LOS ANGELES – (APWG) Hemispheric Unification of Cyber Security Awareness Messaging
Wednesday, October 15, 2014 – 16:30 to 17:45
ICANN – Los Angeles, USA

UNIDENTIFIED MALE: APWG Hemisphere Unification of Cyber Security, October 15, 2014.

CARLOS ALVAREZ: Good afternoon, everyone. We are starting the session. Thank you.

This is the ICANN Security, Stability, and Resiliency Team session in which we are welcoming the APWG, then Anti-Phishing Working Group, and more guests – the Organization of American States and F-Secure – to speak about the "STOP. THINK. CONNECT." campaign.

My name is Carlos Alvarez. I'm ICANN SSR staff. I'm going to be the remote participation manager, so I'm going to read aloud any comment or question received through the chat room.

This session is being streamed online, and here now we have Pete Cassidy. So, Pete?

PETER CASSIDY: Hello, everyone. Thanks for coming in at the end of, I'm sure, a long day. But if people could pull it in closer to the front, we won't have to shout at each other. We've tested negative for most things, except common sense, but our voices are probably strained. So if you could pull up, it would be helpful. It's the nicest crowd. I can testify to that.

My name is Peter Cassidy. I'm Secretary General and Co-Founder of the APWG. I've been running the thing, allegedly, since 2004. One of the

things that the marks the APWG is responsiveness to the common experience of its members.

Our members, as they have since the foundation of the institution, are the people that get up at dawn every day and drive straight through the gates of Hell and manage cyber-crime in real-time. They're the nicest crowd.

But they also see things every day that tell them and instruct them on what we need to do. Very early on, retail-facing members of the APWG came to me and said, "Your wizards are all inspiring. They are awesome. They are relentless gods and mental giants, and they are people that are proud to follow through the gates of Hell every day. But there's one thing you have to know: normal people face the same demons, and you have to do something for them."

"Normal people, who are they?" "Normal people are our customers, Peter. Go do something for the normal people."

So I sat and thought about it and I looked at what was out there. Normal people were being instructed so many different ways they were actually being confused. And as happens with the APWG on many, many occasions, fortune gave us someone who gave us a larger conversation.

Aimee showed up in Tokyo, and I asked her what my – this is Aimee Larsen-Kirkpatrick, Co-Founder to STOP. THINK. CONNECT. Messaging Convention – and I asked her what my members were asking me. "What can we teach the people that they can carry with them to defend themselves from all the bad things happening on the Internet?"

She said, “Peter, the first thing you have to do is get your head out of the technology, because it’s confusing you. It’s not about the technology. It never was. It’s about people and how you shift their behavior just enough to help them help themselves, like smoking, like forest fires.”

That brought up a very different conversation. Aimee’s intervention as a communications scientist changed the conversation about how people can be taught enough to change their behavior to be useful.

From that, we started forging what became the beginning of the STOP. THINK. CONNECT. Messaging Convention as a proposal. What we proposed, really, was to answer a problem statement. The problem statement wasn’t, “There are bad things on the Internet.” The problem statement really was, “How do we get messages across that will stick when everyone’s saying slightly different things?”

If you looked at what was available in 2008/2009, there was tons of stuff coming out of marketing departments, some of which was incoherent, some of which was very good, and some of which actually conflicted with yet other messaging.

So we decided that our real enemy wasn’t the bad guys. Our really enemy was dissonance and to solve that was to do what engineers have been doing from time immemorial. We decided to standardize the messaging.

Here’s the story. From there, we understood one big thing. Once you agree upon a standard set of messages, the thing that will actually ensure its success is nothing less than ubiquity. We were lucky that the

Department of Homeland Security showed up very quickly and adopted it for the United States, but that left 197 other sovereignties we had to worry about, where the Internet crime was rampant and where people were exposed.

So today, a few years on, we have agreements with the Organization of American States to help us bring STOP. THINK. CONNECT. around the membership of the organization, which is all 35, I think, countries in the Western Hemisphere.

What we're doing here today is asserting what we had proposed in 2009: government and industry can work together to do something practical and useful to teach people just enough to change their behavior for the better, to secure their own lives, personalities, and data online. That is sort of what we're pursuing today and we'll pursue as our goal from here on out: complete ubiquity of this messaging convention amongst all sovereignties. Because when everyone is hearing same thing and when everyone can remember the same thing given the number of times it's repeated, there is a slight chance their behavior can be changed.

Anyways, that's my story. I'll give you Aimee, who's doing her bit.

