A F T E R N O O N S E S S I O N

PANEL 3: Current and Emerging Frameworks for Protecting Consumer Information

MS. GARRISON: We appreciate your coming back so promptly. We're sorry we're running just a few minutes late to catch the stragglers.

Once again, I'm Loretta Garrison from the Federal Trade Commission. I'm joined today by James Silver, and we'll be managing panel three.

We're delighted that so many of you could join us for this second half of a two-day workshop on technology for protecting consumer information. We opened our discussions this morning on the business experience, engaging our panelists in some role-playing around a hypothetical business consultant situation. Our equity actors were charged with devising a business plan, then to advise a confederation of retirement communities on privacy and security issues raised by implementing certain technology services for their seniors in their communities. We hope that the issues that were raised in that discussion continue to be amplified as we go through the day.

We also learned about many technological tools that are available to help businesses protect consumers' personal information and we'll be talking more about that

in this panel. In particular, we're going to discuss current and emerging frameworks for protecting consumer information.

As you'll see shortly, there's a wide variety of approaches here.

We have both regulatory and voluntary.

We have very highly technical and also high-level principles.

You'll hear first from each presenter a very brief overview of a particular framework.

Then we're going to move into a broad panel discussion to explore the commonalities among these frameworks, the barriers and incentives to implementing the frameworks, and whether and how we hold businesses accountable for implementing the frameworks.

I'd like to first introduce to you the panel.

From my far right, we have Larry Clinton from the Internet Security Alliance.

Next to him is David Fares, U.S. Council for International Business.

Laura Lundin from BITS, the Technology Group for the Financial Services Roundtable.

And here, even though you can't see him yet, is the one and only Mark MacCarthy from Visa.

Next to James is Fran Maier from TRUSTe, Frank

Reeder from the Center for Internet Security, and Laura Berger, an attorney with the Federal Trade Commission.

Larry, I'd like you to open, please.

MR. CLINTON: Thank you very much.

I have promised Loretta that I will do this in five minutes or less, so if I finish mid-sentence, just let me know.

I'm Larry Clinton with the Internet Security Alliance.

I want to let you know, first of all, who it is that we are.

The Internet Security Alliance was created about six months prior to 9/11 because the folks at the CERT Coordination Center, which, for those of you who don't know, is essentially the fire department for the Internet. They do all the really hard-core, geeky threat vulnerability analysis. They combined with the Electronic Industry Alliance, because CERT was primarily getting this information to the Federal Government, and the private sector, as we know, operates about 90 percent of the Internet.

So, that's what the Internet Security Alliance is supposed to do.

This is a list of our board of directors. A couple of quick comments about that.

We are aggressively international. We are non-NISEC in the sense that we do not operate within domestic cylinders. We are also aggressively inter-sectoral. We have AIG Insurance. We have Visa and Verizon. We have Nortel Networks. We have TATA from India, Sony from Japan, C&W from Britain, et cetera.

This is the Internet. We all recognize this. I remember the Internet when this was first put out in 1980. Everybody thought this was very complicated. How could we possibly deal with that?

This is the Internet today, which is a little bit more difficult to deal with.

Last time I was here, I noted that that really intense purple area is the FTC. I've been told that it is not. Actually, that's my daughter downloading music.

What is interesting here is the trend line. Despite all the attention that we are giving security -- and you've seen a lot of technologies that have gone earlier today -- the trendline for security incidents is straight up through the top. Incidents and vulnerabilities are increasing 500 percent a year.

So, what we are advocating is that we come up with a system.

There is no magic bullet. There is no single technology. You have to have an entire system.

We advocate investing in cyber-security, considering risk mitigation. One of the things that we're going to be talking about today is new initiatives and whether or not the national strategy provides enough of these new initiatives.

One of the things we do with the Internet Security Alliance is we have a deal with AIG Insurance, the largest provider of cyber-insurance. If you become a member of the Internet Security Alliance and subscribe to our best practices, we will lower your insurance rates 15 percent.

We are trying to provide a market-based incentive program.

Mark MacCarthy is one of our members at Visa. Visa has a similar program. If you want to use a Visa card, swipe a Visa card in a store, you have to have a certain level of security.

What we're trying to do is come up with market-based incentives, because the traditional regulatory models won't work.

You can't use an FCC-style model where we're telling everybody in public comment what's around. You're then providing a road map for all of the nefarious people. You can't come up with a three-year program to provide regulatory structure, because by the end of it,

the Internet's entirely changed. If you do it in the United States, it doesn't help you internationally. We need a new model.

We also think that people need to become involved in the policy debate so that we can consider this.

We also strongly advocate the adoption of best practices, and we have a list of them that I'll provide you in a moment.

These have been endorsed by TechNet, U.S.-India Business Council.

We are trying to export these.

We, frankly, don't need to write more new best practices right now.

What we need to do is start implementing them, and we strongly advocate joining an information-sharing organization. Only if the information is shared between operators of the Internet and the vendors are we going to get anyplace.

The Internet Security Alliance operates with the CERT data.

We put out these best practices. We attempt to get people involved in them, and then we provide economic incentives if they will adopt them.

Here is a list of the best practices. They're

available on our website. I also have hard copies available, if people want to look at them here today. Here is what we go through in terms of our education and training.

Again, we try to provide at discounted rates the best possible training coming out of the CERT Coordination Center.

Not only do you need to have a policy, not only do you need to have practices, not only do you need to have technology, you need to have things that are going to make sure that people use the technology.

The comments made before about the wooden doorstop in the previous panel I thought were very excellent. That's exactly what we have.

It's irrelevant if you have a great password technology and everybody is still sticking their password on their computer so they can remember it. We need training for everybody.

This is a copy of the special communications that we provide through the CERT Coordination Center.

For time purposes, I won't go through it any further.

Again, if anybody has any questions for me, please contact us.

Our role is to try to expand the security

perimeter in a market-based fashion, and we're looking forward to and very grateful for the help that we've had with the FTC.

Thank you.

MS. GARRISON: Thank you very much, Larry.

David.

MR. FARES: Thank you.

I'm just going to remain seated. Can everyone hear me?

Okay. I'm going to focus my initial remarks today on the work of the Organization for Economic Cooperation and Development, which is a grouping of the 30 most industrialized economies in the world. The organization is located in Paris.

My organization, the U.S. Council for International Business, is the U.S. affiliate of the business and industry advisory committee, which is the constitutionally chartered voice of business in the OECD.

The OECD recently issued a revised set of security guidelines.

The guidelines were initially adopted in 1992 when systems were largely closed.

They realized, in the built-in review process, which is scheduled for every five years, that they probably needed to be updated to take into consideration

the shift from closed networks to open networks.

Luckily for me, the OECD guidelines and our work is not highly technical, because I'm not a techie.

So, I'm able to meaningfully participate in the work that we do.

But the OECD guidelines coined the phrase "promoting a culture of security." The person that asked the last question before the end of the last panel was talking about the fact that consumers don't know enough about security and that we need common-sense security.

That's exactly what the OECD guidelines attempt to address.

