Building Trust in Cyberspace

By Dr. Ramon Barquin

President of Barquin International
&
BeyeNETWORK Government Expert
Building Trust in Cyberspace
By Dr. Ramon Barquin

Ultimately, success in cyberspace will be determined by trust. We mentioned in a previous article how heartwarming it is to at least see interest in the topic. Last year’s ACT-IAC Executive Leadership Conference (ELC) featured a track on “Innovation, Mobility and Trust”; and some months ago, I participated in a panel titled, “Should a Privacy Ecosystem be a Mandatory Component of the Identity Ecosystem – Are Privacy Challenges Manageable?” It was part of the two-day (March 13-14, 2012) NIST NSTIC/IDtrust Workshop on “Technologies and Standards Enabling the Identity Ecosystem” held at the National Institute for Standards and Technology (NIST). NSTIC stands for the National Strategy for Trusted Identities in Cyberspace, and it is a White House initiative to “improve the privacy, security, and convenience of sensitive online transactions.”

This is, of course, better said than done. The Strategy calls for the creation of an "Identity Ecosystem" for people, organizations and infrastructure. The assumption is that if these entities – persons, groups, things – can be authoritatively authenticated through technology, standards and policies, then we can all be safe from cybercrime and live happily ever after on the Internet.

Fascinating! One goes into the NSTIC’s home page and aside from the reference in the NSTIC name, there are very few actual references to the term "trust." Yet that’s what it is all about.

In my article Innovation, Mobility and Trust, I mentioned that trust is a term to which everyone inside the Beltway pays lip service, but it almost never generates real action. Specific experiences convinced me of this going back to a presentation I made almost thirty years ago in Congress dealing with a closely related topic. It was largely ignored. And when the Digital Government Institute announced a conference on “Building Trust in E-Government” about ten years ago, it was cancelled due to lack of registrants.

The difference between then and now is that we are under siege on the cybersecurity front. The head of the FBI has declared recently that it will be a bigger threat than terrorism. The generals have created a Cyber Command (USCYBERCOMM) and are ready to fight and win the cyberwars. And we are all under a constant bombardment from the press about the perils of identity theft, privacy breaches, industrial cyber espionage, and invasive and destructive malware.

Protecting ourselves from these challenges is going to be expensive and time-consuming. Furthermore, we need to sort out how much of this falls in the realm of our personal responsibility, what should be left to the marketplace and what role the government should play. And if government includes the military, law enforcement and the intelligence community, then
how can we at least safeguard an individual’s civil liberties. Ultimately, people will need to “trust the system.”

**What is Trust?**

Let’s go back to basics. What is trust? Trust is a social construct. It is one of many such elements that compose our reality such as: control, confidence, risk, meaning and power. Trust emerges from a history of repeated reliable interactions.

In my opinion, technology can help, but it cannot establish trust. IT has facilitated a move toward a “technical” interpretation of trust (i.e., trusted systems, identity management, authentication, trusted ID) but has also challenged our traditional views on trust as we shift the question to whether technology artifacts can be attributed with trust. In general, that is not the case. Trust is not attributable to artifacts. At best, one has to rely on our trust in the designers, creators and operators of technology. Properties of technological artifacts form a message to determine the trustworthiness of those agents.

We know from some excellent work done by Annette Baier (See Baier, Annette. 1986. “Trust and Antitrust.” Ethics. 96(2): 231-260) that trust is a three-part relation between the truster, the trusted and the entrusted good, and that for trust to be established, the truster must see the trusted as: having a goodwill, encapsulating the interests of others and be competent to handle the entrusted good.

Think about the technology behind the system, the institution that owns the system, and the rules and procedures to operate the system. The reason trust is so important in a medium that is becoming the preferred one for e-commerce, e-government and social communication in general is because trust lowers transaction costs, lowers monitoring costs and bonds people.

What can we learn from history? Implement, monitor and improve. Technology and transactions will create an etiquette – netiquette – that must emerge from ethics. A framework for monitoring and enforcement will also emerge as an environment of trust emerges.

There is no silver bullet, but there are many examples of muddling through. It means that a combination of market forces, regulation and control, monitoring and enforcement, standards, codes of behavior and, of course, technology will all play an important part.

History provides us with some examples. The telephone, with party lines and telephone operators capable of eavesdropping, developed approaches for dealing with such issues as the technology continued to progress. Yet we know it is still far from perfect since there are many tools and techniques that enable electronic tapping of a phone. Trust in the telephone depends at the very least on what you are discussing, with whom, where and over what medium.

Commerce has a long history of letting the marketplace adjust for lack of trust until standards and regulation develop. The frequently used “baker’s dozen” was a message to customers that they were dealing with a vendor that wasn’t out to cheat them.

*Building Trust in Cyberspace* as published on BeyeNetwork.com October 16, 2012

*Reprinted with permission.*

*All Rights Reserved. Copyright 2012, BeyeNETWORK™, a TechTarget company*
On a trip to Vienna a few years ago, I puzzled over a metal bar embedded to the left of the main entrance of St. Stephen’s Cathedral. (Actually, there are two, but that’s just a technicality to be resolved as you read on.) On inquiring, it was explained to me that it was installed there centuries ago as a way of allowing “visiting merchants to comply with local regulations” since many towns had measures that were of common use, especially with respect to length and weight. In Vienna, length was measured in terms of the “ell” or Viennese yard, which applied mainly to linen. There was a separate “ell” measure for drapery, hence the second bar on the side of the cathedral. This allowed the buyers to verify before paying and hence assisted in establishing the trustworthiness of the vendor in the eyes of the customer. The fact that the measuring rod was on the side of the Cathedral, the House of God, was not lost on the parties involved.

So we can see, in this case, how standards, the marketplace and technology came together over time to address the need for trust in one environment. I am sure that the same “muddling through” will prevail on the Internet too.

We’ve come a long way, but there is still a long road to travel. Paraphrasing Winston Churchill: We are not at the end, nor even at the beginning of the end, but we may very well say that we are the end of the beginning.
About the Author

Dr. Barquin is the President of Barquin International, a consulting firm, since 1994. He specializes in developing information systems strategies, particularly data warehousing, customer relationship management, business intelligence and knowledge management, for public and private sector enterprises. He has consulted for the U.S. Military, many government agencies and international governments and corporations.

He had a long career in IBM with over 20 years covering both technical assignments and corporate management, including overseas postings and responsibilities. Afterwards he served as president of the Washington Consulting Group, where he had direct oversight for major U.S. Federal Government contracts.

Dr. Barquin was elected a National Academy of Public Administration (NAPA) Fellow in 2012. He serves on the Cybersecurity Subcommittee of the Department of Homeland Security’s Data Privacy and Integrity Advisory Committee; is a Board Member of the Center for Internet Security and a member of the Steering Committee for the American Council for Technology-Industry Advisory Council’s (ACT-IAC) Quadrennial Government Technology Review Committee. He was also the co-founder and first president of The Data Warehousing Institute, and president of the Computer Ethics Institute. His PhD is from MIT.

Dr. Barquin can be reached at rbarquin@barquin.com.

Editor's note: More articles from Dr. Barquin are available in the BeyeNETWORK's Government Channel.