AIMEE LARSEN-KIRKPATRICK: Okay, so I guess I'm going to go through sort of the philosophy behind the STOP. THINK. CONNECT. campaign and how we developed it.

So could you go to the next slide? Next slide.

UNIDENTIFIED MALE: You have to push that button on the screen there. See the one that's [inaudible]?

UNIDENTIFIED MALE: [inaudible] yesterday.

UNIDENTIFIED MALE: You just need to get a computer.

UNIDENTIFIED MALE: Or some technical people.

UNIDENTIFIED MALE: That's a Mac.

AIMEE LARSEN-KIRKPATRICK: So I'll just start. I can't quite remember what the next slide is. But anyway, I actually did show up at – yeah, that slide – so I did show up at a bar in Tokyo and I met Peter at an Anti-Phishing Working Group conference in Tokyo – yeah, can you go back to the – I can't talk that fast. I can try. It must be on a timer or something.

Anyway, when I came into the space, I didn't know a lot about security. I knew a lot about communicating with people and trying to teach them and get them to change their behavior, and I kept hearing people at this conference talk about how they're educating people about cyber security. This was the job I'd been hired for. I was working for an organization called the National Cyber Security Alliance, and they'd

hired me to run a national campaign to teach people about how to stay safe and secure online, and I naively thought, "Oh, I know how to do that. That's easy." Little did I know.

People at this conference were talking about the need to educate the consumer and what they were doing and how important it was, and I would go up to people after they'd speak and I'd say, "What are you doing? Because this is what I'm supposed to be doing. I want to know what you're doing and how you're making it work. I've only been on the job for a couple months."

They would say, "Oh, well, we're not really doing anything because you can't teach people anything. The end users are not capable of learning." So I thought, "Well, that's an interesting perspective."

So anyway, I thought, "Well, that's wrong." So what we're really looking at is trying to change people's behavior and get the technical jargon out. What do they really need to know?

My framework that I was looking at is this is social marketing, social marketing being selling an idea instead of a widget. We see this all over the place in the world we live in. We see it in the public health sector with the anti-smoking tobacco-free campaigns and disease prevention. We see it on environmental issues, teaching people how to recycle, protecting the rainforest and endangered species. These are all long-term campaigns. We're talking generational change.

When I was a kid, it was perfectly okay to light up in somebody's home without asking, and now in the United States, most places, heaven forbid you would do that. You would be a social outcast for lighting up

without asking first. I don't think there's probably a hotel left in the United States that you can smoke in.

Anyway, the outcome of that is that we have a better word, a better community, and a better life. How do you apply that to cyber security? It's challenging.

Let's go to the next slide. That's the framework of how I think about this. Okay, so STOP. THINK. CONNECT. was born. It wasn't known as STOP. THINK. CONNECT. yet. Next slide.

Peter and I, between our respective organizations, called together a meeting of interested people from industry to see if we could get them on the same page to see if we could get them to agree that we needed to find a single message, one that everyone could use, and how could we do that together?

There are actually a couple people in this room that were at that initial meeting: David Perry here, and…

CHRIS BOYER: Chris.

AIMEE LARSEN-KIRKPATRICK: Chris Boyer. You were at the meeting – Chris Boyer from AT&T. That was maybe 30 people from all across industry and a couple of researchers that came together to talk about this idea of how can we come together and develop a message that we all can use? Next slide. Okay, next slide after that.

This was our objective: to see if we could develop this one message that could be used across the public and private sectors. Next slide.

This was really the framework that Peter talked about. This is what we wanted to address. How could we eliminate the discordant information of the threat of the cyber menace, develop a single, sound message to offer clear advice – there's a lot of jargon out there – produce a suite of messages that could be used to raise awareness of e-crime and provide simple tips, free of jargon, and then really create that consensus around one message that would be memorable for consumers so that when they see it, it would remind them that there's something they're supposed to be doing here? Next slide.

We were able to do that successfully. It was a very rigorous process that we went through. The group led the process. We facilitated it, but they made all of the decisions about how to move forward.

The decision was made to actually do research to figure out what the message would be, so it wasn't just us in a room deciding that, "Oh, this is the message that I like, and therefore I decree that this is the safety and security message." We actually did very in-depth consumer research to find out what types of messages would work, what types of message would get people's attention, and what would get them to change their behavior.

The initial adoption ran to 30 large multi-national corporations. I think at one pointed I counted that we had six or seven of the Fortune 10 companies involved in the messaging convention, which I think speaks volumes about how important this was to industry.

