card on which is embedded a very long private key and other information.

MR. ABRAMS: But does it liberate the idea of remembering 16 pins or 17 or however many.

MR. WINKLER: Yes. In fact, and that depends entirely on -- this is a technological sidelight. There are different smart card formats, and certain ones allow you to lay down different kinds of information and change it under control by the user, and this control issue is one that really touches as both the consumer as well as the business because businesses are -- businesses and their relationship of the Internet have changed dramatically and are continuing to change with the concepts of network identity now and how that can be exploited by businesses to allow for a richer, perhaps even better consumer experience as they relate with their digital world different affinity partners, airline, bank, et cetera, and being presented with one perspective without having to sign on to multiple accounts, this will add additional responsibilities, raise the bar for the security at each of the partners

that engage in this affinity program where this information is not necessarily shared but aggregated as it's presented to the user.

So it's becoming even more complex which I think begs the question, how does one simplify the overall difficulties that are inherent in architectures and computing platforms, and it really comes down to where information and applications need to live.

And that's the fundamental question that's the same for consumers at home as well as small businesses, large businesses as well as partners, so the question is: Where does what live and how does it get updated are very, very essential questions?

MR. REEDER: I would add here, I'm not also in Vince's employ, but Vince made an important point, and that is especially for the small business and for the individual, you have to make a judgment as to how much of this you can afford to do for yourself and how much of it you're going to simply have to rely on others to provide to you, whether it's going to PayPal for payments because you're not prepared to develop the infrastructure to provide that protection for yourself, or looking to your ISP.

And here again my friends at AOL, they can be my

poster child, but there are others because putting yourself in their hands gives you a certain level of assurance that you don't have if you're simply going to go it alone on the Internet.

There are obvious trade-offs. There are obvious costs in doing that, but part of what we need to do -- and here we need the education of a different sort. I mean, again metaphors sometimes distort. A few of us, myself not included, occasionally lift the head of -- lift the hood of our cars and look to see what's in there.

I've actually owned a car for two years and to the best of my knowledge I don't think -- I couldn't tell you where the hood latch is. It's not that I'm not interested in this as a matter of theory, but I know I'm completely incompetent to deal with it, and I'm prepared to pay a certain price to somebody who periodically maintains it for me including doing all the appropriate safety checks.

But I understand that that needs to be done and that I have to make an explicit choice as to whether I assume that responsibility for myself or pay somebody and in this case proactively actually take my vehicle, while it turns out with this vehicle it tells me when I need to go visit its other home.

That is part of what we're talking about, so again we need to be very careful when we talk even about defining what are the minimum set of things you need to do to be a little more precise about the home we're talking about, whether we're talking about Sun or Microsoft or eBay or PenPal -- PayPal rather as users of technology, not just deliverers of services but as users of technology or again the small sole proprietorship or partnership or our aging aunt on using email.

MR. WINKLER: I think that those are very, very good comments, and a business has to ask itself what its core competency is and what it should grow to be, and if its core competency evolves into fixing bugs, updating software and so forth, it's ridiculous. You're always spending your time doing the wrong thing, so that would become the point where you either go to out source or have professional services manage your computer infrastructure or go to a different scheme, and there are different schemes.

MS. CLAY: Speaking of, one of the things that you mentioned just a few seconds ago, was keeping systems up to date, and we've also throughout the day we've talked a lot about patching. How are businesses actually accomplishing that now? Do you think that it's

being done regularly, daily?

MR. WINKLER: As a vendor we have seen many of our customers with exactly the same problems. They will come to a point where they have looked at patches, and there are different approaches towards patching. You can either -- a vendor can choose to release a patch that's unproven almost immediately, or a vendor can be somewhat more circumspect and release a work around immediately and release a patch that that vendor believes will not break other things running on that system, and so that's the vendor aspect of it.

Then there's the business aspect where you need to know if you -- you need to decide if you're going to trust a particular patch and whether it will run in fact with your legacy software that you inherited from your great grandmother back in 1802, right?

There are a lot of customers who have software that's antique and so you need to decide, and then the question is how do you -- and this is where our customers have a major problem. How do you know that your systems after you patch them are still patched because customers will reinstall software and then miss the appropriate patches?