In very simple, plain language, it states that every participant in the information society has to assume a role appropriate to them to promote security. Awareness of security issues and responsibility are elements of the OECD security guidelines.

So I would recommend that all of you take a look at the OECD guidelines. As I said, it's not a technical document but, rather, a document that frames how every participant should analyze what their responsibilities are and what their engagement should be in promoting a culture of security.

You can access the guidelines at www.oecd.org.

We are working to help promote business

implementation of those guidelines.

To that end, we held a workshop in conjunction with the FTC where Commissioner Swindle spoke, inviting cross-sectoral industry associations to promote a culture of security with their members, and we were lucky enough to have Larry participate in that workshop.

We are also expanding upon the OECD guidelines.

We are developing BIAC, along with the International Chamber of Commerce of which we're also the U.S. affiliate. We are developing a business checklist, a business commentary on the type of questions that executives should be asking their IT department, so that there is top-level support, as well as bottom-up approaches to security.

And then, a next stage of our work will be to develop a checklist for small and medium-size enterprises and companies in the developing world. Again, it's not going to be a set of best practices but a series of questions that these types of companies should be asking themselves when they're developing their security policy.

We also have on our website links to many different resources for security that businesses can utilize.

We have a link to the Internet Security Alliance's documents and to other documents, and our

website is www.uscib.org.

And with that, I will stop.

I've left some information in the back for you which gives a summary of our draft business commentary. It should be concluded by the end of this summer, and at that point, it will be accessible from our website. I won't bother giving you the ICC and BIAC websites. It's in the document on the back table.

Thank you, Loretta.

MS. GARRISON: Thank you very much, David, and I hope that all of you in the audience have checked out the materials that we do have on the table, because there's a lot of additional resource material for you.

Laura Lundin.

MS. LUNDIN: Thank you. Thank you, Loretta.

I am with an organization called BITS. BITS, for those that don't know, is the technology arm for the Financial Services Roundtable.

We are a business and technology strategy group, working on a variety of issues for the financial services industry.

Our primary membership is the 100 largest financial institutions in the U.S.

As you might imagine, this group is very sophisticated when it comes to information security, and

it's often thought of as leaders in this area.

Part of that is driven by the regulatory environment in which we operate.

However, the two frameworks that I want to bring to the table today are some things that the industry has worked on through BITS, and it really addresses the products and the services that are used by the industry. The industry realizes that, as strong as its policies and its procedures and the technologies that it uses in the information security world are, it doesn't stop there.

It has to go beyond its boundaries, and it really depends on the vendors and the products and the services that it uses.

On the products side, we have started a product certification program.

This program is three-plus years in the making. We have corralled the industry to develop consensus-based minimum security features that it is going to look for in the products that it buys.

Most recently, we've harmonized this program with the government's common criteria certification program. So, now a vendor going through the common criteria certification effort can also meet the requirements that the financial services industry has set

forth.

On the services side, we have developed a framework for technology risk management of service providers. Out-sourcing is being used more and more in every industry, including the financial services industry. What we've found is there has to be, again, a common set of security policies and procedures that are followed by the providers of the services to the industry.

Our framework addresses security from everything from the decision to out-source to the RFP process, the contracting, the insurance process, ongoing management relationships.

That framework is currently being updated right now to address some specific issues around security assessments, the more specific issues dealing with cross-border out-sourcing, out-sourcing to international organizations, as well as some additional measures around business continuity. Of course, this framework actually came out just around the 9/11 time-frame, but now that's obviously an area that has to go back and be revisited.

Both frameworks, the requirements that create both of these programs, can be found on the BITS website. They are public documents.

The web site is www.bitsinfo.org.

I also have a one-page hand-out outside that specifically talks about the production certification side of the house.

MS. GARRISON: Good. Thank you very much, Laura.

Mark.

MR. MacCARTHY: Thanks very much.

Let me tell you a little bit about the Visa card-holder information security program.

In the first instance, these are a series of requirements that have been developed for Internet merchants and processors, but it's important to remember that they've been a requirement of the Visa system for a long time -- that those who handle card-holder information do so in a secure fashion. A couple of years ago, we made those requirements more specific through the card-holder information security program, initially for the Internet. I want to tell you a little bit about why we started with the Internet.

Basically, it's because it's a new channel, there are new risks, and there's some brand issues related to the use of Visa cards on the Internet. But it's also important to remember that CISP, the card-holder information security program, is moving beyond the Internet.

It applies now to all entities who touch Visa card-holder information, and eventually, CISP is going to apply to all payment channels, not just to the Internet. But we started with the Internet because it was a new channel for Visa.

It's a growing part of our overall electronic commerce.

It is 6 percent, almost 7 percent, in 2002, of our overall sales.

It's up from 4 percent in 2001 and 2 percent in 2000, and payment cards are used to make most of the sales on the Internet.

Check and cash in the real world account for abut 60, 62 percent of all sales. They're not a very useful method of payment on the Internet.

So, Visa gets a substantial portion of the sales on the Internet.

It's an important new channel of commerce for us.

There are new risks associated with the Internet. There's a perception that the Internet is not a secure place to shop.

Ninety-two percent of consumers are concerned about online security. Sixty-three percent of them are very concerned.

And the reality is that many online merchants retain card-holder data in a way that's accessible from the Internet.

Fraud, as many of you know, is higher on the Internet.

So, there are new risks associated with that new channel of commerce, and that created some brand perception problems for Visa. We did not want the perception to be created that Visa was not a secure method of payment.

For those reasons, we decided to move ahead with this card-holder information security program.

For those of you who want to find out more of the details, there's a packet that I've left at the information table that will give you a lot of the specifications in more detail, but the CISP program starts with 12 basic security requirements.

We developed these in conjunction with the security experts and with the merchant community. They've been effective since May of 2001.

Let me just give you a flavor of what they are. They're very high-level.

Install and maintain working firewalls, keep security patches up to date, protect stored data, encrypt data when you're sending them across public networks, and

use and update anti-virus software.

We've also developed an audit program to make sure that people who are subject to the CISP program actually are complying with it.

We've created a defined and consistent testing procedure for independent validation of these requirements. We have a list of 30 acceptable independent security assessors.

For the top hundred merchants that account for about 70 percent of all of Visa's Internet volume and for various service providers that provide service to Internet merchants, there's an annual on-site independent validation that has to take place.

For smaller merchants, there's a web-based suite of tools that they can use that will give them an online risk assessment, a self-assessment, and they go through online vulnerability scans.

Our enforcement mechanism -- there are penalties for failure to comply.

Of course, there's a period of time where we're trying to move merchants into more and more compliance. We provide them with help on remediation efforts, but there are substantial fines that can be pretty dramatic for particular companies in the case of egregious failures to comply. Penalties can include expulsion from

the Visa system.

The advantages for companies in complying with this -- obviously, failure to provide adequate online security is a business risk. For some, it can be fatal.

But beyond that, there's an insurance discount. For those merchants or entities that hold Visa information and that are compliant with CISP, some insurance companies like AIG will provide a discounted premium for cyber-insurance.

