PANEL 5: BUILDING SECURITY INTO THE ARCHITECTURE FOR SAFER COMPUTING

MS. GARRISON: Good afternoon. Again, I am Loretta Garrison. I will be moderating today. Welcome to the final panel of day one. It has been a really exciting, stimulating, challenging day for all of us, and we appreciate your continuing to hang in there with us. We realize that we have a very full agenda.

I would like to introduce the panelists for this last session. From my left, the far end, Alan Paller. Next to him, Jim Halpert. Then Gerard Lewis, Andrew Patrick, and to my right, Frank Reeder, Phil Reitinger, and Howard Schmidt. Also joining me is Toby Levin, from the Federal Trade Commission, to assist.

We have gained much insight and understanding today about what has happened to the technologies that protect consumer information, and why they have and have not worked, what it is about consumer behavior that makes technology-effective, and what is actually used by consumers it's designed for, and about building protections into the architecture of identity management systems.

Picking up on a design challenge that we heard from this afternoon's opening panel, we are concluding this day with a discussion about building security into the architecture for safer computing.

To begin with, we will have introductory remarks by Howard Schmidt, who is going to give us a report card on the current status of the security of home computing. Howard? MR. SCHMIDT: Thank you very much, Loretta, and thank you all for being here and giving me the opportunity to talk.

I would be tremendously remiss, had I not started out by thanking Loretta and Toby for the work that they have done on pulling this together. I know the term herding cats means absolutely nothing when it comes to the work that they have done, but I very much appreciate it.

MS. LEVIN: James Silver, as well. We're a trio.

MR. SCHMIDT: Oh, okay, great. Thank you.

MS. GARRISON: Thank you.

MR. SCHMIDT: Anyway, I want to just quickly talk a little bit about the report card of where we have been, where we are, and, presumably, where we are going, relative to consumer online security.

And I want to do it by framing it, first, from a perspective that it's not just the technology. You know, we have this other PPT that we talk about. It's the people, the processes, and the technology. And so in looking at that, we look at a broad spectrum, what it means to be safe online, what it means to have a safe online experience, and how computing is safer now than it has been.

Then I want to break it down into four specific areas, and it's particularly rewarding to follow the previous panel that discussed so much the areas around authentication and public infrastructure, and the need for revamping this, and how it relates to the things we are doing. Because one of the first things we need to look at is where we are today, where we have been, as a report card, regarding authentication mechanisms.

It seems that much of the world today is framed in pre-9/11 2001 and post-9/11. But I actually want to roll back a little bit further to pre-2001, and I use January of 2001 as sort of the linchpin, because prior to that, we didn't have that culture of security that Orson and many of us have talked about. We've started to move a lot closer to that.

So, if you look at that authentication piece prior to January of 2001, it was pretty much anybody's guess out there. There were no requirements, no recommendations about strong authentication mechanisms. In many cases, the software that came installed had accounts on there that were administrative accounts that required no passwords and no one even knew that.

Then we zoom ahead to the 2001 to 2003 time frame, where we basically -- every time a window opens up on one of the online services, it says, "Do not give out your password."

There are windows that come up that are basically just for the authentication piece. There is an encrypted session that takes place between your computer system and an authentication computer that makes that a safer experience, so someone can't grab the data as it transits itself and pull passwords out of there, which used to be the older way of doing it, prior to 2001.

We see an increase of use of IPSec and SSL and these sorts of encryption technologies. We also see better protection of privacy, as part of that consumer experience, post-2001.

And I want to zoom into now the future piece, and that's where are we going with the authentication piece from our report card, and that's the fact that strong passwords are now becoming very commonplace.

The downside is it's very difficult to remember, which is why the next piece of this, which we are starting to move to, is the two-factor authentication, whether it's smart cards, biometrics, whatever mechanism one would use, we're starting to see that becoming more and more relevant. We're starting to see a lot of discussion and a lot of the building of that into the consumer space, including the operating systems which now support that.

We have also seen an increase in the number of reportings, which, once again, makes things safer. If you look at the neighborhood watch type concept, where you have neighbors looking out for neighbors, other people putting up signs saying, "Listen, if you see something suspicious, notify someone."

We actually now are training state and local law enforcement. We are getting a tremendous amount of support from the FTC working with the consumer, and understanding how do you report these things, where do you wind up sending information where your experience has been less than positive, for malicious activity? So that's sort of the authentication piece.

The next piece I want to go to is the configuration, and this is very crucial. Prior to 2001, most of the systems were designed for usability and manageability, especially in the consumer space, especially for the desktop person. It was, "How easy can we make this?"

Unfortunately, the easiness also gave us a very wide window to make it less safe, more accessible -- for bad people to do bad things to the system, including just some of the basic, core software running on your system that you didn't know was running on there.

You know, we have seen a number of cases where viruses and Trojans, and some of the things that have occurred that have either pulled password files down off of people's systems, opened those -- installed Trojans, where people could then take over a consumer's system. They were able to be successful because there were underlying components that were running that people didn't know about.

In the 2001 to 2003 time frame we have seen that change dramatically. We have seen a mixed bag of changes that have taken place, normally through the process of doing updates, normally through the process of telling people, "Here is a patch, here is something you need to do to make your system more secure," that either turns off those services or reduces the accessibility from the outside world of those services.