Plus we had seven government agencies that participated in it, including the White House, the Department of Homeland Security, the FBI, the IRS, and a couple of others that I can't recall at this moment.

Then a number of NGOs participated as well, and the campaign is growing and it grows, I think, every day and has begun to grow internationally. Can you go to the next slide?

Public Safety Canada. After the United States officially adopted it, it was declared the National Cyber Security Awareness Campaign by the President of the United States in 2010, and it is the campaign that the Department of Homeland Security uses and supports in partnership with the private sector. Canada soon after, I think in 2011, adopted STOP. THINK. CONNECT. as part of their public safety campaign as well. Next slide.

We have been in conversation with treaty organizations to also bring them onboard, and that has resulted in the 2012 Memorandum of Understanding with the Organization of American States, who has adopted the campaign and is promoting it to their member countries. I think the Organization of American States is on the phone and is going to talk a little bit more about their involvement in the campaign as well. Next slide.

I think Asia is up next. The Japan Council of Anti-Phishing has adopted it, as has Malaysia. So it's really sort of picking up momentum and going global right now, which is really exciting for us to see. Next slide.

Oh, I can't forget our friends in Central and South America who have also joined he campaign recently. Panama, Paraguay, and Uruguay have

all formally joined the campaign signing memorandums of understandings. Argentina is in the process of it and so I Chile. They are in the process of developing their MoUs. Next slide.

Suriname, Barbados, Dominica, Jamaica, St. Vincent and the Grenadines are also considering adoption of the campaign. The one country that isn't on here that should be is Trinidad and Tobago is actually in the process of adopting the campaign. I don't think it's…

PETER CASSIDY: Trinidad and Tobago and Belize have [already interrogated] the MoU. It's just a matter of getting ink on paper.

AIMEE LARSEN-KIRKPATRICK: Yeah. The signing of those MoUs is imminent, and Trinidad and Tobago is actually moving forward with developing their campaign.

PETER CASSIDY: I'm hoping by Christmas to have Brazil surrounded. We're hoping by Christmas to have Brazil surrounded so that we have a story that gives Brazil a contiguous coverage story.

AIMEE LARSEN-KIRKPATRICK: Next slide. I'll go through a couple of elements that I think are key for success to building the campaign. Next slide.

This is how I look at the education continuum. I think this is important. Just because you are aware of something doesn't mean that you're

educated and knowledgeable about it. It's a whole continuum or process that you have to take people through.

You have to start at awareness. Once they're aware, you can educate them. Then you can build knowledge. Then they can build skills. Then they have the ability, and then they can put that into practice. You can always be continuing going through that continuum. As people develop their skills and knowledge base, they can move to the next level.

When I was first really working in this space, people were talking a lot of jargon about what consumers should do. It was very confusing, very technical, and the message was, in my opinion, wrong. I was hearing from people like at the Department of Homeland Security that the message should be: you need to be safe and secure to protect the critical infrastructure.

Now, what that has to do with my neighbor, my mother, or your mother, I'm not sure that they would probably understand that – why it's their job to be safe and secure to protect the critical infrastructure. Now, they might understand that they should be safe and secure to protect their finances, which in turn, by taking those same steps to be safe and secure, could end up resulting in the same practices to help protect the critical infrastructure.

So it was really a message that was a little murky. There was a lot of misinformation out there. There was information that was in conflict with each other. I kind of likened it to that we were trying to teach people trigonometry and they didn't know how to count yet.

That's really where the messaging was, and there was a lot of people in the industry that because the end user couldn't understand this trigonometry felt that, "Well, you just can't educate the end user. They're too stupid to know," which is a really negative viewpoint because the truth is there's a lot of really smart people out there. Just because they don't know how to be safe and secure online doesn't mean that they're stupid. It means that they don't know how to be safe and secure online because they haven't been taught the right way or the message hasn't been clear for them.

So it was really taking a big step back and saying, "What is it that we really need to do to educate people to start where they're at and bring them along to where they need to be?" So that's this continuum right here. You can go to the next slide.

Another key element for building, at least in this arena of cyber security, of building awareness and educating people is making sure that we have strong public-private partnerships. Because the Internet is vast and how people us it is varied. It is an all parts of our lives, from government, to how we do business, and how we do banking. Law enforcement is using it, and it is being used in the education sector, both to secure students to allow them to go online, but we're also expecting students to go online to do research, to participate in social networks – all manners of Internet connectivity. So we need to figure out how to come together as a larger community and work together.