How are we doing? Virtually all of the top hundred companies are in compliance today. The smaller merchants are coming along well, as well.

We're expanding the enforcement to include third-party service providers, processors, web hosting companies, and so on.

It's going to take us months to really roll out that new enforcement mechanism, but the end result -- and let me conclude with this -- the end result is that if third parties are not CISP-compliant, they will not be allowed to touch Visa card-holder data. That's going to be the ultimate way this program is going to be put into place.

MS. GARRISON: Thank you very much, Mark.

I'd like to turn to Fran Maier.

Go ahead.

MS. MAIER: Thank you, Loretta.

Many of you know that TRUSTe is the leading online certification and seal program on the Internet. Our primary purview is over privacy. Of course, privacy does include and require security, and we have some guidelines along those lines, as well.

Our consumer position is about giving consumers choice. Our tag line is "Make privacy your choice," and there's two aspects to that. One is actually providing the means for consumers to have choice about the sharing of the personal identity and information, and also telling the consumer that they've got to take an active role in ensuring that they protect their privacy and don't give it away.

Our mission, then, is to enable trusting relationships between organizations and individuals based on respect for personal identifying information.

We have a set of core privacy principles outlined in our program requirements and in our license agreement. All of the 1,200 to 2,000 companies who join the TRUSTe program have got to abide by and agree to those programs, those principles, and they follow along with the FTC fair information practices.

So, for example, under notice, they have to have a privacy statement, and it has to have the TRUSTEe

seal on it.

They have to say how they collect information, who they share it with, under what circumstances it might be shared.

They've got to talk about cookies, beacons, and other kinds of things.

They have to say how they will notify users of a change in the privacy policy and a range of other notice requirements.

There's choice requirements, and probably the significant point there is that if you're going to have sharing for secondary purposes or with third parties, you have to provide user choice, at least an opt-out.

There's access requirements in terms of giving the consumer an opportunity to correct, to change their preferences, for example.

There's security requirements, and right now they're fairly basic. We're looking forward to working with industry and some of the players here today to try and provide some guidelines to our licensees about the best security.

The simple things that we ask for now are that things like credit cards be under an SSL, that there's password protection for personal identifying information, and so on. We're working now to develop some more robust

guidelines in response to what we're seeing all around us in terms of the need for security.

In addition, companies have to enter into a license agreement with us, pay us some substantial funds, especially if they're large, agree to undergo monitoring, as well as dispute resolution processes, and agree to the termination requirements that we have.

And I'll tell you, we recently figured out about 10 to 15 percent of the companies who apply to TRUSTe and fill out their self-assessment and their license agreement and give us a check -- 10 to 15 percent do not make it through the process. For the most part, it's because we find that they have issues with implementation of the choice requirements or they have issues related to the children's online privacy protection requirements. That's a fairly substantial number. Of course, if they don't come into compliance, they're not available to be renewed, and of course, they don't get the seal.

And I just want to speak quickly about how we monitor. There's been a lot of questions about this over the years.

First of all, we do have dispute resolution services. This year we're tracking close to 5,000 consumer complaints now.

Some of those don't have to do with privacy, per se, but they do look to TRUSTe to put in a complaint.

We've worked with Watchfire. We're working with Watchfire now.

We've scanned about 300 of our sites.

We just started this early in the year. We're looking for things like placement of the TRUSTe seal, whether or not they're collecting cookies, if they've changed their privacy statement, all kinds of things that give us and our compliance team a chance to have a second look. We have found that 57 percent of the companies have passed, which obviously means 43 percent have failed at our first review, and some of these are not egregious problems.

Some of them are just a matter of simple fixes, and we're getting good response to that, and I think it's good for everybody.

We also do a fair bit of seeding, where we join websites, provide information, and we also go to the press and FTC, potentially.

And so, again, in the future, we want to work on the security guidelines. We're looking at a lot of activities and best practices around e-mail, and we're looking at more and more technology to apply to this area, because Watchfire has made us much more efficient,

much more effective in monitoring. We think that there are other technologies, even some that we've implemented ourselves, that are proving to be both efficient, effective and strong, and that's where we're going.

MS. GARRISON: Thank you, Fran.

Frank.

MR. REEDER: We have been told that we will have a hammer thrown at us if we are not finished in five minutes.

MS. GARRISON: Or a water pitcher.

MR. REEDER: Or a water pitcher.

I guess I would like to start by asking you a question, picking up on something that came up in the previous panel. How many of you, if you're buying technology, are interested in buying technology that has all kinds of back doors and means of access, some of which you don't know about?

I don't see any hands. Well, that, in a nutshell, explains why the Center for Internet Security came about. About two-and-a-half years ago -- I guess we're all in the same time-frame -- we convened a bunch of folks to address that set of issues, and out of that came a concept, based on a couple of very simple premises:

One, that most of the damage being done,

according to the industry watchers, people like Gartner, was being done exploiting vulnerabilities -- technology vendors refer to them as features -- that were known to exist and for which the remedies were widely known.

So, the problem here was not that we needed to do new research. The problem here was more of an information dissemination problem.

And the problem, really, as we saw it, had two distinct dimensions. One was -- and here I steal the wonderful phrase that Toby Levin taught me some months ago -- we needed vendors to begin to build security into their products, what Toby refers to as baked-in security. But even that isn't going to be sufficient, because most of us operate technology that is from six months to three to four years old, and data actually show that we're keeping it longer than we were even as much as two years ago.

So, we have an increasing problem with a large installed base of vulnerable technology.

The Center decided to focus on the technical detail. That is not to suggest that policies aren't important. That is not to suggest that user training is not important.

But relying on those alone is like telling people that we're delivering them cars with the brakes

disabled, but they should drive defensively.

Safe computing practices are important but simply not sufficient.

The Center's dirty little secret is it is not five lab technicians in Iowa.

It is a virtual network of high-end practitioners who start with common knowledge about a particular technology -- we started first with operating systems and have moved now into market-dominant technologies in other sectors.

We have benchmarks now for a CISCO router. We're about to release one for Oracle, and for other technologies that are actually out there in use. The Center produces these benchmarks. They're available free of charge on its website.

But even more importantly, the Center produces measurement tools, non-intrusive software that actually tells you the extent to which your systems are not hardened, and you can use those on a continuing basis.

What's really even more exciting for us, to steal a British phrase, is our measure of success is not product produced.

Our measure of success is take-up rate. It's changes in behavior in the real world. And several exciting things have happened, some of which you've heard

about here today.

Microsoft is beginning to produce a Center benchmark-compliant version of its newer operating systems.

Dell -- I'm going to actually take a tape of Craig Lowery's presentation this morning and send it out in lieu of any future public speaking that I do. Dell told you what they were doing. That, for us, is success.

Visa links to the Center's benchmarks in its top 12.

Our success is not in having consumers or even small businesses know about the Center but, rather, about having technology that is Center benchmark-compliant delivered to them in much the way that the questioner in this morning's session asked about how we do security so that it is transparent to the user, transparent in the sense of passive, doesn't require any active intervention.