So the U.S. Army, for instance, a number of

years ago discovered that even though they had very strong requirements for maintaining a patch program for each and every one of their systems, they found that systems kept getting reinstalled, and the patches failed to be applied to them.

So this is something that is extremely challenging for a vendor from a public relations standpoint because you have vulnerabilities in user land that you may have put patches out for years ago that are no longer being carried forward so it's extremely difficult.

There is a strategy, and that is to only install software from computers on your network that you control, not to control -- not to install software from external networks or from vendors' networks without putting it on your systems first, making appropriate images and then loading those images on to appropriate platforms in your enterprise.

This is something that's extremely cost effective for a business or a large enterprise to do because it allows you to do it once, define what that image ought to be for a specific machine or set of clients, and then if anything requires downloading again, you simply go to this well known place. You know

what to download. It happens, it's proven. You don't have to go and change and make sure you don't make mistakes when you select different things, and it's proven to be effective and a number of vendors do this sort of thing.

MR. ZWILLINGER: Combining the last two responses, the question was what do people do now for patches, and before that we were talking about out sourcing. A lot of my clients rely on managed security services that do continually scanning of their networks, and they notify them every time a computer goes up or down.

The scanning runs pretty much continuously, and they have access to log into a web site to get an instant glance what the network looks like right now, what systems are online, and they can drill down to any system, figure out what version and what software is running by virtue of the managed security services running and really keep tabs on their network.

And while that requires some sort of investment, it's not an expensive way to go about it. It's not something for a small mom and pop operation. At the same time it really shifts all the burden and all of the technological know how to an inventor, and at the same

time putting out that information right at your fingertips so you can look in at a secure portal, and that's how my clients rely on and make sure their patches are just changed, in charge of reviewing those reports to see what version, which system patch -- it doesn't do every piece of software but it does the ones they're most concerned about.

MS. CLAY: I think Lynn and Frank.

MS. GOODENDORF: I would say that I'm in user land, that what has worked well for us is rather than the information security grid being responsible for patches, we actually have the various operational teams who look after and operate these systems responsible for that. We hold them accountable.

We do have third parties run vulnerability testing as well, but as far as who actually is tasked with doing those patches, it has worked well for us to have that reside in operational teams because they are the most thoroughly familiar with the system. They want it to be up and performing well. It fits well with their other duties so that has worked for us.

MR. REEDER: Again, looking back on things that both Vic and Marc said, the Center for Internet Security that I described earlier puts out security benchmarks, one

aspect of course is patch management, and most important puts out software tools that are non intrusive, that measure where the systems are against these benchmarks. These again are available without cost on the web site, so that the user can continuously measure not only whether the system settings are as they were originally set but whether they continue to be.

But I say that with the important caveat that that doesn't help the individual consumer or the small enterprise for whom that would be beyond their technical skills. It certainly works.

MR. ZWILLINGER: Although it does help the individual consumer, again in the context of letting them know who they're doing business with, to the extent you're a consumer and you're getting your financial information to a site, the sites that are running management security services or using the software you've talked about, sometimes you can see that in the organization.

They have announced that. They have a seal. They have some sort of way to tell consumers this is what we're running.

MR. REEDER: And my not so secret agenda for what I hope comes out of the series of conversations

that the Commission has begun is if you will have better information in the marketplace for consumers about the level of security that they're buying when they engage in a relationship with a supplier.

It seems to me ultimately the difficulty is not that smart people don't already know what to do, but that an awful lot of people use technology that they shouldn't have to worry about it, who shouldn't have to think exclusively about it, but then don't understand as they do with automobiles or airplanes or selecting a medical care provider whether this individual is licensed, whether they really had been inspected regularly by some accrediting body where the other cues that we understand to look for when we purchase other services that are both critical to our existence and have the potential to harm us if they're not provided safely.

MS. CLAY: I would like to ask another question or two and then open up to questions from the audience, so if you have any that you're ready to ask.

We've talked a bit about insider threats, and I know that the CSI FBI survey that recently came out, at least the people that they surveyed say that 30 percent of the threats are still coming from insiders. Is there

something that businesses can do to minimize or try to better control that, the insider threat?