Where can government support efforts? Where does it make sense for the private sector to lead efforts? How does law enforcement fit into the picture? How do they educate the public? They can do it

proactively, but oftentimes it ends up being reactively as well, and they need to appropriate resources to be able to do that. And then how do we work within our education system to make sure that we're raising smart, savvy digital citizens from the time that they're first going online so that they're protecting themselves and then are ready to go into the workforce? Next slide.

Again, this may seem simple, but it is really important: who is your audience? Who are you trying to reach? Doing the appropriate research, making sure that you got the message right. Conducting focus groups can provide a lot of insight on how your message graphics is being perceived and is there any stickiness to it? And the establishing good metrics, which in this arena is really tricky because how do you measure somebody's digital awareness/cyber-savviness? It's challenging.

So having all of these things in place are important so that you understand where you're at, where you're going, and if you've met with success. Next slide.

Then establishing goals: what do we want success to look like? What do we want to see as the end result? I don't think we need to talk a whole lot about that. Next slide.

What are the resources that we have available to us? Of course, financial is the one that always pops into people's minds, but partnerships, partnerships, partnerships can be amazing resources. What are the existing platforms that we can leverage to send a message out, whether it's marketing that's already going out?

I always like to use the AT&T example. Every October for the last several years, as part of their support of the campaign, AT&T has printed the STOP. THINK. CONNECT. message on all of the bills that go out to their mobile customers, which I think is pretty amazing.

But how do we leverage even more things like that? Microsoft has done things. Facebook has done things. And it hasn't cost the campaigns any money. Those companies have invested resources to be able to do that. But it's raised the bar for everyone.

Who are the evangelists? How do we get those people out there that can talk about it in a positive way and that people will pay attention to? Next slide.

Some key elements for the message. This is based on the research that we did, but this is also based on research that has come out of social marketing in general. You want to keep it simple. Avoid jargon as much as you can. Keep your language simple and clear.

Stay away from fear-based messages. Fear-based messages cause people to shut down and feel like there is nothing they can do about the problem. "It is so big it's hopeless, so why should I even bother? I'm just going to stick my head in the sand." That's the type of feeling it gives to people.

Instead, use empowering, action-oriented language. You can talk about the problem, but then talk about the positive steps that people can take to protect themselves. That's the tenets of the STOP. THINK. CONNECT. campaign. Next slide.

We can talk about collateral and distribution all day. We can skip this slide.

We talked a little bit about this, but I really believe that this is so important in this field that we know where we're going, that we establish the metrics, that we understand where we're at, if people have heard the message, that we continue to refine the message, and as we meet with success or we meet roadblocks, that we evolve the campaign in reaction to that, so that it stays fresh and new and that it is reaching the audiences that we want to reach in the appropriate manner.

PETER CASSIDY: Metrics are really the next and probably most important frontier in the development of unified messaging for cyber security. When we finished the research on the [original] development of the message, we looked at it and we said, "This is good. It's not ambiguous, and there's not enough hair on the message to get people into more problems or more trouble or to be used against them online."

But the issue is not really the message, per se. It's how effective it is, and at what point does it become operationally potent? In other words, does deployment of the message actually make a difference to the number of infections and botnet nodes and that kind of thing?

This was something that will require more resources than we had at the time, but in spring of this year, we had a meeting in Paris of interested stakeholders mostly from the EU At the end of it, the principal investigator, Director of Research, Dr. Manel Medina of the APWG.eu,

based in Barcelona, proposed a very simple but provocative research proposal: let's teach these people. Let's send these messages down to people, and then let's measure their effectiveness over time within different cohorts. And let us make a science of understanding what messages they receive and how useful they are in helping people protect themselves.

I believe this is the beginning of a completely new frontier in message engineering because we have to take it that seriously in order to gain the benefit of it. And it has to be engineered to this level because the threatscape is so dynamic. At every point along the way, you're going to have new things you're going to have to teach people or emphasize or ask them to pay attention to. So I think this is a very good sign.

Ubiquity of deployment is one thing, but what I really am excited about with the messaging convention is the numbers of communities building out and meeting each other and being able to share information and to join into research projects like that to fire messages into different clouds and see how they work so that we can make messaging an efficient operational instrument for the security of the Internet.

That make sense? That hang together? So that's where we are right now. Sorry, Aimee. You go.