We also have been working with the major vendors of security software.

Again, while we provide the Center's tools on our website free of charge, the typical computer user is not going to search out the Center for Internet Security but may buy tools from vendors like Symantec or Net IQ or BindView, all of which are now building the Center's

benchmarks into their security suites.

Again, take-up rate is important for us, and that's a way of penetrating the market.

The Center's website does tell you far more cogently than I have what we're about and who we are, and it gives you direct access to all the products I've described. The URL is www.cisecurity -- no punctuation -- dot-org.

MS. GARRISON: Thank you very much, Frank.

Laura Berger.

MS. BERGER: Good afternoon, everyone.

The FTC has been very active in the area of security, and I'm just here to tell you about some of the latest things that we've been working on. One of those is the FTC's Safeguards Rule under Gramm-Leach-Bliley, which took effect on Friday, May 23rd. We've been talking about, as Mark MacCarthy said, fairly high-level security standards. The Safeguards Rule, for those of you who want to see it or have had a chance to look at it, is on our website at FTC.gov and accessible under our brand new privacy initiative website that's newly revamped.

It is very high-level. It applies not just to a specific Internet site or a specific type of business context but to a specific type of institution, financial

institutions.

I won't get into describing exactly every kind of entity that fits under that rubric. People who have had experience dealing with Gramm-Leach-Bliley and the private notices and Privacy Rule are probably fairly familiar with it. But it's a very diverse range of businesses and entities, from very large and sophisticated entities to very small, even sole proprietorships that engage in financial activities.

It's not just about addressing Internet business but also about addressing physical storage of records and how employees handle records and what CEO's tell their IT people. It's very broad, very high-level, and it has two parts to it that I'll first just touch on very, very briefly. Then I'll talk briefly about our outreach.

The Safeguard’s Rule has a reasonableness standard for what the overall security of a financial institution has to accomplish. That standard also embodies required elements, and I won't go over all of those here, because there are five of them, and I think that would exceed the five-minute time limit if I did.

But they're high-level. For example, one of the elements is assessing risks to the security of customer information.

It's up to companies to really unpack that and figure out what they need to do to assess the risks that face their organization and the customer information they're maintaining.

What are we doing to help businesses address this new challenge? A lot right now. We're doing a lot of outreach to try to alert businesses that may not be aware of the new requirements and the way that they apply to their business.

One of the things we're doing that you can pass along to people is I will be conducting, along with another staff attorney, Ellen Finn, on June 9th and June 23rd, one-hour training sessions.

There will be dial-in instructions for participation in those training sessions posted on the FTC's website at least the day before the training sessions, and people can also come here to conference room A in this building on those two days, according to the times posted on the website.

That's our most public outreach, but we're also just handling a lot of industry queries and working with a lot of industry groups to help them apply the standard to their particular industry and their types of circumstances.

The standard which I mentioned -- referred to

as a reasonableness standard -- specifies that what's going to be reasonable will vary according to the size and complexity of the business, the nature and scope of its activities, and the sensitivity of information. A lot of entities have wanted to talk to us about, what do you really mean by that and how does that really work. Of course, we can't give definitive answers, but we've been working hard to talk these things through and help industries get their own analysis onto their websites and into their newsletters, and we'll continue to do that kind of work.

With that, I think I will turn this back over for general discussion.

MS. GARRISON: Thank you very much, Laura.

The frameworks or the approaches that we've just heard very briefly discussed, as you can see, are quite varied.

Some of them are mandatory, either by statutory requirement or by membership requirement. Others are voluntary.

Some are very high-level. Others are quite technical.

Frank, as you think about this, do you find any common features or core principles among these frameworks, and what role does technology play here?

MR. REEDER: On the latter question, I have a bias, but I'll save that for last.

On the former, it's actually wonderful to hear -- it may be boring for the audience -- a fair amount of harmony around this table.

What I've been hearing -- and I think this is a growing chorus -- is we're all trying to identify, through some sort of a process, what I would call consensus best practices.

This is less, I would argue, except at the very high-end, a matter of invention as it is a matter of information-sharing.

Much of what is going on relies on, to some degree, some fairly detailed technical work.

Fran made mention of the fact that they're working on the assurance side.

The third trend I see is an increasing reliance -- and this came through in other panels and in Toby's nice phrase, baked-in security -- making security more a part of the product offering.

And I think related to that -- and here, I think both TRUSTe and Visa are teaching us about the importance of branding -- ultimately the consumer and the small business, the entities that don't have the capacity to make complex technical judgements, rely on cues in the

marketplace that tell them or give them reasonable assurance that a product or a service is, in fact, safe from their perspective. We're starting to see a lot of push in that direction, and ultimately that gets to the point that several of the folks on the panel made.

This ultimately has to be market-driven. But it's not going to be market-driven based on individuals looking at the technical pieces of security and privacy but, rather, some more general set of assurance backed up by some of the organizations around this table and, ultimately, the threat of enforcement from the Federal Trade Commission if they make claims that are un-substantiable. In other words, when they see a brand or a mark that says you can expect this level of assurance and this level of protection, indeed that is a valid claim.

MS. GARRISON: Larry, what core commonalities do you see from your perspective?

MR. CLINTON: I was just thinking about it. I think I see four kinds of commonalities.

The four that I see are systemic, cooperative, creative, and ongoing.

There seems to be a consensus that technology is not the answer, training is not the answer, insurance is not the answer, international cooperation -- they're

all the answer. It has to be a systematized approach.

In the same sense, everybody seems to be interested in learning from each other.

Oh, that's a good idea Visa has. Nortel is going to try to apply that to its vendors.

Oh, that's a good idea AIG has for Visa or ISA, maybe we can bring this into other things.

So, there's an attempt to cooperate here which I think is indicative of what the Internet is. It began, really, as a collaborative element.

There's creativity going on, the recognition that maybe the old paradigm for regulation, if you will, that was built off the industrial revolution and, frankly, static technologies -- automobiles, for example -- which were good, but you need to have a new paradigm, because the Internet is itself a new thing.

Individuals are much more involved. It's ongoing. It's changing. So, we need to be ongoing and changing, also, and that's the last piece, is that it's ongoing.

Nobody at the table is saying okay, I got it, now we can move on to Internet 2. Nobody is saying this is what we've done.

Everybody's saying, well, this is what we're doing, and we're listening to everybody else, and we're

delighted to be here and we have to constantly move forward.

So, I think those are four macro things that I'm seeing that I think are all very positive.

MS. GARRISON: That's good.

Fran, you look at this from a privacy perspective. An awful lot of this conversation is about security. As Frank and Larry and the others here see commonalities on the security side, do you see common or core privacy principles emerging?

MS. MAIER: Yes. I think almost everybody has adopted, to some degree or another, the fair information practices, and I think that that framework has been a very powerful framework under which to develop specific privacy policies and programs.

Now, there's a lot of debate. There's debate over what is adequate choice. Should it always be opt-in and opt-out, how best to monitor for some of these things, what really is notice, and there's not only the base, there's activities, like the short notice program and the P3P program and others that try to bring more of these notice things up to the forefront.