MR. WINKLER: Well, looking back about 15 years, there was a great deal of discussion in the security research and developing community about this kind of question, and at that point in time research and development in computer network security was essentially funded either directly or indirectly through the DOD and the intelligence community.

And when the question was posed to the business community, it became evident that in fact the business community had done something about this. It was called the well formed transaction, and it simply amounted to that no individual user of a system -- and if this was a paper process and a paper process, no single individual could both order, pay or approve and pay for a fictitious item in order to gain off of that.

And the same really holds true for automated systems, so, yes, it is possible to, first of all, limit the damage that's potential and then the second thing is of course intrusion detection, fraud detection and other prone to error automated processes, and I can say that legitimately because I was one of the first developers of such an automated system. The number of false

positives and false negatives are really, really difficult to manage.

But it doesn't mean that this is something that fraud detection or intrusion technician are technologies that should not be used but they should not be viewed as the line of -- the only line of defense, so I think that number 1 again it's an issue, how do you characterize applications so that users of a minimum amount of knowledge can use it, and two, how do you rectify that with intrusion and fraud detection.

MS. CLAY: Frank, did you have a comment before we go on?

MR. ZWILLINGER: Can I jump in on that? I spend the majority of my time responding to insider incidents. That's usually what I get called in to do, and when I respond to them, I usually find three things can go wrong in preventing the company from figuring out what happened and prevent it from continuing loss.

One is they haven't turned their auditing on. That is they didn't have enough storage space and storage wasn't as cheap when they decided to put their policies in place, so they weren't monitoring everything that happened on their networks from an auditing point of view or they weren't monitoring everything from a

legal point of view, that is, they didn't have policies in place that said any time you do anything on the network we're going to monitor and record it and if we want to we can disclose it.

Sometimes it's a conscious choice. They don't want to create an environment where everyone is being monitored. More often it's not. The company wants to have that, but they just never put it in place.

And there are tools out now that are just wonderful at doing forensics like over the network. For example Guidance Software and Cases just launched an enterprise version where you can have an output on anyone's computer system, and if you think there's some kind of insider threat you run the output and image the system immediately, and that's part of the growing movement toward preventive forensics.

That is before you give someone a computer -- when a computer is turned on you image it before you recycle and image it before you send it out so you know what that employee did. You take an image every time you're about to lay people off so you know what their system looked like so they don't do any mischief in the last couple days or if they did, you know what went on.

It's questionable whether they want to do this.

A lot of people in this room who are probably cringing right now at these comments because they feel as an employee perhaps that this is not the right type of privacy model that they like, but it really does protect the corporation so auditing, monitoring and preventive forensics are ways you can limit drastically the insider threat because if people know that you're doing that, they're less likely to commit mischief, and if they do, you can figure it out earlier and recover the losses, but it's a question of tolerance for it.

MR. SOLLITTO: One really easy thing is to simply separate responsibility for security from IT, having people who are responsible for maintaining the security network and protecting against bulk intrusions and internal mischief, making sure they report separately up the chain from those actually installing and maintaining the network is an immediate -- that's a large source of possibility for mischief.

MS. CLAY: Good points. Yes?

MR. KUO: I have -- Jimmy Kuo. I have a two-part question, one the first part anybody can jump in, and the second part is for Mr. Winkler primarily but anybody else first.

How do you decide on which patch to apply

whenever you hear all these patches coming out? And the second part is, Do you have any suggestions for how an end user can ascertain the necessity of a particular patch, assuming he even gets the information that a patch is available, and perhaps do you, Mr. Winkler, do any type of semiannual or annual roll up such as patches so that they become easier?

We were talking earlier about the Stay Safe Online campaign having semi annual campaigns to get people to patch, and if we can get more companies to do these semiannual roll ups so that we just have one thing happen all at the same time.

MR. WINKLER: Right, first of all though, caveat of my response, Sun is really not an end user consumer computing client company, right? We sell servers predominantly. We do sell workstations and start up business because that's not our focus.

So our work station users are typically much more sophisticated users than actual consumer or business users, would be more on the side of engineering, so my response as I think the only vendor on the panel would be to identify which patches are necessary.