AIMEE LARSEN-KIRKPATRICK: No, I think that's the next slide? I think I might be done. Yup, I'm done. So that was what resulted in STOP. THINK. CONNECT. So on to you, David.

DAVID PERRY: Hi, I'm David Perry from F-Secure Corporation. I've been spending my entire adult life educating people about computer security. I was the very first tech support guy on Norton Antivirus version 1.0 for DOS. I was there for five years. I went to McAfee. I went to Trend Micro.

By the time I got to Trend Micro, I was running all of the tech support, and then they moved me into the marketing department as an evangelist and public affairs guy. I started handling what I think of as mass tech support, where I'm trying to get a message out about what's going on.

I want to tell you something that is evident, and if you've never worked in a tech support department, you could learn a lot from tech support. The main thing that I leaned from tech support is that end users misunderstand the nature of what's going on in a profound way. They misunderstand what the resources are that they are protecting. They misunderstand what the nature of the threat is, and they misunderstand what the nature of the solution is. This is to a very extreme degree.

I wrote a paper on it in 2002 for the Institute of Computer Research Analysis in Hamburg called, "Virus Information, Disinformation, and Myth," and I went through online queries to tech support of 2.5 million messages, and 2 million of the 2.5 million had no idea what was going on.

The main problem that we have is that the public are afraid, not of the real threats in the real world, but of mythological threats that they see in movies and on television. They expect malware when it show up to have immediate and dynamic and dramatic effect that they can tell

what's going on. We have people who say, "I'm not having any malware problems. I'm going to remove this thing off my computer that I pay for every year."

They don't realize that it takes a team of 1,000 people keeping to look at Internet traffic. Today, as of this month, we are receiving an average of one million new, unique threat signatures a day. One million a day. The entire first decade of viruses was less than 100,000 viruses, and now we receive a million new signatures a day.

What's funny is that they're almost all gone by the next day, so that has kind of broken the old antivirus mold, and you get people say, "Antivirus is dead." You all saw that in the paper six months ago when a guy from Symantec said antivirus is dead. Symantec lost $20 million in revenue over him saying that, and he now works at GM.

But the flipside of that is that the nature of the threat has expanded enormously. I'm not trying to scare you with a million new pieces of malware, but we're looking at new threats were mobiles are concerned that are not malware-based at all but that are about the compromising of the connection points that you're using to connect to. Mobiles, actually, we've seen the line blur from crime over into unethical business activity, where its intention is to break your privacy. This comes almost entirely under the aegis of ad-supported software and apps for your mobile. And if you're – yes?

CARLOS ALVAREZ: Excuse me. I'm afraid I'm going to have to interrupt. The OAS is mentioning that they are going to have to leave, that they are an hour and 15 minutes too late.

UNIDENTIFIED MALE: Can they go now?

DAVID PERRY: Yeah. Let's let him go and I'll get back and yell at you in a little bit.

CARLOS ALVAREZ: Okay. Thank you. I'm so sorry for interrupting.

DAVID PERRY: My pleasure. Please, take the field.

CARLOS ALVAREZ: Can you put the call up on the speakers, please? Belisario? Belisario? Can you hear us? Brian? Belisario? Brian? Are you guys there? IT is fixing the issue, Beli and Brian. Try again, please. Beli? Belisario? IT is working on a fix. Sorry for the wait. It's coming.

UNIDENTIFIED MALE: Check, check. Check, check. Check, check, check. Check, check, check. Check, check, check, check, check.

Check, check.

UNIDENTIFIED MALE: [inaudible] test check out again?

CARLOS ALVAREZ: Beli, can you hear? [inaudible]

UNIDENTIFIED MALE: Do the laptop now? Testing, testing. So how [inaudible]

UNIDENTIFIED MALE: The call says I'm the first to join the conference. They must be dialed into the wrong bridge.

UNIDENTIFIED MALE: Test. Test, test, test. Check, check, check, one, two.

CARLOS ALVAREZ: We're going to try to do something. Apologies. Most sincere apologies for the technical issues. There was some weird thing going on with Adobe Connect.

UNIDENTIFIED MALE: Test, one, two. Test, one, two.

CARLOS ALVAREZ: Something weird happened with the Adobe Connect room and the phone bridge. So what we're going to try to do is have the OAS that's kindly waiting there, I'm going to hook them up through my laptop

speakers for them to talk, and with this mic, we'll get them up on the room speakers. Let's hope we can hear them.

Beli can you please turn up? Beli, can you please turn up your speakers?