To the point that Larry made, there's a lot of, again, creativity, there's a lot of activity. I know that, for TRUSTe, we're working right now on TRUSTe

license agreement 9.0. We've been around about nine years, and that really speaks to the fact that, every year, there are more things that come up, either because consumers are bringing them up or because technology has changed, or some combination.

So, for example, in 1997, I don't think we talked about web beacons or perhaps cookies, but clearly, that's been in the license agreement for a long time.

I anticipate, in this next agreement, we will talk more about security and e-mail best practices, because right now, for a lot of reasons, those two things are coming up, and I think that evolution talks about that. You can sit here and talk about what is the best practice and where it's going to go. Sometimes you have to start a little lower than maybe you'd like, but over time, you're probably going to get to the place that you really need to get to in terms of consumer protection. That whole idea of the process being ongoing and evolving is an important concept to keep in mind.

MS. GARRISON: I think that's true.

David, can you tell us or summarize what you think has been the progress in the last year in adopting these various frameworks, and do you see any new frameworks that are under development or that are emerging?

MR. FARES: Well, I will begin by expanding upon the progress that I've seen in implementing the OECD security guidelines. By the way, I forgot to mention at the outset that they are voluntary guidelines, but the OECD governments have been working to implement those guidelines. The U.S. Government and the FTC have an active work program in that regard.

The OECD will hold a workshop in November, in Oslo, to continue to raise awareness about the need for all participants to promote a culture of security.

I already mentioned what the international business community is doing to raise awareness through the efforts of the International Chamber of Commerce and the Business and Industry Advisory Committee, but the OECD guideline process has spurred other inter-governmental organizations to also begin to look at how they can start creating awareness for the need to promote a culture of security.

The U.N. General Assembly basically adopted the OECD guidelines in January 2003. The Asia Pacific Economic Cooperation also has a program to promote awareness on cyber-security, and the EU is basically creating an information-sharing mechanism.

There are also a whole host of private sector initiatives apart from the OECD guideline process. The

International Chamber of Commerce has a cyber-crime unit where it attempts to track security incidents and provide guidance to businesses and law enforcement agencies about trends.

There are the ISAC, CERT, SANS. There's a whole host of private sector organizations that are trying to create awareness and information-sharing so that people can better respond to security incidents. As we work toward implementing these frameworks, Loretta, creating awareness is one of the most important things, because there are a whole host of resources that exist. Resources will continue to be developed, but we need to create, in the mind-set of all participants, that they need to engage, that they need to be a part of the solution, and I see a lot of progress in that regard.

I think we're in the stage today where we were probably in 1998 in the privacy debate, Fran, when people just started to pay attention to privacy and really put it on the agenda for all participants, whether it is consumers exercising their choice, or whether it is businesses promoting and adopting and posting their privacy policies.

We've seen significant progress in the privacy debate with corporate policies being posted online, with organizations like TRUSTe and BBB OnLine. So, I am

confident that we're going to continue to make progress, and this awareness-raising exercise is really going to be helpful, and it is going to produce success.

MS. GARRISON: Frank, from your perspective?

MR. REEDER: Well, I think there's been enormous progress, as I said, in take-up rate, but I'd like to focus on one aspect of your question. That is are new frameworks developing.

There are risks in relating cyber-developments to the physical world, but some of those comparisons are valid. I think if we look at other areas of risk or consumer safety, something very exciting has happened in the last year in the cyber-world that happened perhaps 30 years ago in the automotive world. That is, rather than viewing security or safety as a cost, as the manufacturers were telling us when they said they couldn't afford to put air bags in cars, we see companies beginning to sell safety and security as a feature, whether it's the branding of a service, like Visa is doing, the TRUSTe mark, or Dell's announcement that you can now buy a securely configured technology at a nominal additional charge. It's a vision I've had for a long time.

The Mercedes and the Volvos in the cyber-world are beginning to emerge, and that, in turn, I would

argue, just as it did in other areas, will begin to drive practice. The reality is, in the physical world, very often, then regulation follows when the dominant practice becomes something that it is unreasonable to allow others to ignore, rather than using regulation as a way of driving practice.

So, I think there has been, in my view, a significant shift in the last 12 months that is very exciting and I think should dramatically accelerate the use of privacy and security technologies.

MS. GARRISON: Fran, do you see the same thing from the privacy perspective? David alluded to it a few moments ago, saying that we're now at the stage in security where we were with privacy four years ago.

MS. MAIER: You know, I think there is some good news and some not-so-good news.

In terms of online privacy, I think the adoption of privacy statements is almost ubiquitous, especially among the larger companies -- you'll see it in probably the top 500 -- and it's almost a requirement. Everybody thinks about having a privacy statement.

However, enterprise privacy, software privacy, product-related privacy -- the fair information practice frameworks still work, but implementation of consistency in those areas plus the ability to monitor and audit and

so on has not quite emerged yet. I think it will emerge, because I think, actually, the whole effort to get security under control, which is a requirement for privacy, is driving an effort within industry to take a look at their own enterprise data flows, their own enterprise security programs and so on. Once that's in place, then hopefully the question of privacy comes up.

It is interesting. I had dinner with somebody last night who was attending the Gartner security conference, which I think is going on here in D.C. this week. The conference didn't have anything on privacy, and it struck all of us -- the couple who I was talking with -- as that's not really up to date. Hopefully they'll change that, because I think the privacy question goes along with the security question.

MS. GARRISON: We've heard different terms used -- standards, frameworks, benchmarks.

Frank, you've, of course, alluded several times to the adoption of the CIS benchmarks, but can you talk briefly about benchmarks, perhaps what they are, as distinguished from frameworks or standards? Are they helpful? If so, why?

MR. REEDER: Well, the penultimate question is easy. Of course they're helpful.

We have deliberately adopted the use of the

word "benchmark" because of the baggage associated with the use of the word "standards," although I was delighted to hear on a previous panel that some in the industry are increasingly welcoming standards at this point.

The benchmarks are, in fact, for the technologies for which we developed them, hardening scripts. They're essentially a set of specifications on how a piece of software or piece of technology ought to be configured so as to eliminate known vulnerabilities.

They are highly technical documents. I will confess, as I think a previous panelist did, I cannot read a CIS benchmark and make heads or tails of it except at a fairly conceptual level.

The companion piece, of course, is a piece of software that then measures the degree to which the way your software is configured matches those.

Are they of value? The simplest metric I have -- and this is an independent measure -- is that out of the box, the technology that is generally delivered to users is highly susceptible to attack, based on studies that NSA and others have done. When the technology is hardened to comply with the Center's benchmarks, for all of the known attacks that we have seen spread around the world in the last 18 months, essentially adoption of the benchmarks would render the user of the benchmark immune

from those attacks.

But the simple measure of success is does it afford you protection? Absolute protection, certainly not, but for protection against the prevailing threats that we know of, we have a very high degree of assurance based on independent examinations that have been done by others, not just by the Center.

