RSA Conference 2014 Keynote for Art Coviello (Feb. 25, 2014)
Script

Welcome to RSA Conference 2014.

When I heard someone from the cast of *T. J. Hooker* was opening the show, I was hoping it was going to be Heather Locklear.

I guess I should have known better when Priceline.com asked for a sponsorship.

All the same, it was appropriate to have William Shatner do the opening because I think it's safe to say this year's Conference will boldly go where no conference has gone before!

It promises to be the biggest ever, with more than 25,000 attendees, more than 400 sponsors and exhibitors, more than 550 speakers, and the press in record numbers.

For more than twenty years, the RSA Conference has been *the* place where the world talks security.

But this year seems different.

Well, maybe it isn't *that* different. Shortly after its birth, this Conference was the focal point for the battles over key escrow, the Clipper chip and

our crypto itself… at that time, classified as a munition with an export embargo. We had discussions over the nature of privacy and how government and industry could engage in productive collaboration rather than paralyzing conflict. Sound familiar?

Almost 20 years later we seem to be back at that crossroads again. And while I try to use my keynote to highlight the macro issues facing us, including guiding principles and best practices to take us forward - and I will do that - this year I need to start with a discussion of RSA itself. Because unlike nearly 20 years ago when we were seen as leading the charge against the government to secure the privacy of digital infrastructures, we've been accused of being on the other side of that battle.

We spoke to this issue when the claims surfaced in December. But what's hard to do in the fast moving swirl of today's 140-character – based media dialogue is provide any broader context for the state of the industry at the time. Or the state and evolution of RSA's business. And that's what I hope I can do here today.

Ironically, the situation RSA finds itself in today traces its roots to the same battle that RSA and its founder, Jim Bidzos, led against the NSA in the 90s. Just as we were prevailing in those fights, the age of one vendor – RSA – controlling much of the direction of encryption was ending. Because our encryption tools were under export controls until 1999, and without international patent protection, most of the rest of the

world had already implemented the RSA algorithm using open source toolkits. With the expiration of our U.S. patents in 2000, the entire world headed that way. And that is why encryption in use today has been overwhelmingly implemented with open source toolkits.

Recognizing that reality, and encryption's inevitable shrinking contribution to our business, we worked to establish an approach to standards setting that was based on the input of the larger community rather than the intellectual property of any one vendor. We put our weight and trust behind a number of standards bodies – ANSI X9 and yes, the National Institute of Standards and Technology (NIST). We saw our new role, not as the driver, but as a contributor to and beneficiary of open standards that would be stronger due to the input of the larger community.

In the early 2000's, that transition took place. So, when the industry began discussions on using an elliptic curve-derived algorithm for random number generation, rather than hash-derived, we were happy to support what had already coalesced in the community as a strong method. A method that became a NIST standard in 2006 with little opposition.

Given that RSA's market for encryption tools was increasingly limited to the US Federal government and organizations selling applications to the federal government, use of this algorithm as a default in many of our toolkits allowed us to meet government certification requirements.

And that brings us to today. When, last September, it became possible that concerns raised in 2007 might have merit as part of a strategy of exploitation, NIST, as the relevant standards body, issued new guidance to stop the use of this algorithm. We *immediately* acted upon that guidance, notified our customers, and took steps to remove the algorithm from use.

So now I turn to the NSA itself. Has RSA done work with the NSA? Yes. But that fact has been a matter of public record for nearly a decade. You see, many people forget that the NSA is not a monolithic intelligence gathering organization. The NSA also has a defensive arm – the Information Assurance Directorate (IAD) – whose stated mission is to defend information systems and U.S. critical digital infrastructure. In practice, NIST, RSA, and indeed, most, if not all, major security and technology companies, work primarily with this *defensive* division within the NSA. In addition, we all receive valuable intelligence from the NSA on threats and vulnerabilities.

Regardless of these facts, when or if the NSA blurs the line between its defensive and intelligence gathering roles, and exploits its position of trust within the security community, then that's a problem.

Because if, in matters of standards, in reviews of technology, or in any area where we open ourselves up, we can't be sure which part of the

NSA we're actually working with, and what their motivations are, then we should not work with the NSA at all.

To eliminate that possibility, we endorse NIST's new proposal for the creation of cryptographic standards. And, perhaps more important, we support the recommendation of the President's Review Group on Intelligence and Communications Technologies to simplify the role of the NSA – that it should be solely a foreign intelligence organization – and that the IAD should be spun out and managed by a different organization. Sadly, much of the great work of the IAD is getting lost in the feeding frenzy around this controversy. It's not only sad, it's dangerous for the country. *However* its done, creating greater separation between the offensive and defensive roles of the NSA would go far to repair relations and rebuild trust.

But I don't want to limit this critique to the NSA, as it has become clear that they are not alone. I would repeat what I just said to *all* governments and their intelligence agencies.