We're really focused on a different set of users, and it's perhaps more difficult for an average

consumer using our products to determine whether or not a patch would be appropriate.

But to answer the other question, the one about roll ups, we do -- being a vendor we're in business to sell things and so we sell new versions of our operating system. Every about 18 months we have a new release, and we have quarterly releases.

So it makes absolute sense to reinstall the operating system on a quarterly or biannual basis not just from the standpoint of rolling up patches but of being able to access new functionally that's gone through an 18 or 36 month studying period.

MR. KUO: Your standard is just to have quarterly reinstalls of the operating system.

MR. WINKLER: No, updates of the operating system. Most would involve patches as well that have come with that.

MS. GOODENDORF: I would just say that we try and do our patch management the way we do version control management, and we're fortunate in that on our mission critical systems, we have test environments where we can test patches and test new versions before we actually put them in production.

And some patches we frankly don't apply if they

don't seem to be relevant to us or provide any value to us, so we do make decisions about which patches to apply.

MS. CLAY: NIST does also maintain a database of products and vulnerabilities and available patches. However, it does make it very easy for you to go in and click in a spot and have the -- and get to the right patch, but you may want to know whether or not you want that patch before you go to the database because it doesn't help you decide whether or not you want to add that patch, but it does sort of centralize things.

MS. CLAY: Yes, ma'am?

MS. LEVIN: Toby Levin. I'm concerned that we're talking a lot about sort of a patch work of patches, and my question really is -- I wasn't here this morning to hear Dick Clarke's remarks but we have a critical infrastructure problem that is at high risk today, and I don't mean to be an alarmist, but it's frightening when you think about our transportation, telecom, financial sectors, all air transport could all be brought down by some of the viruses and hacking and technology issues that we talked about today.

So my concern is that what you're talking about and what we talked about for the last few panels are

answers that could take decades to put into place, and I don't think we have decades for that to happen, so my question is: Y2K, an effort that was launched with a very short time frame fully involving high levels of leadership, government, industry played key roles inputting out resources that even small businesses and consumers could get help quickly, and we had very little negative fall out from that effort.

My question is: Why can't we do a Y2K effort to deal with these same technology security issues that we're discussing now?

MR. REEDER: I would say facetiously since he's my good friend because John Koskinen refuses to take another task like he did on Y2K. A very good question, a couple of reactions.

One, the level of problem we've been talking about here is not the -- I don't think goes to the question of protecting nuclear power plants or the power grid or the telecommunication system which are indeed for a variety of reasons subject to a higher level of risk than other kinds of -- even notwithstanding its economic importance to the economy and its stockholders, the reservation systems of six Continents -- so we're really talking about an order of magnitude different

problem although the nature of the problem is the same.

I have a problem with the Y2K metaphor because unlike Y2K, I mean one we're not faced with a date certain, and it's not clear that -- and I hate to use the reference like the war on terrorism, it probably will never be over. It's simply a problem of continuing to mitigate and manage the risk which suggests building into our processes and building into our psyches, if you will, a whole different way of approaching the problem than one could if there were more waging a one-time push to get us through January 1 or to midnight of December 31, 1999.

The success of Y2K tends to -- we always like to replicate our successes, but I think the problems are not only in their scale but by their very nature fundamentally different problems. We understood the nature of the problem. We had a date certain by which to fix it, and we went ahead and did that, and in fact we -- and the sum of money involved was reasonably well understood within two orders of magnitudes at least.

I think the problems are simply very, very different.

MR. ZWILLINGER: They're different in part because Y2K was a technology problem, and the threat of

attacks on the infrastructure is a people problem, and the technologies used to help solve the problems, it exacerbates the people problem and it's used to defend against the people problem, but it's a people problem, so it's a very, very different sort of situation.

MS. CLAY: Next.

MR. PALLER: Alan Paller from SANS again. This panel had the end of the day job of pulling it all together, and I didn't expect that to happen, but in fact something really good came out of this and I want to see if it's feasible.