BELISARIO CONTRERAS: Ready to go?

CARLOS ALVAREZ: Yeah. Turn up your speakers.

BELISARIO CONTRERAS: Now?

CARLOS ALVAREZ: Turn up your speakers.

UNIDENTIFIED MALE: [inaudible] technical difficulty.

DAVID PERRY: We promise that we'll make sure in advance that we've got them connected on our next thing.

Anyway, so all of this experience has taught me a number of things. What we're finding out at F-Secure is, like I said, that the threat on mobiles is not –

UNIDENTIFIED MALE: It seems to be working.

DAVID PERRY: Oh, now you're okay?

UNIDENTIFIED MALE: [I think so.]

DAVID PERRY: Okay, go ahead.

CARLOS ALVAREZ: Beli, can you hear?

DAVID PERRY: Carlos, if you can get it going, in the interest of brevity could you ask them to start on slide number six to get it along?

CARLOS ALVAREZ: [inaudible] Web cam?

DAVID PERRY: Okay. Can you guys speak now?

UNIDENTIFIED MALE: Go ahead [inaudible].

DAVID PERRY: Okay. I'm really sorry, gentlemen. They can hear me, though? Are they listening to us?

CARLOS ALVAREZ: Yeah.

DAVID PERRY: I am so sorry that you weren't able to get connected. Right, so what we're learning is that the malware threat has gone over the top. The phishing threat has gone over the top. The spam threat has gone over the top, and it is difficult to get messages through to the public that cannot be turned toxic.

This is the main thing that I brought to the table when we were having the STOP. THINK. CONNECT. meetings: you have to be very careful not to put out a prescriptive message. If you tell people something concrete like, "Always update your antivirus," the day will come when the bad guys will read that message and will use it against you.

These days, you do not have to update your antivirus. It's all updated against your will, and bad guys frequently come out with, "Click here to update your antivirus," and you are infecting your system. Fake AV is a very regular kind of phishing attack.

So this expands clear across the board. I recently wrote a blog entry called about it called "The Damned," where I was talking about how we are giving people advice that eventually is used against them, which comes up in a very large segment of tech support calls. People call and say, "You told me to do X. I'm doing what you told me." Well, now that

increases your exposure to the bad guys. The blog can be found on my blog site, which is at DavidPerryVirus.com.

I am very happy that the APWG and the NCSA got together with the DHS and made up STOP. THINK. CONNECT. I'm very happy that so much of industry is interested. I think that there is a lot of education need and a lot of awareness need that is not yet being addressed. I am willing to put my time forward on this, and F-Secure is willing to put my time forward on this, and we're happy to be here if we can help at all because something has to be done. Something has to be done, and it has to be done fairly soon.

That's all I have to say.

PETER CASSIDY: Thank you, David.

DAVID PERRY: So who does that leave?

PETER CASSIDY: Are we giving up on Beli? Why don't we just go over his couple slides – his two slides that are very interesting?

UNIDENTIFIED MALE: Why don't we let Peter do it because we should at least get the message out.

PETER CASSIDY: I first encountered the Organization of American States in Strausberg in a meeting of the Council of Europe, where I was one of the expert interveners for the Cyber Crime Convention. He says, "Whatcha working on?" so I says, "I'm working on this." He said, "You know what? All of my member states need to do this. Can I see it?"

He looked at it and this is what they found: we filled the gap that Organization of American States saw with their own member countries because everyone was having exactly the same problem at different points along the curve.

What we did that was different than everybody else is instead of saying, "Well, tell the marketing department to come up with something," we said, "No. We're engineers. We test things to see if they work well, and then we deploy them because that's what you do."

What they saw was that the message was not only sound, it was accessible and adaptable. It was free – a major concern of developing countries, which is a big part of the brief of the portfolio of CICTE at the Organization of American States.

Available already in multiple languages, the Organization of American States has four lingua franca: the French, the English, the Portuguese, and the Spanish. We had already done the translations and rationalized the logo design for use in those languages. It basically sold itself. It meant immediately that Panama and Paraguay, we signed them as member nations of the messaging convention in June 2013, followed soon by Uruguay.

Now the biggest interest we have and the fastest growing interest nexus in the program is from the Caribbean. We believe if we can get the Caribbean nations lined up and finish the Southern Cone, we can sweep the rest of South America and do, I think, a credible job in a year of covering the Western Hemisphere.