Then, of course, the current state, and once again, increasingly so in the future, is the whole concept of secure out-of-the-box. When you log in on the system, whenever you first turn on your system and plug it into your cable modem, you won't have blank passwords on the system that someone could automatically take over.

You won't have services running on the system that someone can then compromise and work there.

And the same thing goes with access points for wireless. Cable modems, DSL, and wireless technology are phenomenal. I have been using it since I could get my first cable and load them up on the mountain. I have been using wireless since it first came out. And what we're seeing now is that transition over the past two years, where the wireless manufacturers, the cable manufacturers are putting personal firewalls into the hardware, in addition to software-based things you are running.

You are also seeing upgrades that they have on their systems for those of us that have older systems, where basically you can go into the system configuration on the wireless access point, and it says, "Download your free personal firewall, download your free anti-virus software." Those things are there now to better protect the consumer, to make our online experience much better.

The third piece of this is the awareness. Prior to 2001, it was word of mouth. If we knew somebody that had something bad happen to them, you would generally hear about it, but you didn't see much publicity about it. You saw instances where SANS and organizations like that would publish information, generally to the IT professional community, but the consumer side generally didn't subscribe to those sort of things.

So, in the 2001 to 2003 time frame, we have seen SANS, vendors, the information sharing analysis centers, the ISACs, media, FTC through the Dewey site and the information security site, the White House, working with the Cyber Security Alliance to put up websites, FAQs, how to help consumers better enjoy the experience, while protecting themselves.

And of course, moving forward, what we will see taking place are situations where customer service will have security and privacy as part of the core competency. When you call in to someone about why something doesn't work, there will be the discussion about security and privacy. "Do you have this enabled? Do you use a strong password?" These are things that are going to be part of the core DNA, as we're moving forward.

And including the ability to provide services for the websites. One of the things I have seen recently, particularly on the broadband deployments, where when you log into the website at whatever cable carrier it is, just like they do on the modems, they have a link that says, "Click here for security, click here for privacy." So these are things that we're seeing in the awareness piece.

And lastly, and the one that I think eventually we will be able to say, "Gee, that used to be a problem back in the early 2000s," and that is that whole concept of patch management.

Whether it's Linux, Windows, OS10, Sun, Oracle, we have seen in the past it was sort of a pull. If I knew there was something that I had to fix, I would go out and pull the bits down and fix it. I would pull the data down and fix my systems. And the 2001 to 2003 time frame, we saw this service where you can sign up for it, where it will say, "You need to fix something on your system. Here is the data that you need to do that, here is the link to do that."

And you have some options. Currently, in most of the situations, they will automatically install it for you. In many of the operating systems and many of the major applications, for the consumer space, the same thing.

You have a box. If you're technically competent, like some of us may be, we may want to say, "Well, tell me what it is before you install it." Other cases, "Please do it, because I don't want to have to worry about it." I use that 86-year-old father of mine as the example of, "Please do it, I don't know what I'm doing. Fix it for me."

And then, in the future, of course, it will all be push. We will have the self-healing, the self-repairing systems. We no longer will need to worry about having a bachelor's degree in computer science in order to have a full and safe consumer experience.

So, in closing my opening comments, I want to cite something that I attribute to Doris, and a lot of the work around the OECD, and that's my definition of the culture of security in the online world. And the analogy I use is the seat belt example that some of you may have heard before.

You remember back when seat belts first came out? We found out a couple of things about them. First and foremost, they were extremely uncomfortable, because when we sat on them they hurt after a while. But that's what we did, we sat on them. And despite the best efforts of the highway transportation folks, despite the best efforts of law enforcement, we sat on the seat belts.

Then, later on, they put those annoying buzzers in there, and we learned that they become even more uncomfortable when you get them a little bit higher behind your back, because we would connect them behind our back to shut off the buzzer.

And then, eventually, it got to the point where it became part of the infrastructure, part of the car. And I remember the first time I sat in the car, closed the door and this belt automatically goes across me, and I think, "If you're going to go to that much trouble, I'm going to wear it."

Then I ask any of you today, as I have said many times, find a six to eight-year-old child, put them in a car, and what's the first thing they do? They buckle that seat belt. That's the culture of security that we have seen in that world. In some instances, it took regulation, and in many, many instances, it was done because it was the right thing to do.

And that's the same thing as I see us moving into the consumer space as I look at our report card two years from now, in saying we will have that culture of security. These things will be built in from the very beginning. We will have a user base that is much safer, respectful of privacy, and has a much richer online experience as we move forward.

So, thank you very much for the opportunity to give those opening remarks.

(Applause.)

MS. GARRISON: Thank you, Howard, and we do look forward to that report card in two years.

We have heard an awful lot today about people who are struggling in many different ways in trying to use their technology. The 144 passwords certainly stands out.

But the big message that we also heard from the consumer groups and from the academics, is that it has to be usable, it has to be simple. It has to be integrated into the system, you just turn it on and it works. And it has to be interoperable.

So, part of the challenge here today is how do we talk about designing technology for safer computing that incorporates these features?