In short,

All intelligence agencies around the world need to adopt a governance model that enables them to do more to *defend* us and less to *offend* us.

Stepping back, the tension between and among the competing interests of governments, businesses, and individuals in the digital world should

not be surprising. Information has become more easily accessible, *and* more valuable. We are in the midst of a fundamental and historic shift in the use of Information Technology, a shift that is already having monumental implications for the future of our society and culture. The rapid expansion and democratization of technology has brought the agendas of disparate groups crashing together with unpredictable consequences.

The collision of these agendas highlights the lack of societal norms to guide our digital world. We've had centuries to figure out the norms of behavior and rules of engagement in the physical world. Even after all that time, we're *still* figuring it out. We've had a scant decade or two to figure out the rules for the digital world.

The resulting chaos and confusion that reigns online, in the media, and in legislatures and courtrooms around the world reflects the lack of digital norms.

A famous or should I say infamous humorist once said, "Mankind is facing a crossroads - one road leads to despair and utter hopelessness and the other to total extinction."

As funny as that sounds, it accurately portrays people's views of the current situation. We *are* in the midst of chaos and confusion, but if we don't figure out digital norms and do so quickly, the alternative may be extinction. Extinction of the Internet as a trusted environment to do

business. Extinction as a trusted environment to coordinate research and development. Extinction as a trusted environment to communicate with each other.

Digital technology, Big Data and the Internet of Things are becoming a potential path out of just about every societal ill. On Thursday, Scott Harrison will be sharing the inspiring story of his organization, charity: water. Without the Internet, though, his story wouldn't be a *success* story, and thousands of communities would still be without fresh, safe water to drink.

Yet, these same digital capabilities are also becoming a path to a destructive power that rivals anything since the coming of the nuclear age.

Clearly, we are at a crossroads. How we in the industry and governments around the world choose to lead on these issues will have profound implications for good or ill for generations to come. We cannot shrink from this responsibility – we must embrace it.

Therefore, I am using this keynote and we must use this Conference to call upon all nations to adopt and implement the following principles:

First, to renounce the use of cyber weapons, and the use of the Internet for waging war;

Second, to cooperate internationally in the investigation, apprehension and prosecution of cyber criminals;

Third, to ensure that economic activity on the Internet can proceed unfettered and that intellectual property rights are respected around the world;

And, fourth, to respect, and ensure the privacy of all individuals.

Why now? Why these four?

First, the genie is out of the bottle on the use of cyber weaponry, and unlike nuclear weapons, cyber weapons are easily propagated and can be turned on the developer. Paraphrasing a famous quote, those who seek military advantage riding the back of the tiger will end up inside. Many of you may have seen the *New York Times* article yesterday on this very topic. We must have the same abhorrence to cyber war as we do nuclear and chemical war.

Second, the only ones deriving advantage from governments trying to gain advantage over one another on the Internet are the criminals; criminals who grow bolder by the day. Our lack of immediate, consistent and sustained cooperation, globally, gives them the equivalent of safe havens.

Third, the benefits to all of us from productivity improvements in commerce, research, and communication are too valuable, to not achieve agreement on the rule of law. Rule of law must rule!

And fourth, our personal information has become the true currency of the digital age and while it is important that we are not exploited, it is even more important that our fundamental freedoms are protected. But with our personal freedom comes responsibility. Governments have a duty to create and enforce a balance. A balance that embraces individual rights and collective security. A balance based on a fair governance model and transparency. As to governments themselves, let me quote one of the U.S. founding fathers, James Madison, "the great difficulty lies in this: you must first enable the government to control the governed; and in the next place oblige it to control itself." Openness and transparency will be paramount.

Many of you will be skeptical or, worse, cynical that these principles could ever be adopted. Many will think I am naïve. Yet, there is precedent. We already live in a dangerous world, but it is a world that has been made less dangerous by accords on nuclear non-proliferation, the outlawing of chemical weapons, and the outlawing of war in space.

Why not cyber space?

When I recently spoke to a noted hacktivist and self-styled anarchist about these concepts, he said that he didn't want to hear about any Cold

War analogies. I'm sure his lack of faith in *any* government would lead him to believe that these principles are unrealistic and impossible to attain.

But that is a dangerous belief and leads to the conclusion that chaos - and worse - are inevitable. We must reject that notion.

I *am* inspired by perspective from the Cold War and a speech given by President Kennedy at American University in 1963, a speech about peace in an age of nuclear confrontation. I believe his words *are* relevant to us today … this is what he said:

"Our problems are man-made. Therefore, they can be solved by man. And man can be as big as he wants. No problem of human destiny is beyond human beings. Man's reason and spirit have often solved the seemingly unsolvable – and we believe they can do it again."

I'm not talking about these principles as some utopian vision of the future. No nation will or should act unilaterally. The lack of trust, and the genuine, conflicting ambitions of so many will make adoption a difficult task … A task made even more difficult by the lack of constructs for proving attribution of actions online. It will take inspired leadership and a more enlightened world. Nations act out of self-interest. But, whatever our differences, there should be no doubt that these principles are in the interest of *all* nations and *all* of humanity. So let us devote

ourselves to a series of concrete, achievable actions on a path *toward* these principles.