But the real lesson isn't the message, the formation of it, or the adoption of the idea that messaging [inaudible]. I think the real message of STOP. THINK. CONNECT. is that people of diverse polities can actually do things together without heroic effort and without heroic costs. We just have to name the problem statement that we're answering and figure out what space we can answer that question in.

That's the lesson of STOP. THINK. CONNECT. I think if we can do this hemispherically, what will follow I think is other problem statements that assume there is a space where we can work together.

That's my story, and I'm sticking with it. Thank you.

Mr. Piscitello?

DAVE PISCITELLO: I'm in the wrong place. I'm going to move. This is Dave Piscitello. I'm the Vice-President of Security and ICT Coordination at ICANN.

What STOP. THINK. CONNECT. is doing in our hemisphere doesn't surprise me at all because I've been to the Caribbean, I've been to Latin America, I have met with ministers, and across the board one of the first things they ask for when looking for capability-building is security awareness.

One of the things that I tend to do is look at a problem statement like, "Making people security aware," and if you peel back some of the layers and you listen carefully enough, there are more layers to security awareness than what the STOP. THINK. CONNECT. project is filling.

So what I'd like to do is talk to you a little bit about what we would like to do at ICANN and what we, unfortunately, are a bit slow in delivering as a result of some staffing issues. We'll still continue to try to do and promise in 2015.

STOP. THINK. CONNECT. is such a good and successful program that when we were talking, not only in our hemisphere but in Middle Eastern and Africa, there's just an insatiable drive to get more people to do this. I think it'd be great if we had a success story in our hemisphere, but I can't imagine it's just going to be constrained to that.

One of the things that I noticed when I was talking to ministers is that they had three actual areas where they were talking about security awareness and didn't realize that they were different. STOP. THINK. CONNECT. is essentially for consumers. It's for the average person. If you listen to Emily's talk, there was a very good emphasis on making very simple language, not using complex terminology.

The focus of it is really on the things that consumers do on the Internet and protecting the data that they are concerned about. You can't expect consumers to be protecting databases of banks, and you can't expect consumers to be worried about critical infrastructures.

From governments' perspective, however, they have other users, and I call them ICT users. Those users not only have to think about protecting

their personal data, but they also have a responsibility to protect data of their organization or their government because they actually have two roles now.

So one of the training initiatives that I've convinced John Crain, our CSO, to undertake is to help us put together some training material for ICT users. We will be developing that over time, and we're actually trying to very aggressively enlist some people that we really think can do this well.

The third component is that you can't just train the ICT users, but you also have to provide people who are IT administrators in these ICT worlds how to manage those users, how to deliver the training. For example, how do you phish your own organization so that you give people an actual learning moment that they should not have done what they do. How do you turn that into a learning moment as opposed to a disaster? So a third component is training that we're hoping to do to complement what STOP. THINK. CONNECT. has done is to have this training and material for ICT admins.

So I think with that sort of trifecta of education, what we can do in a lot of the hemisphere, having people like Carlos on my staff who speak Spanish and getting others who would throw in, as you say, without a lot of heavy hauling and add the languages that we need for the region and the hemisphere, I think we can actually deliver to governments the basis of really, really improving digital citizenry, improving the operations of governments, the appreciation of how to protect the critical infrastructures, and also to educate them outside the ministries in these governments that understand IT.

If you go to any of these meetings and you sit down with the Minister of the Water Systems, he says, "Why should I worry about anything that has to do with digital? I'm responsible for water and irrigation and things like that?"

It's only when you get to explain to them, "You are probably going to put in these things called process control systems, and you're probably going to have some reason to be connected to the Internet to download updates to the software, and this is how this gets really hairy in a hurry."

These kinds of Stuxnet scenarios are things they don't understand, and part of the education process beyond the three that I mentioned is actually writing something very high-level and elementary for ministers to understand, "Oh, this really does affect my ministry."

So you've just sort of scratched the first layer, and the exciting thing is you've got so many people already involved in it. Because you've given them a taste, it's going to make it easier for us to start coming in and going, "By the way, if you really like that, you're going to love this."

So I'm excited that Peter and Aimee have come here to do this. I'm excited to see David again because we're old cronies from other areas. And I think that just the enthusiasm by people who have spent a lot of time in this and the willingness to come to the ICANN community and say, "Join us, and here's what we're doing," is a great first step.

So I hope that we can find other ways to amplify what we're doing here. I hope that the recording can be – we'll use a little bit of Audacity and take out all the comic relief here and long pauses. I think that we can

really do well from what we've started here and make this a little bit more important. And perhaps at a future meeting, even if we do it remotely, I think we can carry on with this kind of message.