All day we heard it's got to be easier, Scott Charney said we have to have easier to use and we had transparent security, invisible security, we have to get securities out of being a problem and into being easy. And you talked about having your test systems and Frank you talked about having agreed upon benchmarks this is what we want to install and, Vic, you talked about having a server somewhere, and that everyone downloads the current version of the server. I think you know that like --

MR. WINKLER: I'm sorry, I like using servers for lots of things.

MR. PALLER: Yes. Virginia uses some of your

servers. They tried awhile ago to install the operating system. They had great success in installing the operating system. They knew they had to get patches down to protect against known vulnerabilities.

While they were downloading the patches they were infected. They could not get the patches down in time because there are so many automated attack programs on the Internet, and I've been sitting here all day trying to think of what's the general solution.

MR. WINKLER: JAVA, right? It was defined to address exactly that.

MR. PALLER: Right. You install it on your computer. You have Java on your computer, and while JAVA goes and in fact gets the uninfected patches, some hackers take your machine over. JAVA doesn't solve this problem.

MR. WINKLER: To the traditional fat client that happens. If you run a thin client --

MR. PALLER: This is the Microsoft/Sun argument. Let's stay with the servers you sell now. In the future you may sell non servers but right now --

MR. WINKLER: You're focusing the problem on the operating systems, downloading operating systems.

MR. PALLER: You had this great idea which is

users have a version, this is a version. It's a safe version, and we can all go get it if you need it, and that would solve the problem if the safe version were handled by the op staff and the op staff kept the patches up to date.

My question is: How far are we from doing that for consumers? Right now if I download or install a copy of Windows 2000 server edition, odds are I won't get patches down before it's infected with Code Red. There's still 18,000 Code Reds.

So how far are we from getting you, Sun, to deliver to the people who are willing to buy it an up to date patch version of your system every day so that I don't have to buy one that's four months old. It's the end of the day. Let's keep it interesting.

MR. WINKLER: I think I used the term evolution earlier, and we continue to evolve, right? It's a story from the movie in the early 90s, but it is an issue, you just described, circumscribed, a whole bunch of different issues and there are a number of different answers for different parts of those different problems.

One thing that consumers can do is they can choose to buy a different platform from a different vendor who is considered do be a niche player but whose

products interoperate completely with the ones that you mentioned, and that I don't think work for that vendor, but those products have been around for a long time and all you have to do is think different, right, so when you installed that operating system, it doesn't present itself with hostile facing opportunities.

So it's been done. It has been done, and in terms of when a vendor like Sun will deliver a highly complex server product, that shouldn't be installed by uneducated end users, the target installation should be done by somebody who's trained.

We're freshly moving towards that fairly quickly but to put it into perspective, our focus really is on a different layer up in the cloud than the end user layer despite the fact that we did design and build JAVA which is the best computing solution for end users. Or so I think.

MS. CLAY: Frank, did you want to make a quick comment?

MR. REEDER: No.

MS. CLAY: Sorry.

MS. SAVAGE: I'm Jenny Savage from Capital One Financial. We've been talking about standards for software and various pieces of the security program that

we need, and I guess I'm wondering what the feeling is on a little bit tougher standards on the people that you hired to deal with the customers' information.

We as a company fingerprint everybody before they touch customers' information, but not everybody does that, and I guess I would like to know: Shouldn't there be standards across the board for anybody that touches customer information, as far as maybe checking in to background, criminal history, that kind of thing?

MR. WINKLER: Absolutely, and in fact it's odd but I had a VA conference last week and I was looking at different booths and I have a little pamphlet here which the -- I need my glasses. Otherwise I can't read. I don't know who puts this out but if you can read it.

God bless you, it's entitled personal security position sensitivity level designation process, and it is really oriented towards exactly that and this is for the government.

So clearly different positions require different background checks, different ways of trust in those individuals just like different systems in their environment required different degrees of protection or trust.

MS. GOODENDORF: I guess because I'm in the

hospitality industry, though, I would say that in hotels and restaurants, throughout hospitality, consumers prefer to use credit cards, and the nature of our industry is such that to try to do background checks on all the various people working at the front desk and working in restaurants, that type thing, it just wouldn't be manageable for us.

MR. ABRAMS: There are many cities that are full of call centers that do consumer affairs similar to the consumer affairs that you do at Capital One. I think it's a great idea to only have the best, the brightest the most honest.