MS. GARRISON: Are the benchmarks at level one that the CIS has available -- are they something that just the ordinary consumer can actually do, or do they really require a lot more technical expertise to install?

MR. REEDER: I think an individual who fancies him or herself as an expert user could certainly adopt them, but I think we encourage folks to use other products that do that.

That's one of the difficulties that we are encountering in getting adoption at the consumer level, and that's why we're placing so much emphasis and we're so delighted to see products being delivered that are already configured. Certainly, the typical system administrator, even if he or she is just a part-time systems administrator in a small enterprise, can implement them.

MS. GARRISON: Okay.

MR. REEDER: But whether our aging parents or

uncles and aunts could, I doubt that they would.

MS. GARRISON: I was thinking more of someone who's technically challenged like me.

MR. REEDER: We'll send someone over to help you.

MS. GARRISON: Thank you.

Larry, I'd like to move to a discussion about barriers to businesses in adopting these frameworks. Can you begin the discussion?

MR. CLINTON: Yes.

I think we've all said there's a lot of progress being made, and that's great. That's a good news, bad news situation.

A lot of people say, oh, well, there's a lot of progress being made, it's not so much front page now, well let's move on to other things. That's a problem. Success can sometimes breed over-confidence, and we really have to watch out for that.

A second major problem is that, despite the creativity we have spoken about previously, a lot of corporations still view security as a cost center, not an opportunity. There are some exceptions out there, and they should be highlighted, but still, the typical investment in cyber-security is probably not what it should be, particularly the ongoing operation of things.

We've already discussed how important that is. It is something that is a problem.

People are putting in security systems, but they are not checking up on them, not updating them, not updating their training, not enforcing the procedures that they have.

There are also some market-based problems with some competitiveness, notwithstanding a lot of cooperation we're seeing.

There are a number of people who are saying that the information sharing that we believe is critical is being impeded because there's a resistance to communicating with your competitor about the problems that you have. A lot of the structures that we have are, frankly, built on the former economic model.

We started building ISACS following PDD63. We said okay, let's put all the technology guys together and all the financial services guys together. Financial service has been one of the most successful of these, but still, we've got everybody in the old silos that now we all kind of dismiss as archaic, but those are still the structures that we're working with. We think we probably need some new structures that are across industry, international, more cooperative, and I think we can still do a lot of work developing incentives.

We at the Internet Security Alliance, supported the National Strategy to Secure Cyberspace, but I don't think that the plan is perfect.

I don't think it speaks adequately to how we're going to have private sector incentives. I don't think it speaks adequately to how we're going to create good data upon which we can build an awful lot of cost-benefit models, et cetera, and these are the things that industry is going to look at.

So, I think we've got a ton of work still in front of us. We've got a number of barriers -- cultural, economic, and structural -- that need still to be broken down, but I don't want to diminish the work that's being done.

MS. GARRISON: What about the issue of corporate support?

I know that we've read some general reports about investments by corporations in their IT programs, and of the IT funds, actually it's a fairly small percentage that, on average, goes to security itself. Is that a pervasive problem?

MR. CLINTON: Well, the first principle that we have in our five principles is investing more in security. So, we think that it's certainly a problem.

One of the problems with it, which I just

alluded to, perhaps not as cleanly as I should have, is that the data for what counts as security investment is pretty loose. Are we counting training in that, or is it just IT technologies, is it software, et cetera? So, it's kind of hard to really tell, even in some of the better studies, what the measurement is.

I think we need some better models, starting at the academic level, for that. But to get to your point, yes, investment is still a problem. IT investment is a problem now, and we still see that in the IT sector of the economy, and the security portion of the IT portion is a problem.

Another problem is the degree of commitment that senior management has to security -- boards of directors, CEO's, and the like.

A lot of this still resides with the CIO, not the CEO and not even the chief security officer. It's the chief information officer.

I think we have to broaden the perspective of security so that security becomes part of the operation of the corporation just the same way payroll is an operation of the corporation, management is an operation, human resources.

These are things that everybody in the organization needs to be focused on. That's our first

best practice, and the first is geared to getting to senior management.

I don't think we have crossed that barrier yet. I think there are a lot of people interested. We're working with Technet on that. They're going to have a big program coming out.

There are a lot of people working on this, but that's not to say we're there yet.

MS. GARRISON: David, do you see any barriers from your perspective?

MR. FARES: Yes. I'll just expand a little bit on what Larry said, and then I will move to a different focus. But, as I said, there's been a lot of work on awareness raising. That work on awareness raising is beginning to create an understanding within the business community that security is a business enabler and not a business cost. As we move toward that as a broader understanding within the business community, where I think we're making significant progress, I think one of the major barriers will come down.

We've been spending a lot of time talking about IT expenditures, but IT expenditures is only one small element of a security policy, as many others have discussed. Training. Security is a process, and we need to make sure that all participants understand that they

have to not just attempt to adopt a quick fix, but they need to implement a security policy that includes reassessment, that includes training, that's ongoing and continuous. Finally, I've alluded to it several times, but I think that many other participants feel as though security is simply a business issue.

It's not just a business issue. Everyone has to work to enhance security, whether it is a consumer, government, a network operator. Everyone has to work as an awareness raising organization.

I think there needs to just be a broader understanding, consistent with the OECD guidelines, that everyone has a role to play, and it's not just one participant's responsibility. Once we're successful in that, I think we will also overcome a lot of the barriers.

MS. GARRISON: Laura, you work with a whole industry that, in fact, is under a regulatory regime to implement security measures. What is your experience as to the barriers that may be impeding the adoption of frameworks in this area?

MS. LUNDIN: Well, I have a couple of comments.

First of all, I echo a lot of what has been said amongst the panelists about the necessary change in culture needed on behalf of the product manufacturers and

the service providers to actually build in that security and the need to value security as much as the business functionality that comes in a product or the processing capabilities on behalf of a service provider.

So, I think the need to value security is still a primary impediment to adoption of some of these frameworks.

On the other hand, it's also very difficult, I guess taking the stance from an organization that tries to create these frameworks, to strike a balance. You try and be high-level enough so that it is a flexible framework. You can't be too prescriptive within the context of risk management.

Various situations are going to require different types and levels of risk management. So, you have to account for that, and you have to maintain that flexibility within your frameworks.

On the other hand, if you get to too high a level, people don't have that understanding, and there's certainly a learning curve.

A lot of the regulatory regime that's come down on behalf of the financial regulators was very broad-brush. It's taken several rounds of examinations for these organizations to really figure out the intent and the level to which the regulations come down and then, in

turn, how they pass that along to their service providers or their product manufacturers.

So, again, trying to strike that balance is a real challenge.

MS. GARRISON: Frank, what about small businesses? Are there special challenges here?

MR. REEDER: Absolutely. I think one needs to make an important distinction between large enterprises and small enterprises, which in many ways behave more like individual consumers, at least in the information technology marketplace, where it's not reasonable to expect that there is technical critical mass within the organization.

It's probably the youngest person in the organization who gets you out of trouble when something goes wrong, but there again, the small business is more reliant on buying safer products.