But before we get there, I would like to ask first, is home computing safer today than it was a year ago? Why, or why not? Jim, can you help us with that?

MR. HALPERT: Loretta, I think it is. And Howard outlined a number of very important ways in which things have gotten better, if one takes 9/11/2001 as the measuring point.

There is greater awareness among consumers -- and we're focusing here on the consumer market -- and on the providers of various technologies, and providers of Internet service.

I am here as general counsel of a trade group of leading ISPs called the Internet Commerce Coalition, and I can tell you that all of these companies invest very heavily in upgrading network infrastructure, increasingly in R&D, actually, to develop network security solutions. They are working actively on rapid and coordinated and collective responses to security threats in the network, like denial of service attacks and worms.

And in many cases, companies will discover problems and alert their competitors, because this is a common issue of trust in the network, and something that network operators are uniquely situated to address.

They are also investing in detecting and filtering out the transmission of malicious codes, such as e-mail viruses, worms, Trojan horses, and denial of service attacks. These are automated mechanisms to try to stop these transmissions. They are not always successful. The back-up is to have a very rapid and coordinated reporting mechanism, so that Internet companies can alert each other to problems that are coming down the pike, and alert their customers.

There also is a significant effort to educate customers regarding the importance of network security. This is something that the government can play a very important role in, and the press can play an important role in.

Howard mentioned going to websites and being able to download security tools. Our member companies are investing in robust and prominent security portions of their websites that educate consumers about what to do and not to do with regard to network security, and give them easy access, through clicking on hyperlinks to additional tools to upgrade security.

Finally, there actually is an important role in providing customers with ready access, at the edge of the network, to tools that come with the sign-up for service.

For example, customers of broadband networks can get, through our broadband members, discounted firewalls, in some cases free firewall technology, free anti-virus software with upgrades provided, say, for a year on a free basis, some password protection tools to make sure that customers use secure passwords and have encrypted connections as they log into the network.

And also -- and this is very important on the theme that the FTC has spent a lot of time on in the past -- parental control software, to protect other aspects of security for children, for example, who are on the Internet.

ISPs are much better situated to protect the security of their actual network, rather than the activities or software on end user computers that are just off the network. However, even there, our members have made major efforts appropriate to the particular market they serve. And this will vary widely.

For example, a big backbone provider that provides a direct Internet connection to a corporate network is going to provide a very different set of security tools to network administrators than will a narrow band provider that is serving consumers in the home.

In addition, proprietary online service providers, like our member AOL, have a different -- and in some ways, an easier job protecting security than providers that are simply entirely open to the Internet.

So, there are a range of different tools, but companies are spending a lot of time and effort on this increasingly important area of providing a good and safe network.

MS. GARRISON: All right, thank you. Jerry, can you give us a summary from Comcast's point of view?

MR. LEWIS: Sure, thank you. And, first of all, thanks to Commissioner Swindle and the FTC for having us. We appreciate the chance to be here. And to the staff, who has done a great job organizing this.

Let me give just a little bit of background. Part of our panel topic today is network architecture, and I would just like to spend a second talking about where we are in the history of network architecture, particularly with respect to cable-based Internet service providers.

You may remember almost 18 months ago Excite@ home filed for bankruptcy. They were the outsourced Internet service provider for many cable operators, Comcast included. And that forced us and the other cable companies that used Excite@home as their ISP solution to scramble quickly, and at great cost, to deploy and build our own networks so that we could, in effect, keep the lights on for our Excite@home customers.

And we, like the several other cable ISPs, did that in about 90 days, literally, logically and physically deployed an ISP network that we had planned to deploy in about 9 months. It wasn't without some fits and starts, but it basically worked, and it's been humming along very nicely ever since.

So, we at Comcast, and I think many other cable ISPs – are at a fairly early stage in the architecture of the network, and as a result, many of our decisions with respect to customer-facing security, I think, have been driven more practically and tactically, given where we are.

And so, what we have decided to do -- at least currently, at Comcast – is offer a McAfee and -- I'm not necessarily promoting them, it's just that they're the partner we're working with currently -- firewall, client software. It's their standard retail offering that our customers can download directly through our website for free. And it's a one-year free firewall.

McAfee actually owns the customer, provides all the technical support, the updates automatically, and handles the customer relationship, because they're best suited to do that. We don't necessarily have a lot of expertise or depth yet at 1-800-COMCAST for dealing with firewall questions, for example.

That's a model that has worked fairly well. We have had a relatively high adoption rate among our subscribers for the firewall. And when we look at this relationship and other things that we can add to it, we certainly will look at adding anti-virus and privacy, and other types of security tools into the mix. It's really dictated by business considerations, in large part, and by our desire to provide a valuable solution to our customers, who do communicate with us and say privacy is of concern to them, security is of concern to them.

And right now, I think where we are, as many other cable ISPs may be, is that this is a best outsourced solution right now. That may not always be the case. And over time, our security solution may be a hybrid of outsourced technologies like a McAfee, as well as some home grown things.

MS. GARRISON: Jerry, one question.

MR. LEWIS: Sure.

MS. GARRISON: When did this go into effect for your customers, and what is the adoption rate? Do you have that figure?