The fact is for years losing 25 to 35 percent of your workers each year was a bigger issue than making sure that they were the best, the brightest and the most honest. I think that absolutely we should have systems to make sure that we have -- that we're indeed eliminating the people problem. I think it's easier said than done with the pressures we have in filling positions.

MS. SAVAGE: I don't think it could be completely eliminated but I think if you run a thorough background check with anyone that's dealing with customer's personal information could -- it could be a

future.

MR. ZWILLINGER: There's incredible reluctance even when you've identified someone who is in some sort of network management role who is a great employee from a technical point of view to do anything to them, even when you've caught them red handed doing something improper on the networks.

I've been in positions where I would have to produce evidence of this person is stealing from another employee in the company and this is how they're doing it. Yeah, but they're so good, isn't there something we can do.

MS. SAVAGE; that's right, and I think that's where we need standards. If we have standards, we could have all the legal jargon where we need it that says if you had this kind of criminal history or if you've been fired from a job for this or that, you can't have a job that is going to be dealing with customers' information.

I wouldn't want somebody knowing my Social Security -- the more -- if they've had any kind of shady background at all, there's more chance that they're going to do something with my information, so I think that's as important as the software and packets and the

patches and all that.

MR. ABRAMS: Then you have to follow up and indeed make sure your procedures are indeed followed. It's not that many years ago that I was at the Federal Reserve doing bank supervision regulation, and typically it wasn't that the procedures weren't there, and the policies weren't there.

It was, Well, you know, we couldn't afford for them to take two weeks vacation or whatever was the breach, so I think that again building the forensics into the system I think is as important as doing -- yes, you should do -- you should do what's prudent but it's not always prudent to have, it's not always cost effective to do a huge investigation of every single employee.

MR. REEDER: I have nothing to add to the substance, but I would add only two words of caution. One, a labor market concern which I think has already been raised and the other is a humanitarian concern. I worked in an environment about ten blocks down the street where we used to have a policy that anybody who had ever used any controlled substance without authorization was ineligible for employment until we realized that we couldn't hire anybody under a certain

age. I offer that as caution number 1.

Caution number 2, and clearly I wouldn't argue that we should employ pedophiles or individuals with substantial histories of substance abuses as school bus drivers, but people who have had -- who have in the past engaged in activities that we might not approve of need to be kept in society so I urge an awful lot of caution apart from labor market considerations instantly disqualifying large numbers of people.

MR. WINKLER: I have two names to drop, Ames and Hansen, right? These are people who their organizations are and yet --

MR. REEDER: That's the other quick one.

MR. SOLLITTO: One quick follow up on that as well. One thing that I know we try and do at PayPal is, how much information do employees really need. Does CRS really need to know all 16 digits of your credit card to help you?

No. Actually all I need is four numbers so you can be sure you and he are talking about the same credit card but you don't have to worry he has the entire number so we do a number things beyond the vetting and fingerprinting that we do and a variety of things to also say, Let's try to minimize any possibility that

there could be.

Do we really need to have your street address, your town, and your Zip Code or can we simply say are you still on High School Way, and in fact that's one thing we do is limit access to employees of information about customers.

MS. CLAY: Good point s.

MR. AVILA: John Avila. This is primarily a legal question so primarily directed to Mr. Zwillinger. What happens when preventative measures fail and there's a compromise by a consumer enterprise? That disclosure might occur either by intrusion, by an inadvertent disclosure by the enterprise or by some internal malfeasance?

What liability would apply in that situation? Would it be a strict liability? Is there a form of statutory liability? What sorts of damage would be available -- limited to monetary loss by the consumer or with emotional distress, would damages be available, punitive damages, and finally what class of people would have standing to assert a claim? Would it be limited to consumers or for example would the banks that issued credit cards have a claim for their losses as a result of the misuse of consumer credit card?

MR. ZWILLINGER: How much time do you have?

MR. AVILA: How much time do you have? Finally the question would be relating to the last question, I believe there were a couple years an enterprise hired prison inmates for their call centers and they got access to credit card information and of course they took it and used it for criminal purposes.

What kind of liability would be attached to that kind of security procedure?