Certainly, education can help with respect to management practices, but there's one other actor we haven't talked about in this conversation, and that would be the service provider, the VPN provider or ISP. There, again, we need to look to that sector to build more security and privacy technology into the offerings that they provide, simply because it's not reasonable to expect individual consumers or small businesses, apart

from the cost question, simply to spend the energy. It's not a question of being smart enough but of being able to spend the energy to make the technical judgements that they have to make.

MS. GARRISON: Laura Berger, I know it's a little early to do an evaluation, because the Safeguards Rule just went into effect, but are there special barriers or issues that you've become aware of in this short period of time?

MS. BERGER: So far, some of the panelists have addressed these. My evidence is very impressionistic, but it is a cultural issue, and change is kind of slow.

We've had meetings with lots of industry representatives, and without picking on anyone by identifying them, I've met with large groups where their message has been we just don't think of ourselves this way, and I think that it's going to take time before people start to think of themselves this way.

And to echo what Laura Lundin was saying, as well, the standards that the agencies put forward are fairly general. I think it takes time to translate those into specific practices and to figure out what works over time. Building on what Frank was saying as to service providers, there is a requirement in the Safeguards Rule -- and this is just one example of one of the many

changes that's got to come about and really get streamlined through practice.

There's a requirement that financial institutions oversee their service providers, including by entering into contracts with them. At this point, I think one of the barriers that I'm seeing is there's not yet a streamlined process for how that's supposed to happen. We've been concerned about this all along and really tried to anticipate, but we have, for example, small businesses saying, well, what kind of agreement should I enter into with my data processor? Some of this eventually is going to have to come from the service providers.

They're going to have to start off with built-in security guarantees to their financial institutions so that these things won't be negotiated in an inefficient way.

I already said that we're trying to get at this through education and through outreach to the industry. We're also working to educate consumers and raise awareness and demand to help bring about the cultural change that will make businesses see it in their interest to provide security.

One of the nice publications available on the table -- and I can honestly say one of the few with color

illustrations that's available to you, is our Internet security initiative publication featuring Dewey the turtle. It's our big consumer ed piece talking about what consumers need to do to stay safe online. I point smaller businesses to it at times to say this is what's appropriate for you, because, as Frank was saying, you're a lot more like an individual consumer. The rule is adaptable to your situation, and you can look at these kinds of measures to address your needs.

So, I'm seeing a lot of need to synthesize these broad standards into streamlined practices that businesses can keep a handle on.

MS. GARRISON: So, the common consensus here is that we need to figure out ways to translate these principles into practices, and we've already started talking about some incentives.

I know, Larry, you've already mentioned some. Do you want to quickly summarize some of the incentives that you see in the marketplace or elsewhere to adopt these frameworks?

MR. CLINTON: Well, I think we've already probably hit on most of them.

We try to lower business costs.

So, if you'll adopt best practices, you'll get less insurance cost.

If you do training, we'll get you discounts.

We're very supportive of the Visa program, and we try to encourage that sort of thing with our other member companies.

I think one of the things that's been alluded to here is that those corporations with -- I use this term in quotes, an advisory -- "market power" can use that ability to improve security in their own enlightened self-interest.

While I'm sure that, in Visa's case, Nortel's case, and a bunch of other cases, it was done out of an awareness of security and the public good, I'm sure there was also a recognition that an insecure network is economically threatening to the corporation.

I think that a whole lot of corporations still need to embrace that and insist that, if you are going to be our vendor, if you are going to be our supplier, if you are going to be our customer, we need for you to adopt this system of security, because the Internet is an interwoven network of networks, as everybody in this room knows, and a threat to one is a threat to all.

I think there's a lot more creativity that we think can happen, but as I say, we really need to work on a new paradigm.

The old regulatory paradigm probably doesn't

fit this one.

We need to be a little more creative. I think there's a lot of creative ideas out there, but I'm sure we haven't exhausted the market on them.

MS. GARRISON: This, I think, plays into Mark and what you've been doing in your CISP principles, because from what I have heard it sounds as though branding and consumer confidence were drivers in adoption here. Do you want to speak a little bit about that?

MR. MacCARTHY: I think the major points have already been made.

You know, security is a large topic that crosses a lot of different industries. So, I can only really speak about the incentives that Visa might have had for doing what it did, and it's only in the area of keeping card-holder information safe and secure. But there may be ways in which you could generalize our experience to other companies, as well.

When we looked at the Internet several years ago, we saw some concerns about the security of online shopping.

We saw security as a major threat to the development to that channel of commerce, and we saw it as a potential brand problem for Visa, being associated with an insecure method of payment. For all those reasons, we

decided to step forward and make our program not just a set of “we hope you do this kind of practices” but requirements for actually taking a Visa card.

At the time that this was first being introduced, there were a large number of Internet hacking incidents, there was large publicity about them, and so, we got a pretty receptive audience initially, because people realized that what we were putting forward were ways in which they could then turn around and protect themselves against a business threatening possibility.

The biggest troubles we ran into were when we insisted on audits, when it wasn't just us saying we want you to prove that you're doing the right sort of thing not to Visa but to independent outside security assessors.

A lot of companies would say, well, we do it ourselves, we already know how to do this, why do we have to go out and prove it with an external assessment? We had a lot of discussions in that area, and I think we've gotten over that hump.

A lot of people realize that, in this circumstance, you can't take people's words for it when they're repositories of very, very large amounts of card-holder information.

So, that's the way our program has developed so

far.

MS. GARRISON: Fran, we've heard Frank speak earlier about the shift in thinking from the product developers who are now seeing security as a feature rather than a cost.

Do you have any experience on return on investment, because that clearly seems to be an important driver here for corporations.

MS. MAIER: We're always looking for ways to help a company not just talk the talk but to walk the walk and really have the real commitment to privacy. What we have found, while we might be very successful with the chief privacy officer or the risk manager or the general counsel, legal counsel, and they believe that having sound privacy practices and the seal program makes sense, it's the marketing people and the people who are driving the revenue that we want to try and convince.

And we're undergoing a lot of different studies to try and figure out the pay-back for privacy or for the seal program. I'll talk about one I think you'll be hearing more about in the future, about a little company called Big Dates.

They're not a dating service. They do anniversary-related kinds of things -- birthday party, reminder service -- and they sent out, randomly, 80,000

e-mails. 50 percent of them had the TRUSTe seal at the bottom saying we protect your privacy. They had the seal linked to the privacy statement.

Well, the company saw a 40-percent increase in the join rate and the click-through rate, and that's pretty remarkable.

Now, that's not a well-known brand, but I think it shows that the consumer recognizes TRUSTe. Overall, we're talking to a number of companies who are joining our program to do testing. What's important about that is that it's going to put even more emphasis on having the right programs and the right enforcement and the right strength behind the seal, because if it means that much, then it really has to deliver both for the consumer as well as for the organization.

MS. GARRISON: Mark, you mentioned earlier about accountability. That also seems to be a common theme that's popping up from various panelists.