MR. LEWIS: We haven't publicized the adoption rate, but in the areas that we have heavily promoted it, it has been very high, and we have been very pleased with the adoption rate. And we are in the process, as we all know, of merging our AT&T broadband systems into Comcast systems that will be complete this summer.

And at that point, we will have over 4 million ISP subscribers, and we will be looking to make sure everybody has the opportunity to upgrade and get the benefit of the firewall solution.

We started offering the firewall, if I remember correctly, about six months ago. Prior to that, we had offered anti-virus services through McAfee. And the way the affiliate relationship works is that people who take the firewall for free can get a special deal from McAfee on the security and the privacy components, as well as their security threat assessment center, which is actually a pretty cool little thing if you have played with it.

When the deal comes for reupping, we will certainly look at adding new things into the mix, and new values for customers, and give them perhaps a mix of free and discount, so that they can continue to get the benefit of the services.

What we have done in terms of customer notification and education -- and that's really where I think we and a lot of the ISPs, not just cable-based, are really at the early stages -- is developing home-grown materials, FAQs and other education, as well as leveraging what third parties have done.

We're linking to Dewey the Turtle, when the new portal rolls out in about 60 days. There are a lot of other good third-party sources out there that we direct our customers to, so we will continue to grow and enhance that area.

And the user education piece, I think, is very important. It's something that I think we have a responsibility to do, and we take seriously, and are doing that.

In terms of the future direction, the architecture, if you will, of network security, what things might be coming down the road? A couple of things to speculate about.

I think Jim alluded to it, there will be things beyond pure security that will be of value and interest to our customers. Parental controls is one example. Pop-up blocking, spyware filters, there is an awful lot of things out there that many ISPs currently address that we may address as part of an overall security solution.

You may not think of pop-ups necessarily as a security issue, or parental controls as a security issue, but they all start to get into the overall category of user control over their Internet experience. So, that may well be something that we look at next.

Anti-virus is something that's critical, that we promote heavily. Anti-virus licensing, however, is not always the easiest or most cost effective thing for ISPs to do. So I think for the time being, anti-virus is probably something that will be deployed on a client basis to individual customers, as opposed to on an enterprise basis, where the ISP might do the vast majority of the anti-virus filtering, though we do do some at the network level.

And the last point I will make is with respect to where these solutions go, the privacy and security solutions. Right now, we are following a client model which puts the obligation on the customer to download software and install it properly on their hard disk. With good tools and wizards, that can be a relatively painless process.

But again, that's work. And as I think we have all heard today, and I think we're all in agreement, the more work for people, the less likely people are to use it. So we want to simplify that.

We have looked at, and will continue to look at deploying security and privacy technologies on our network at our end. There are different issues and considerations there.

If we were to deploy a security tool that four million or five million ISP customers had to access, that's a whole different calculation for us. Different hardware requirements, scalability requirements, that we don't necessarily see if we push the solution down to the customer. So that's part of the cost benefit analysis that we constantly do.

And there may be other extended factors that impact security on the network. They may be external factors. For example, law enforcement requests or requirements on the telecommunication side. The Communications Assistance for Law Enforcement Act (CALEA) Statute sets fairly strict technical requirements on the telephone network for intercepts, and the like. Perhaps there will be some counterpart or equivalent on IP-based networks at some point in the future.

So, there may be a variety of external constraints or guidelines, legal or standards, or otherwise, that are impacted. But that's, in a nutshell, what we have been doing. I would be happy to answer any questions later.

MS. GARRISON: Thank you very much. Phil, can we hear about Microsoft?

MR. REITINGER: Sure, Loretta. Thank you. But I'm not going to talk just about Microsoft. I also would like to compliment the FTC for separating Alan and me at far ends of the table to prevent me from needing a transfusion by the end. But it was unnecessary.

MS. LEVIN: Not deliberate.

MR. REITINGER: I will take Alan's criticisms with good grace, and thank him for his compliments for the things he thinks Microsoft has done right.

Let me answer the question as directly as I can. Is computing safer now than it was several years ago? The answer to that is yes, but I think it's a complex answer.

First, statistically, I don't think we know. In other words, we don't have good statistical metrics for how secure the Internet is, and we don't know, statistically yet, how prevalent cyber crime is. There is a lot of good work that has been done, including by groups like the FBI and CSI out in San Francisco. But a lot of that is anecdotal. So we don't have good measurements yet to know how good a job we're doing.

However, we do know that software has become more secure, for a lot of the reasons that Howard identified, and Alan identified, also, earlier.

The old paradigm of functionality over security has changed. It no longer is prevalent, I think, in the industry, both for Microsoft and for other software players. And I think there are a lot of reasons for that.

September 11th is part of the reason. I think we see a greater market focus on security every year. All you have to do is attend the RSA trade shows, and watch the number and quality of security products that are available.

And I also think the industry is maturing. And as the industry matures, it's doing a better and better job of addressing the spectrum of issues that it needs to.

So, you see things like -- and I will use Microsoft terminology here, because it's what I am most familiar with, I work for Microsoft -- the creation of the trustworthy computing initiative January 2002, which has 4 distinct elements: security, privacy, business integrity, and reliability. So, security and privacy are both in that, and let me drill down a little on security.