MR. ZWILLINGER: Without providing any specific legal advice, let me give you a general sense of where the liability doctrines are going in the area of this. You obviously raised a lot of specific points.

For awhile there was no real net of liability in the area. That is there were no standards to look to for a negligence obligation. You have to find what the -- what the standard of care is that you have a duty to live up to and then you find a breach, and we were sort of absent all of those things.

And now we're moving towards a much more liability prone environment because there are standards of care. There's the Gramm-Leach-Bliley Act. The FTC finalized rules that came out on May 17. You have the SEC rule regulation SP. You have HIPAA. You

have a bunch of places where there are regulated entities that have obligations which will rapidly become the standard of care.

But they're not very specific. They don't say, your bylaws are configured this way, your policy has to look like this, but it says you have to do a risk assessment. You have to put in place a policy. I think regulated entities will start being held liable or there will be a move to hold them liable by those people to whom they owe a duty.

And there aren't -- it wouldn't be every third-party down the line, but here would be the shareholders to whom they have a fiduciary duty. It would be the customers to whom they have financial information, but it's not there yet.

There's no third party liability, and where there's been downstream liability efforts, there hasn't been any published decisions. There's been the First Net versus Nike case in Scotland where traffic was redirected and they said Nike didn't manage their domain name well enough so therefore I got a lot of your traffic and you have to compensate me.

It's not there yet so who will be liable? At first just regulated entities. Second after that people

who have the same type of information but aren't regulated. Who will they be liable to? People who they owe an existing duty. Shareholders? What will they be liable for? All damages that are reasonably foreseeable.

That doesn't mean necessarily every consequence. I don't think that's where we're going to start, but coming from a position of no liability moving into the liability environment so it will start slowly and go from there but you have to be concerned about liability that you didn't have two or three years ago and that's about it.

MS. CLAY: One last question.

MR. GARFINKEL: Really short. I'm a big believer in out sourcing and I know the gentleman from PayPal is also and I'm a customer of his, and I read on the mailing list when they filed papers to go public that they only have one data center which they said in their papers to go public that the risk of the catastrophic failure would put them out of business, and so because I'm one of your customers, I would like to know, do you have a second data center yet?

MR. SOLLITTO: We do. Unfortunately I believe they're both within the same fault structure.

MR. GARFINKEL: So how do you vet the people you out source to, not that I'm implying --

MR. SOLLITTO: I'm not sure who we out source to today. There are very few data management systems left in business now in California, but we're fortunately going to be able to take care of a number of them. One of the things we do --

MR. GARFINKEL: I meant how do customers -- let's refer to customers, consumers.

MR. SOLLITTO: How do customers or consumers know the firms they're out sourcing to are taking adequate precautions? Well, I guess that puts the burden back on the consumer usually for education information which perhaps can be a theme of this entire event.

MR. GARFINKEL: The problem is I do not have a lot of access to the information about the companies I could use to make an informed decision. They say that's proprietary information. We know about this. You put it in your 10 K or whatever it was.

MR. SOLLITTO: S 1.

MR. GARFINKEL: There's so many other firms that they do things with my data and I'm told to trust them. VeriSign has taken the credit card on the same mailing

list. I read when you submit your credit card to VeriSign, it doesn't get incented and there's many, many cases where FTC maybe should be enforcing under the advertising stuff that it used to go out to privacy but there are many, many cases where they encourage out sourcing. People we're out sourcing to are not acting in an ethical or responsible manner.

MS. CLAY: Is there some place where businesses can go now to either get a list of questions that they should be asking of someone considering out sourcing or where they can look at the business practices?

MR. SOLLITTO: I know a number of firms retain research consultants and outside experts to help them in their efforts to evaluate proper vendors. My firm looks at Gardner Jupiter and others to help us in a variety of research fronts which include vendor selection and analysis so yes there are resources for businesses.

I think the point is well taken in that there may be less resources available for consumers to either get information or fully evaluate the company they're choosing to use, but that's something that a good business will do.

I know that just off point real quick many customers always ask, Well, gosh, where is my money when

it's with you all, and so one of the things also we did is put a little pop up on the front page, click here to see the six banks your money is current sitting at today.