Thank you for coming.

CARLOS ALVAREZ: I'm going to read a question sent by Kat McGowan through the chatroom. She's with LinkedIn.

"Will the STOP. THINK. CONNECT. message be translated into non-English languages to non-English-speaking countries?"

AIMEE LARSEN-KIRKPATRICK: Absolutely.

CARLOS ALVAREZ: "And not only the message, but the name itself: STOP. THINK. CONNECT?"

AIMEE LARSEN-KIRKPATRICK: Yes. So STOP. THINK. CONNECT. has already been translated into several other languages. It's been translated into Spanish – I think there are two Spanish versions – French, and a handful of other languages I can't recall off the top of my head.

UNIDENTIFIED MALE: Portuguese and Japanese.

AIMEE LARSEN-KIRKPATRICK: Portuguese, Japanese, and I think a couple of Scandinavian languages, and maybe German. I think the good example here is probably Spanish. One of the things that we know is that the words STOP. THINK. CONNECT. don't necessarily translate straight across the board for all countries and all languages and that it's important that the right words are found that have the right meaning.

For example, it was translated into Spanish, and then when we went to Uruguay last November, I was there with the Organization of American States and talking to the folks with the Uruguay C.E.R.T. and they were struggling with the Spanish translation that we had provided to them of STOP. THINK. CONNECT. The way the word "stop" had been translated in Uruguay was very aggressive and it was not the right word for "stop" in Uruguay, even though it was the right word in, say, Mexico. So they were working on coming up with what the appropriate word would be to address the citizens of Uruguay.

So that's something that we've been very sensitive to and open-minded about, making sure that it's translated correctly for the audience that it's being presented to.

CARLOS ALVAREZ: Okay, well, I believe that concludes the session. Peter, would you have anything else to add?

PETER CASSIDY: Fantastic. Thanks for coming out so late. How many people here belong to enterprises or nation states that are members of the STOP. THINK. CONNECT. Messaging Convention and use the logo and slogan?

Oh, good! Oh, wow! I'm preaching to the choir.

AIMEE LARSEN-KIRKPATRICK: I would just say that if your company or government is interested, they can always reach Peter and myself. My e-mail is up there. But more information can be found at the website StopThinkConnect.org. The information that you need – contact information is there, how to join the campaign, particularly for companies is there with countries we've been signing memorandums of understanding. So StopThinkConnect.org.

[DAVID PERRY]: That was StopThinkConnect.org?

AIMEE LARSEN-KIRKPATRICK: Yup.

DAVID PERRY: I would like this dialogue to go on. I would like to bring your voices to the table, and I would like to hear from other people who have other constituencies and other concerns.

This is just getting started, basically. You said we've just scratched the surface with this. So if you're really interested, you ought to get more

involved, and I know there will be more talks in the future about STOP. THINK. CONNECT.

AIMEE LARSEN-KIRKPATRICK: Security Awareness Month, yes. It's National Cyber Security Awareness Month.

UNIDENTIFIED MALE: And what's it about?

AIMEE LARSEN-KIRKPATRICK: National Cyber Security Awareness Month.

UNDENTIFIED MALE: In this nation for the whole month of October, we're aware of cyber security.

CHRIS BOYER: It actually is broader than just the U.S. this year.

UNIDENTIFIED MALE: That's right.

CHRIS BOYER: There's actually an EU initiative, so National Cyber Security and Awareness Month…

UNIDENTIFIED MALE: Could you please provide you name and affiliation?

CHRIS BOYER: Oh, sure. Sorry. My name is Chris Boyer. I'm with AT&T, but I'm also a member of the Board of Directors of the National Cyber Security Alliance, who runs the month.

Yeah, the month is basically an awareness month, so in the U.S. it's declared by the president to be National Cyber Security Awareness Month in October. There are events all over the country throughout the month to kind of raise awareness of cyber security issues. It kicks off on October 1 every year, and there was actually a kick-off of it in Brussels this year as well from an EU perspective.

So it's starting to be adopted in other countries as well. I think in Canada, also. So it's starting to spread more. If you're familiar with Data Privacy Day, I think it's a similar type of concept.

CARLOS ALVAREZ: Okay, well, thank you so much, everyone, for attending. Thank you, Pete, Aimee, David, and Dave. Thank you, Beli and Brian, although they're not there anymore.

Thank you, everyone.

[END OF TRANSCRIPTION]