Howard, I think, has already covered most of the major elements of that, but it's not something that's relatively simple. There are four elements in Microsoft's terminology.

"Secure by design." And this gets to the specific topic of the panel. It has two features, essentially. One, writing better code, not putting vulnerabilities in. And secondarily, architecting for security. As you go forward, designing products so that, for example, processes run at the lowest level of privilege possible, if we can get to some level of technical specificity there, dealing with some of the issues that Alan raised earlier.

Second, as Howard was talking about configuration, "secure by default." Products that are secure out of the box, both server products like Windows 2003 that Alan talked about earlier, and consumer products, so that products like Outlook, from Microsoft, now ship with much more secure default settings.

And then critically, as we move to unmanaged environments, "secure by deployment." Making, as Howard said, patching easier so it's automatic, it can be done as transparently as possible to the consumer, and providing guidance on how to configure systems securely. Microsoft has done configuration guides, and we have been assisted by other configuration guides, such as those done by CIS and Frank Reeder, on my right.

And finally, "communications." Providing a rapid response capability that's also associated with secure by deployment, and communicating with people about what we're doing, such as through the MSRC, the security response center at Microsoft.

Now, what does all this mean? Does it mean that we're not going to see vulnerabilities in the future? No. I would like to harken back to where Commissioner Swindle started us. And if I could paraphrase you for a second, sir, we're not going to find a solution, but we're going to solve a lot of problems as we work towards that end. That's exactly right.

We need to make computing reasonably secure, so that it's functional and that we address the problems, both as they come up, and proactively, before they come up. So that's the second point.

The third point, yes, software is more secure. But it is also true, as we learned this morning, that the threat is increasing. Hackers are really, really good at developing new attack technologies. And they are a lot better at sharing information than we tend to be in the private or the public sectors.

So, industry needs to continue to innovate, and continue to develop more and better security solutions and architect products better. Because we've got, essentially, two growth curves, increasing security of products and increasing threat. We have got to make sure that we widen the gap so that security increases, rather than decreases, over time.

And the fourth point, and then I will close, is technical solutions are not sufficient, in and of themselves. As Howard had emphasized, we really need a multi-disciplinary response, more secure technical infrastructure, management solutions, education, R&D, deterrents so that when cyber crime happens, we put the bad guys in jail.

So, when the question is put what do we need to do to address computer security, the answer is D, all of the above. And you can write whatever you want there, it's all of the above. Thank you.

MS. GARRISON: Thank you. Phil and Jim have both said that home computing is much safer today. But Andrew, can you quickly recap what consumers think about safer computing?

MR. PATRICK: Great, thank you. Yes, I want to buck the trend and say computing, from a home user/consumer point of view, is a much scarier place than it's ever been.

When you think about users' concerns in terms of the major things they are concerned about, their security, their information security, their information privacy, their experiences when going online and threats to their system, it's a very scary place.

Consider, for example, a scenario where you're asked to go and help a couple with children go and buy their first computer at a computer store, and you've been asked to tag along, because they think you know something about computers.

So, you go and pick out a reasonable computer configuration for a home computer, and you might pick up an office suite, because they want to do some word processing, and they want to go on the Internet.

You can't stop there. We have talked about at least eight different things that you also must buy at that computer store in order to be running something that is reasonably secure, safe, and will have good experiences. Anti-virus software, anti-spyware software, cookie management systems you either have to buy or learn how to use, things like P3P and cookie washers.

Firewall, perhaps two of them, hardware and software. A pop-up blocker, because that has a lot to do with experiences, especially experiences with children and what they see, and what you might not want them to see.

Some kind of a spam control system, and some kind of a parental control system. That's a lot of stuff to buy and to configure and use. My quick calculation on the back of an envelope says it probably adds about 15 percent to the cost of the system before you've been out the door, which is not insignificant.

All of this is for something that you don't want to do. You didn't buy the computer to do this. You bought the computer to do some office applications, to write some good-looking letters and reports, and to help the kids with the homework, and go on the Internet.

So, the other big problem is none of this is your primary task. Your primary task is not to operate a safe computer. Your primary task is to do the things that you want to do. So, we have problems that are not related to why people are using computers, and that makes it very hard for people.

MS. GARRISON: Thanks. Howard, I would like to talk about barriers to safer computing. For example, lack of education, technology, money, will, and also about legacy systems. Are older computers a risk for security, for personal use?

MR. SCHMIDT: Yes, I think I will start with the last question first, and address that, because that, indeed, is one of the issues we have looked at for a long time.

If you envision the IT space today in three boxes, there is the legacy systems, there is the world we're living in now, and the future systems. The future is one I think we are all very, very convinced that things will be more secure. They continuously work better, as Phil pointed out, as have a few of the other speakers.

The space we're living in today is we're enjoying the experience, while we're fighting some of the Trojans and the viruses and some of those things. But all in all, it's a positive experience for many people.

But the legacy piece -- that's the part that creates a lot of the problems for us. In some cases, the software was not designed to be in such a threat-ridden environment as you know, "always on" connections provided us. The software is, often times, not as robust in looking for viruses and blocking malicious codes, and things of that nature.

