

Microsoft at **RSA** Conference 2008

April 7-11 | Moscone Center San Francisco

Creating a More Trusted Internet

By Scott Charney, Corporate Vice President, Trustworthy Computing, Microsoft Corp.

Published: April 8, 2008

Imagine what the Internet could be if everyone had a more secure and privacy-enhanced experience, an Internet where devices and software enable people to make more effective choices about who and what they trust in their online interactions.

It is not an overstatement to say that the Internet has transformed the way we live. Social networking represents the new town square; blogging has turned citizens into journalists; and e-commerce sites have spurred global competition in the marketplace. But with people of all ages flocking online, and with the proliferation of high-profile, targeted attacks on individual or organizational information, assets and identities, more and more people consider the lack of security and privacy on the Internet to be at an unacceptable level.

My introduction to cybercrime occurred in 1991, when my career as a criminal prosecutor took a surprising turn: I was tasked by the United States Department of Justice to focus on cybercrime. As a lawyer, I was trained to study past cases and apply the rule of law to the facts at hand. But here I was on the electronic frontier with no precedent, no guidance, and, as a prosecutor, I was challenged by the global connectivity, anonymity, and lack of traceability that the Internet provided to cybercriminals. In the years that followed, I worked on amending computer crime laws, developing guidelines for searching and seizing computers, brokering new international agreements to combat cybercrime, and understanding the intersection of security and privacy (I was on the Clinton administration's Privacy Working Group and served as vice chair of the OECD Expert Group on Security and Privacy).

In March 2002, I was hired by Microsoft Corp. to be its chief security strategist. My assignment was to focus on the security (and later privacy and reliability) of Microsoft's products and services, but I soon realized that my thinking was too narrow. It was not just about protecting our customers, but protecting everyone; even someone without a computer was dependent upon computers at his or her bank or telecommunications provider, or in his or her government. I realized that I was once again responsible for public safety; but in the private sector.

During my 17 years of security and privacy work, the Internet and its uses have grown dramatically. Indeed, the Internet has had a positive impact on many, many aspects of our society, but greater global connectivity combined with the increasingly valuable information stored online has resulted in a new array of threats and an increase in cybercrime. It has become increasingly clear that if cybercriminals remain anonymous and untraceable, there will be no meaningful accountability for online crime and little by way of deterrence. In the physical world, we have effective proactive measures (locks and keys, community watch, law enforcement patrols) and effective reactive measures (arrests and prosecutions). Many crimes are prevented, and many crimes are solved. But the Internet is different. Despite improvements in effective proactive



Join the Dialogue

- **Public Policy:** How should we enhance security on the Internet while supporting social values such as privacy and anonymity?
- **Technology Innovation:** How do we, and how should we, build a Trusted Stack that enables a safer, more Trusted Internet?
- **Economic:** How do we create economic incentives to drive a more secure, and privacy-enabled Internet?

www.microsoft.com/endoentrust

measures, criminals are not held accountable for their actions and are increasingly emboldened. If we want the Internet to reach its full potential, we need a safer, more trusted online environment.

To that end Microsoft and other companies continue to make progress on security and privacy issues. For six years, and as a result of our focus on Trustworthy Computing (www.microsoft.com/twc), Microsoft has made significant progress toward improving the security and privacy of our products and services. We embraced the Security Development Lifecycle, as well as defense in depth and threat mitigation technologies. Along with our industry partners, we continue to build a more secure, private and reliable computing experience. But Microsoft and the technology industry alone cannot create a trusted online experience. For that to happen, industry must not only band together but must work with customers, partners, governments and other important constituencies on a road map for taking Trustworthy Computing to the Internet.

We believe there are three key pieces to creating greater trust on the Internet. The first is creation of a trusted stack where security is rooted in hardware and where each element in the stack (hardware, software, data and people) can be authenticated in appropriate circumstances. The second piece involves managing claims relating to identity attributes. We need to create a system that allows people to pass identity claims (sometimes a full name perhaps, but at other times just an attribute such as proof of age or citizenship). This system must also address the issues of authentication, authorization, access and audit. Finally we need a good alignment of technological, social, political and economic forces so that we make real progress. The goal is to put users in control of their computing environments, increasing security and privacy, and preserving other values that we cherish such as anonymity and freedom of speech.

The opportunity is *now*. Some serious issues, such as botnets, ID theft and child safety have served to focus people's attention on security and privacy issues. Some important technologies, such as public key infrastructure (PKI) and smart cards, are now mature enough for broad deployment. Some important debates, such as how to achieve more security and more privacy instead of trading one for the other, have led to new thinking about how we can create a more secure *and* privacy-enhanced Internet. And we have learned through past experience how to align technology, social forces, political will and market dynamics to achieve great progress on important issues, just as we have learned why important efforts sometimes fail.

Therefore, at this year's RSA event, Microsoft will not announce a new company strategy. Rather, we will use this opportunity to ask all who care about online safety to join in a robust and meaningful discussion about building a more trusted Internet. At the same time, we know customers have concerns about threats today, so we will also talk about integrated solutions we are delivering to help customers address current needs for maintaining more secure and private environments. To facilitate the dialogue, we are providing a white paper describing End to End Trust, Microsoft's proposed vision to help create a more trusted Internet. So we invite everyone to read this white paper, posted on www.microsoft.com/endoendtrust, and join the dialogue through our discussion forums.

A more trusted Internet is good for our business and for our customers, but the paper also reflects Microsoft's sense of corporate and social responsibility, values that we know are shared by others in the Internet community. So in the coming months, we will share our thoughts about the feedback we received as part of this dialogue. We will see if there is consensus on what a more trusted Internet might look like and how such a vision could be achieved and share with you Microsoft's next steps toward establishing End to End Trust.

"... if we want the internet to reach its full potential, we need a safer, more trusted online environment."

**Read the whitepaper
Join the dialogue**

Go to Microsoft's End to End Trust forum, and let your voice be heard.

www.microsoft.com/endoendtrust