Governments can't do it alone. They need our help as well. So what can we, we in this industry and as individual organizations, do?

We can bring together vested interests so that an environment of positive dialogue is built. This week, the RSA Conference is bringing together the cyber czars of 12 nations to discuss security and privacy. Last Summer, RSA Conference Asia Pacific, similarly brought together the leaders of the ASEAN countries. Last year at the RSA conference, we brought together the leadership of the US Financial Services – Information Sharing and Analysis Center (FS-ISAC) and the leadership of 50 international banks. The result has been the expansion of FS-ISAC internationally, aligning the interests of the world's financial services industry in strengthening the security and reliability of financial systems. We need more of these collective efforts and I'm proud of the role RSA is taking in creating these opportunities for discussion and adding our voice to the debate. Many other organizations and conferences have engaged in similar efforts.

But the entire industry must take a more active role than ever before. We, all of us, understand both the risk and the threats facing us better than anyone. We can also move quickly knowing that governments often cannot.

Therefore, we must as an industry strongly advocate for the principles I laid out.

We must in a thoughtful, factual, and persistent way raise the level of understanding of the consequences of inaction. Instead of headline-grabbing hyperbole, we must lay out a series of coherent, compelling arguments for why inaction leads to a lesser and more dangerous future for generations to come. We must shine a light on these issues and inspire our political leaders as never before.

And we must do our job continuing to develop process and technology frameworks to implement the Intelligence-Driven Security model that I have spoken of in the past. We are already under way and are making progress with NIST under President Obama's executive order.

Finally, we must do what we do best: develop and implement the technologies that will protect us now and into the future.

In all of my years in security I have never seen the scale of investment and innovation that we're seeing today. And, none too soon.

As we all know, the expansion of the attack surface and increasingly sophisticated malware and methods have outpaced conventional controls.

Never before has the need for Intelligence-Driven Security been greater.

We urgently need anti-malware that is intelligent enough to spot zero day threats AND block them.

We urgently need security systems that are intelligent enough to see patterns of attack and by correlating and analyzing data from numerous, diverse sources across an organization, give us the actionable information we need to respond. That's why RSA is partnering with our sister company Pivotal to provide a new model for deploying and leveraging Big Data across all parts of an organization.

We urgently need these systems to be intelligent and integrated enough to automate responses and prevent harm, not only in today's hardware-defined infrastructures, but also in the new generation of software-defined networks and infrastructures.

We urgently need a new, more intelligence-based approach to identity systems. We need to recognize and adapt to the age of user-defined IT, reflected in trends like shadow IT and BYOD. It is essential that these systems enable security teams to accept the changing balance of power between users and IT departments, while still being able to exert policy and control over user devices and sessions as they relate to their organizations. These systems must operate in mobile and cloud environments, so identity governance can be managed consistently.

Also, we urgently need tools to improve our ability to articulate and manage digital and operational risks, which are converging in today's technology-dependent environment.

And, finally we need to make it easier for organizations to take advantage of these tools even if they don't have the resources or expertise themselves. That's why RSA is expanding our managed security service partnerships, working with companies like Verizon, who can provide security management services for customers leveraging technology from RSA and others.

This is a very important, but not an exhaustive list of what we need to be doing as an industry.

What I want to convey is that while we urgently need to help the governments of the world develop the digital norms, we as an industry need to do *our* part as well by developing and implementing the capabilities that secure those norms and our future.

Neither of us can do it alone. It will take industry and government working in concert to create the digital world we want. That is why I am calling on the nations of the world and all of you to work together for the benefit of all of us, all humanity. I know this will not be easy to achieve. We all have our own interests and we clearly have differences.

But let me once again refer to President Kennedy's American University speech. He delivered it about six months after the Cuban missile crisis; six months after the U.S. and the Soviets almost blundered into thermonuclear war; six months before he was assassinated. I was ten years old at the time. Most of you weren't even born.

This is what President Kennedy said, "let us not be blind to our differences, but let us also direct attention to our common interests and to means by which those differences can be resolved. And if we cannot end now our differences at least we can help make the world safe for diversity. For in the final analysis, our most basic common link is that we all inhabit this small planet. We all breathe the same air. We all cherish our children's future, and we are all mortal."

Premier Khrushchev was said to have been deeply moved and impressed by President Kennedy's speech, and the Nuclear Test Ban Treaty was signed two months later.

So let's make President Kennedy's words breathe once again and spur us to action. Let governments adopt the four principles I outlined and let industry create the secure frameworks and technology we need. Let all of us put aside our differences and move forward this week, and in the weeks, months and years to come with confidence and resolve to make our digital world safer for all.

Thank you and enjoy the Conference.