So, consequently, I think the easy answer is for just everybody to upgrade to the latest product, which is more secure, more privacy aware, but unfortunately, there are some financial constraints in conjunction with that.

So, I think that's the biggest barrier I see right now for being more secure quickly, it's just some of the legacy systems or products that's out there.

MS. GARRISON: And Howard, is it true that when you look across product lines, and the extent to which people retain older systems, or older products, that in the computer world there is a much higher retention rate among older systems?

MR. SCHMIDT: Well, I think it goes two ways. It depends on your penchant for technology. I'm the proverbial early adopter. I'm the one that will buy a $600 piece of equipment, knowing in six months it's going to sell for $49.95. And those of us that are of that ilk, we obviously will continuously upgrade.

You will have sort of the middle range, where people will have a family computer that, as the prices continue to go down, the experience becomes more rich, more robust. They will pass that on to the kids as their computer, as they buy themselves a new one.

So we will see some migration of some of the products, but often times we will see some people that say, "Hey, it works. I like it. I don't want to change it, I'm afraid to do something different," so they will keep the hardware and software longer.

MS. GARRISON: And are there any special problems in terms of security of information with disposal of old computers?

MR. SCHMIDT: Well, now that you mention it, that's a concern especially in a consumer environment, but even more so in the corporate environment. Many times people will just turn their old computers in, recycle them, and personal data is sitting on the hard drives.

So, by developing a process before you turn it out -- it's almost like the analog, the paper world now. Shredders are selling at this unbelievable rate. There's a TV commercial saying, "Here, protect your information by buying a shredder." We see that now.

Same thing, electronically, we have to remember that much of that data on your computer is accessible, even if you reformat the hard drive. You have got to take some steps to wipe it out completely before you turn it in to a salvage operation.

MS. GARRISON: Thanks. Alan, do you have anything to add to that?

MR. PALLER: No, I think he did a great job.

MS. GARRISON: All right. Andrew, do you want to speak very briefly about password vulnerabilities? We heard an awful lot about it in the earlier panel.

MR. PATRICK: We heard a lot about passwords. I just wanted to add one other thing, which was we talked a lot about users and users' password behaviors -- writing them down, forgetting them, sharing them. We should also talk a little bit about what can be done from an operator's point of view, in terms of making password systems more usable and more secure.

For example, practices like forcing password changes immediately are very bad practices. People don't forget on demand, and so asking them to immediately choose a new password -- forget the old one and remember the new one -- is just a very bad practice. You get much better password choice and password remembering if you give people warning.

Obviously, asking for multiple passwords, especially when they're not absolutely necessary can be a concern. We have talked about having clear password rules, teaching people how to make good passwords. There is a lot of software around that will look at passwords as people choose them, and make recommendations on those, and that software is not used very much. So, if people enter weak passwords, they can get feedback from the software immediately, before that password is accepted. Those kinds of practices can really help.

There is a reason why people share passwords. They write them down and they share them because, often, the work requires the sharing of information. If you're operating systems that don't support information sharing, such as sharing of documents across users, if you're operating a system that doesn't support people who may forget their passwords, if you don't plan for password forgetting, then it's no wonder that people start writing them down.

If there is at all a high cost, such as social or work or otherwise, for users forgetting a password, of course they're going to write it down. So if you don't have 24/7 password support, or an easy way for people to get their passwords reset, what are they going to do? Of course they're going to write it down.

Although passwords are weak, they are weak for a reason. Users' behavior with passwords has been well studied. There are lots of things that can be done here, and it really can be summarized in focusing on three questions.

You have to consider teaching the users why good passwords are important. Many people feel that they are a small cog in an organization, and so their particular password may not mean very much. But we know that a small vulnerability can be a large vulnerability.

So, you have to answer the question why. Why do I need a good password? You have to answer the question how. How do I create a good password? You have to show examples, get feedback, and support passwords that allow people to get the job done, such as group passwords and work sharing.

And finally, you have to answer the question of how many, and we have talked about that. You really have to think about how many passwords, and what you're really asking people to remember, and realizing that they are not going to remember it, they're going to do something else. And until you have solutions like single sign-on, and whatever, realize that people are just being asked to do too many.

MS. GARRISON: Thank you. Alan, I would like to ask you what are the principal threats that weak security causes for home users? Is it primarily that hackers can steal personal information for identity theft? And what can consumers do, technologically or otherwise, to protect themselves?

MR. PALLER: I think what you described as the principal threat is the one that's most often called up when somebody is trying to sell people security, it's almost never the real threat. There are three real threats.

But before I answer the question, today is actually a celebration day in the security field. Listening to Jim talking about ISPs in a sense competing for who has got the better security offerings -- not all of your ISPs have all of the services, and then Comcast says, "And we have these" -- that's a huge change.

And the man sitting over there, and the man sitting over there, and Dick Clark all get enormous credit for changing the marketplace to where the consumers expect it. It wasn't you saying it to the vendors that changed anything. It was you saying it to the consumers and the consumers saying it to the vendors and then the vendors said, "Oh, well, our customers want it."