Can you talk more specifically about how companies in the Visa system are held accountable for complying with the CISP principles?

MR. MacCARTHY: It's indirect. Visa is an association of financial institutions. So, we have no direct relationship with Internet merchants or processors or web hosting companies.

So, the mechanism we use to make sure that these requirements move out into the marketplace is through requirements we put on the banks that work with the Internet merchants.

If there's a problem with a particular merchant where they haven't fulfilled the requirements of the CISP program, then ultimately a fine goes on to the bank that works with that particular merchant, and that merchant bank then moves that penalty on to the merchant.

Ultimately, the way of enforcing the mechanism is through continued membership in the Visa system. It's clearly possible to make sure that merchants aren't permitted to use Visa cards. We enforce that, as I say, through the system of financial institutions that are part of the Visa system.

MS. GARRISON: And have you already taken action, either fines or other types of action?

MR. MacCARTHY: We've had a major processor who did not live up to the responsibilities that it had under the system. We fined them $500,000. They're under suspension right now.

MS. GARRISON: That must have served as a wake-up call to everyone else who participates, too.

MR. MacCARTHY: It catches people attention at high levels.

MS. GARRISON: Yes, I should think so.

Frank, do you have anything more to add about accountability? How do we get there?

MR. REEDER: Accountability is tough, and I guess all accountability ultimately occurs in the marketplace. I would also argue for it -- and here I'm echoing what Mark has already said -- through independent audit. We, again, also haven't talked about the audit community, but they're a part of the assurance network that ultimately goes to fundamental questions that are being addressed by things like Sarbanes-Oxley.

I would like to be mildly contrary on one small point.

MS. GARRISON: You have the privilege to do so.

MR. REEDER: Thank you. Lest this sound like a chorus.

It's probably true that we're not spending enough on security, but I think, as Larry said, quite correctly, we haven't the vaguest idea, because we don't know what we're measuring.

Starting with the fact that developing good software is essential to good security and the ability to provide the privacy assurances. I'm sure nobody is counting that in their security budget, so I simply don't know how one measures that. Probably the deltas are

meaningful assuming that people are consistently measuring. At least we can see change from year to year, even if the base number is mush.

But I think it's even more important that the money we're spending, we're spending badly. Again, what you are hearing from this panel and I think the message that needs to go out is the way you start a good security program is not to hire a very expensive consultant, with apologies to the very expensive consultants who may be in this room, to do a zero based risk assessment when we already know that there is a set of baseline practices that you ought to be implementing and auditing yourself against and then looking at whether there's differential risk, whether you are unique within your industry or sector and ought to be doing something beyond the baseline.

But we've got it exactly wrong. There are a lot of people making very good money -- unfortunately, I'm not among them -- who are selling the same snake oil over and over again, rather than promoting the adoption of knowledge that is already in existence and that is available relatively inexpensively.

Most of the things we're talking about here are not expensive, and so, I would argue that the problem is not money. It may well be how it's being spent.

MS. GARRISON: On that high note, we'll open it up to questions.

Is the microphone working? It is now. Okay.

Brian.

QUESTION: Brian Treddick from Ernst & Young.

I just wanted to call to the attention of the Commission and the participants in the workshop the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants released yesterday another framework, enterprise privacy framework, after about a year-and-a-half of development, friends and family review period over the winter.

It's open for a three-month cycle of review -- June, July, August. We're hoping to get comments from everyone to make it stand out as what we'd consider in the industry as established criteria.

The goal is to allow a company to assess and align its practices around the handling of personal information or allow a public accountant, a CPA, an auditing firm, to come in and audit some set of systems and processes around it.

So, it's available for download, and if you have any questions, I'll be around for the rest of the afternoon. I can answer those then.

MS. GARRISON: Thank you very much, Brian.

Yes. Go ahead and state your name, please.

QUESTION: Thanks. My name is Allen Wilcox. I work for the Vanguard Group.

The question I have for you -- despite my profession's dominant certification and professional organization, it's not just information systems security, it's information security, whether it's in a Rolodex, a baggie, my head, or a computer.

How are any of these frameworks addressing non-technical information security rather than just the places where things are stored and patched and systems are maintained?

What about the actual information -- because systems are just capital assets. Is the information itself being addressed within these frameworks?

MS. GARRISON: Larry?

MR. CLINTON: We agree with what you say. We have copies of our best practices, and we agree completely with that sense.

The first thing that you'll see in our best practices is that you need to have a policy for information security, not just Internet security, and in fact, it includes physical security. Although, frankly, a lot of the same procedures still apply -- you need to have a policy, you need to enforce the policy, you need

to assess the policy on an ongoing basis, you need evaluation -- these are all spelled out in our best practices comment. At this very moment I'm aggressively trying to get people to embrace these.

I completely agree with Frank's comment that there's a lot of stuff that's pretty good that's already out there. What we'd like to see is us moving away from, hey, let's write something new. I'm sure there's lots of new stuff that needs to be written, but let's implement what we've already got, and let's then evaluate that systematically. Then let's rewrite it and move on. I'm sure that's necessary.

MS. GARRISON: Laura, did you want to add anything to that?

MS. BERGER: Sure.

In my opening remarks, I mentioned that the context of our rule takes into account all aspects of how an organization deals with information and not just transactions on the Internet, and that's really embedded in the requirements of our rule. Just to give one example.

In assessing its risks, a company has to take into account all areas of its operation, and we spelled out three particularly essential ones that are required. One of those is employee management and training, and

that's been one of my favorite ones to talk to people about when they call with really difficult questions about how to implement some online protection and they're just really grappling with it.

I just say, well, have you trained your employees yet, and typically, the answer is, well, no, but we haven't really drawn up our employee training plan yet. So, we tried to build that into our rule.

MS. GARRISON: Frank?

MR. REEDER: Yes.

If I may set aside my Center for Internet Security role for the moment and step back into other personas, the whole privacy debate as we know it probably was prompted by a book most of us read for different reasons by George Orwell and the revelations in the '60s and '70s that technology was being used in ways that we didn't anticipate. But if you look at the laws and principles underlying it, there's nothing about technology in the Code of Fair Information Practices or, for that matter, in the Federal Privacy Act of 1974.

It's about information practices, and your question is exactly right. All of the prescriptions that we've talked about have nothing to do with the manner in which the information is stored and processed and everything to do with the processes and content.

Your question is a very healthy reminder that a robust privacy program and an assurance program that supports that cannot stop at the boundaries of the technology system.

MS. GARRISON: With that, we're concluding this panel.

Please be back at 3:15 for panel four, and I would like to thank very much each and every panelist here this afternoon for their contribution to this discussion.

Thank you.

(Applause.)

(A brief recess was taken.)

PANEL 4: Designing Technologies to Protect Consumer Information

MR. SILVER: Welcome back, everyone, to this session, which is not only the final panel of today but the final panel of this pair of workshops which began in May.

This panel will consider how to design technologies to protect consumer information.

Are the microphones working? All right.

And to that end, we've gathered an impressive group of engineers and policy experts.

First, we have Edward Felten from Princeton