And then it changes daily and they know that information is there, so good businesses will recognize that consumers are not like the Simpsons. Most consumers want to know as much as they can so they can make the evaluations they need and hopefully those customers will be rewarded by usage, and that's frankly how the market shortly will look.

MS. GOODENDORF: I would say something there that I think there's a predicament when you're running an information security program in a company like I am which is that while I want to reassure consumers, I don't want to give clues to the bad guys on the particulars of how we're arranged and what platforms we have and so forth.

And I kind of wish that we could have something that would resemble the Good Housekeeping seal of approval, that we could have something that would be a standard or an independent kind of a mark to tell consumers, Okay, we meet this criteria or these standards without giving them the particulars of how we

perform our security.

MR. ZWILLINGER: There are certification authorities. I mean, there are three I can think of right now that do it, network information security systems, but I think there will be a move with the new standards like in Europe with British Standard 7799. There will be a lot of certification authorities who will give you your good housekeeping approval, and Foundstone Internet Security System and TRUSTe and other people will do it.

MS. CLAY: Frank? Okay. You kept fooling me, Frank.

Well, that's all we have time for. I think this was a very good discussion, and again I just want to say that the panelists are going to provide Mark with some resources to put up on the FTC web site so you can get more detail on some of the things we talked about. Thank you again.

MR. EICHORN: Just a moment here. I want to introduce Howard Beales for the close, if you could get settled for one moment.

MR. BEALES: I promise not to keep you very long, but before we close I would like to thank the panelists for speaking about information security. I'm

very impressed with the knowledge base we've assembled here, and I hope we'll be able to continue to tap into that expertise as we go forward.

I would like to make a few observations on some of the themes that I've seen emerge from the first day of the workshop. There's more of the workshop tomorrow, but I think we can look at the panels today as focusing on where we are now and what businesses and consumers can do about it today.

Tomorrow, fittingly, we'll be looking at what can be done tomorrow, what approaches or ideas or movements are beginning to develop that may take a little longer to happen and may make things a little better.

Here's what I think we've learned so far. Our first panel made clear that there's a growing number of threats out there of different varieties and that technology advances like broadband, Instant Messaging, and wireless have created new areas of vulnerability.

The potential threats are daunting. As a technical matter, securing one system from a sophisticated determined hacker is extremely difficult, but there are things that knowledgeable consumers can do to significantly decrease their exposure to the most common security risks.

Some of these steps involve simple good security practices and little or no expense. For example, you can physically disconnect a broadband Internet connection when it's not in use or not open email attachments when you don't know what they are.

Other steps take more effort and involve monitoring threats and updating or patching accordingly, and as we learned today there's a wide variety of products and services available to assist consumers in reducing their risks.

We've also heard about some imaginative methods for delivering these products to consumers so maintaining one's security is a little bit easier. We've learned that although there's a lot of people here today who are working to educate consumers, there are a lot of consumers who don't know the dangers or what options they have to reduce the risk or why security is important.

As a result, many people do not take simple steps to safeguard their own security and their own information. More consumer education would be helpful in getting the message out. From the business perspective, managing security is a constant process that involves frequent trade-offs between considerations

like security and privacy, security and convenience and security and cost to name a few.

A vigilant chief security officer or chief information officer, sometimes with the help of outside consultants or managed security services, can do a lot to reduce the risks by planning, analyzing, and managing risks, and by responding quickly to incidents when they occur.

That's where we are at this point. Tune in tomorrow.

(Whereupon, at 5:05 p.m., the workshop was adjourned.)

C E R T I F I C A T I O N O F R E P O R T E R

CASE TITLE: WORKSHOP

HEARING DATE: MAY 20, 2002

I HEREBY CERTIFY that the transcript contained herein is a full and accurate transcript of the notes taken by me at the hearing on the above cause before the FEDERAL TRADE COMMISSION to the best of my knowledge and belief.

DATED: JUNE 4, 2002

DEBRA L. MAHEUX

C E R T I F I C A T I O N O F P R O O F R E A D E R

I HEREBY CERTIFY that I proofread the transcript for accuracy in spelling, hyphenation, punctuation and format.

DIANE QUADE