And listening to Dell talking about what they're doing, it's a massive shift in everything, and I think there are some bows that you all should take.

Having said that, there are still some threats. Everything is getting better, much better, but there are still some problems. And the problems, actually, are not quite solved by what we have heard, so I want to talk about three threats to the home user.

The most common one is their machines are being taken over, generally, by automated software, or by downloading something that they shouldn't have downloaded. Often, their kids do the downloading, and it's on the parents' computer. So it's not quite the user who could be educated, it's the kid you wouldn't want to give a driver's license to being out and doing things.

That's happening at the rate of what we believe is between 30,000 and 50,000 a week. And honestly, I couldn't care less. Meaning if 30,000 people get their computers taken over and they have all got trouble, it wouldn't matter, except we have got a different problem, and that problem is -- well, let me talk about when they learn about it.

The way they learn about it is either somebody puts pornography on that system they took over, or they put software on it, or they used that computer to attack the Defense Department. And the way they hear about it is when the FBI knocks on their door and says, "Why is your computer attacking DSA?"

And I asked the head of the FBI's cyber crime unit in Baltimore, "Does that happen very often?" And he said, "Alan, all the time." And then he paused, and he said, "All the time."

So, this is not uncommon, and that's a bad thing, that's bad. But that's not what I'm worried about. I am worried about it because, as you will all learn later in the summer, somewhere between 500,000 and 1,000,000 machines taken over is sufficient to take the Internet down and keep it down. And 30,000 to 50,000 a week doesn't divide that badly into 1,000,000. And that's the reason we care.

And so, when I tell Phil that I worry about the older machines, and I don't just worry about the new machines that are coming out, you've got to do something for me about the older machines -- it isn't because I'm worried about somebody losing their personal data. It's that I don't want another 30,000 machines being taken over by somebody who can use them in a concerted fashion to attack what we think of as our e-commerce engine.

The other two threats, though, real quickly, are that the attacker can damage your computer. This happens a lot with Kazaa and other things, but that software can actually take you out, and you can't do anything. And your machine dies, and the idea of backups for most of us is a foreign term, it's not English, we don't know what it is.

So, cleaning the machine up and getting it back is really a very difficult thing. And just as an example, of the 150,000 machines that were taken over with Code Red, we think about 30,000 are still just as infected as they were before, because it's so much trouble to clean up. And the reason we know that is there are about 30,000 machines out there trying to infect other people, so it's likely.

But the last one that I think is important as a real threat -- you all have heard of VPN, virtual private networks, and you think, wow, cool security system. I can use the Internet, I can sit at my home, go through the safe system, and get to my computer.

It turns out that's right, but there are lots of cases where the attackers know this. They infect your machine, and if you think you're smart enough to beat being infected, challenge me some time. They take over your machine because they know you're an employee of the Justice Department or employee of DEA, or an employee of something else, and then once they have your machine, they have a complete open pipe to the Justice Department's machine. It's not a secure pipe, where there is security, it's actually an open, fully open pipe. That's what a VPN is, it's an encrypted open pipe.

So, those are the three risks. Your machine gets taken over and the FBI comes knocking on your door. Your machine gets broken, and your machine gets taken over and they use that to get to your employer, your employer finds out, he is a very unhappy person. Those are the three main reasons.

MS. GARRISON: Frank, I wondered if you could add to that, and answer the question what can consumers do, technologically, to protect themselves from these threats?

MR. REEDER: There is a risk of being on the last panel at the end of the day, and that is repeating everything you have heard before, but that's just about everything that has been said. So let me avoid saying that, by adding a "me, too," and hit a couple of points.

First -- and here, Andrew, you were very helpful in an earlier panel, in suggesting that we are using "transparency" in two very different ways -- and let me suggest, without going back to Descartes, that, in fact, when we use "transparency" in the sense of something happening without our having to intervene, let's think of that as being passive, as opposed to active security.

And I would argue in the consumer space, for all of the reasons that were discussed on the second panel this morning, the notion of expecting consumers actively to be chief information security officers of their own desk tops or of their home networks, I would argue, is hopelessly naive.

So when we talk about what the consumer can do, the short answer is buy safe products. The barriers to that are, I would argue, twofold.

One is -- and they have both been touched on -- the age of the installed base, the difficulty in doing that for old technology, and second, the complexity of what we're doing with the result that accountability is diffused.

Dean Mark Grady, at George Mason Law School, talks about why tort law won't have the same effect in cyberspace that it has had in other consumer areas, largely because the finger pointing looks like this.

Like Alan, I am delighted to see the ISPs stepping up. I am thrilled, not only because it's based on work that the Center for Internet Security has done, that we are starting to see ISPs, we're starting to see equipment manufacturers like Dell, we're starting to see software vendors make safety security a feature.

I think the simplest thing that we can do -- and I think here the Federal Trade Commission can be enormously helpful -- is begin to identify a set of things that represents safe products, and then validate claims that vendors make that their products are, indeed, safe -- essentially, a truth in advertising role, rather than a regulatory role.

This is not a polemic against teaching safe computing or strong passwords, but I would argue that the notion that such practices will become pervasive in the short run, I think, is -- let me be slightly provocative -- hopelessly naive, which is not to suggest that we shouldn't do it.

It's not obvious to me even that passwords represent a serious threat, because nobody has shown me any data that break-ins into home computers have resulted in any serious losses. The losses occur because of viruses which have nothing to do with secret passwords, or the difficulty of passwords.

So, that's where I think we can be of help to the consumers, by starting to produce, as we are hearing today both from the software vendors, from the hardware vendors, and from the ISPs, safer products and services that are clearly identified to the consumers, so that consumers, in the marketplace, can make those choices with reasonable assurance that the claims being made are as advertised.

MS. GARRISON: Well, your comment about benchmarks I think leads us into the big question for this panel, and Howard, I would like to ask you to initiate the broader discussion.

What mechanisms allow us to achieve the goal of a culture of security, and specifically, how do the adoption of security benchmarks help in this regard? Or, are there additional incentives needed to encourage development of safer computing tools and practices?

MR. SCHMIDT: Well, I think first and foremost, there is a tremendous number of incentives out there. Just from the consumer perspective, we want to enjoy the experience. We want to be able to feel secure in our purchases, we want to be able to feel secure in our research that we're doing online. So there is an incentive for us to learn more.

Now, what are the mechanisms? First and foremost, I think the mechanisms that are in place have been described. The ISPs are not only looking to remove that burden from the consumer space, but they're looking to do it in a rather rapid fashion. So that helps move the culture of security to the backs of those that can better handle it.

The education, training, and awareness component, whether it's the FTC website with Dewey, or Stay Safe Online, or the individual vendors that have security and privacy sites out there. Those are some of the mechanisms that, once again, are just as routine as buckling your seat belt, or making sure you have an airbag in your car as you move forward.

The other thing is this automated process for updating of anti-virus software, personal firewall signatures, those sort of things.

And the last one is just learning about security and privacy, how things work. You know, it's interesting. As I learned how to drive, I learned that the big one was the one that made you go fast, and the short one next to it made you stop. We need to do that more in the online world, and make sure people understand. "Here are the things that will make you go good, and here are the things that will cause problems for you."

MS. GARRISON: Thank you very much. Any other comments from any panelist?

MR. PALLER: I think Rich Lloyd -- since some of you weren't here when the Dell representative was talking -- Rich Lloyd said this morning that they couldn't have done the new system, safer system, if he hadn't had independent benchmarks.

You can't ask every vendor to develop their own standards of what means safety. And so, I think it is the consensus, the government and industry consensus, on what a safe home system is, what a safe workstation is, what a safe web server is, that allows people to deliver them that way, and I think the same thing will happen with ISPs. Determining what a safe ISP service is will allow the ISPs to all get to it really quickly.

MS. GARRISON: Jerry?

MR. LEWIS: Yes, just a quick follow-up on Alan's earlier point, which I agree with completely. Consumers have definitely told us and other ISPs, "We want security, we want privacy," and we have certainly responded.

And you know, the situation he posited about a zombie computer attacking the Defense Department, that's something that draws resources off the Secret Service, or the FBI, and it's certainly something that draws resources off the ISPs.

We have lots of those zombie computers that show up on the abuse team's radar screen, and it's often an old machine with Code Red trying to port scan somebody else, to infect them. It draws a tremendous amount of resources and dollars and time on our part, that we could be spending doing other things to help protect our customers.

And some of it is legacy systems, some of it is just bad consumer behavior, some of it is just completely unknowing consumer behavior -- the kid home from college downloads a lot of files, goes back to school, and the parents are left holding the computer.

So a tremendous amount of resources that goes into that. And part of why we think better security, both at our end and at the consumer end is a good thing, is that it helps us reduce our cost and our expense of dealing with these kinds of issues, and likewise, can help the consumers reduce their frustration.

MS. GARRISON: Jim, just very briefly -- we, unfortunately, are out of time.

MR. HALPERT: I would just add that there is a great diversity of different situations in which consumers and business users access the Internet. And talking about what a safe ISP experience is will vary greatly, depending on whether it's a broadband connection, a dial-up connection, a narrow band, or a proprietary online service, which often has a greater security environment, because all traffic has to go through one place in the network, typically.

And it's very important, as we think about these, that we understand what the security challenges are, and whether the standards are sufficient to meet those challenges.

Also, as we have heard repeatedly, security needs to evolve. And the notion that we can just establish a benchmark and sit on it may actually lead to less security, because security has to be dynamic.

And we need to have a sophisticated understanding when we talk about what these things mean -- and they really are a lot more complicated than just having one single stamp of approval. FTC deception authority, making sure that when vendors are selling products and saying that they are secure, they really are secure, is a very, very important role, and one that ISPs, as purchasers -- really, as middlemen, who simply purchase this technology and pass it along, as you heard from Jerry -- need to depend on, as well.

So, we applaud the FTC's role so far in its security work, and look forward to working with you in the future.

MS. GARRISON: On that note, I am afraid that we have run out of time. And I would like, at this point, to thank the panel very, very much for a fascinating and informative discussion. Obviously, we need to continue this another day.

I would like to introduce Howard Beales, the Director of the Bureau of Consumer Protection, who will make closing remarks.