Since its modest beginning in 1969 as the EDP Auditors Association, ISACA has come a long way. In those days, relational data structures were still emerging. The proof of concept for the Internet was in progress, but not yet ready. Ronald Rivest and his colleagues were looking for an alternative model for authentication that would work in a network environment. Telecommunications infrastructure was doing reasonably well, but it was inextricably bound to land and the analog signals. Efficiency from computers was the key focus, and mainframes were the rule of the day. Power of data and scale of communication had yet to emerge. 

So much has changed! The power of telecommunications has unleashed whole new industries, mobile devices and apps, data floods, and social networks. Business has gone global in a virtual sense and new companies with innovative technology backbones are surpassing older, established giants in market capitalization within years of their origin. 

With this change, ISACA has embraced trust in information systems in a timely and visionary manner. Trust is a rather complex, age-old concept with political, social and moral dimensions. In recent decades, the rainbow of implications of trust and trustworthiness has grown in size and shades. At the same time, the risk of breakdowns in appropriate levels of trust has increased in scope and materiality. It is timely that the microscope is on trust, although control and security are also going to remain issues of the day. 

In his book, Liars and Outliers, Bruce Schneier states: “Society runs on trust. We all need to trust that the random people we interact with will cooperate. Not trust completely, not trust blindly, but be reasonably sure that our trust is well founded and they will be trustworthy in return.” Trust involves “giving discretion to another to affect one’s interests.” Whereas an overwhelming majority of people obey the implicit societal contract on trust, there are always defectors. Because of them, the ecosystem of trust breaks down; as a consequence, people stop trusting each other. This is the beginning of a whole new set of actions: regulating, policing, monitoring, surveying, screening, checking and so forth. Because the defectors violated trust, everyone pays to maintain an infrastructure to check on the violators. 

Among all the developments affecting the role of trust in modern times, the Internet stands out both in terms of scale of impact and enormity of challenge of maintaining trust. This system of loosely connected networks includes 40,000 privately managed networks among 425,000 global routes that cut across national boundaries and cultures. Arguably, this system is functioning remarkably well. Perhaps this is due in large part to the fact that the technology in place nurtures trust; the online retailer can expect payment for what it sells and buyers can expect delivery of what they bought online. People can use mobile devices to donate to a worthy cause; the donee gets the funds and the donor gets the proof of his contribution. So far, the level of trust has seemed to grow along with the impressive growth in Internet-based organizations. 

But cracks in this trustworthy system have begun to surface. At its recently held conference in Dubai, the International Telecommunications Union (ITU), a United Nations agency, approved by a majority vote a treaty giving governments new powers to close off access to the Internet in their countries, effective 2015. Authoritarian governments will be able to place control over access to the Internet. Although selective censorship of content has been practiced currently at individual, organizational and national levels, this change could result in a massive authoritarian control. Nations can censor content, monitor traffic and go after those who violate their “law.” Their citizens will not be able to access unfiltered content such as that which caused the Arab Spring, for example. Call it a digital Cold War, or just plain resistance to rights...
of information access—it will change the logically seamless, free-flowing and always accessible network of networks. A digital Iron Curtain would mean a less-resilient network and the loss of truly global web sites. Undoubtedly, the nations that are standing by the concept of a free Internet and have not signed the treaty will also lose—all because of the conviction of the supporters of the treaty that cooperation, or keeping the trust, is simply not to their advantage. And the recourse to compensating controls to offset the treaty’s impact seems almost unrealizable in this case.

The following is another example with relatively much less concern, but which, nevertheless, brings home the point: Consider a neighborhood community or a large apartment complex that permits pets on its premises. People walk their dogs and are trusted to pick up after their dog. A few residents violate this trust. Of course, the hunt for these violators, if feasible, will promptly appear on the neighborhood’s board of directors’ agenda. Technology is now available to nab the violators. How? Businesses like PooPrints offer to create a database of resident dogs’ DNA, which is then used to identify violations by looking for matches between the unattended waste and the database entries. In sum, violation of trust by some pet owners results in the deployment of a technology to free the neighborhood from those who stray from the implicit social contract. And this, in turn, restores the trust mechanism so that those who stray can expect few, if any, instances of the undesired behavior.

A key difference between the Internet access issue and policing wayward dog owners is that in the latter case, the problem is local and can be addressed locally. Although the cost of governance will also hit the pockets of otherwise cooperating dog owners, the undesired behavior can be controlled and trust of the community can be reestablished. The Internet issue is different, however, in that the scale is global, where it is hard for communities of nations to agree on and commit to their common interests.

There is another major difference between the two cases. One can say that the action of violators does not make the Internet untrustworthy. Put differently, you can still trust the system to provide trust in the Internet. It is the user community that brings on the restrictions of rights to access, not the system as such. The question is: Do we consider the user nations in this case an integral part of the system, or outside of those who build, maintain and provide the Internet? In contrast, the neighborhood community in the second case can be asked to accept monitoring as a part of the contract to belong to the community. Interestingly, the technology comes to help maintain the trust among the community residents, rather than being the lever that prompts the breakdown of trust.

So the scope and reach of individuals, communities, organizations and nations in nurturing trust and trustworthiness is a complex issue. Technology may only be one of the forces in the mix.

Distrust rules out the beneficial effects of trust. Failure to be trustworthy is not the norm, but it can happen anytime, anywhere. Take, for example, the December 2012 Newtown, Connecticut, USA, tragedy, where a young man shot to death innocent school children and staff at the school. Regardless of the reasons why this happened and whether it can be prevented in the future, deep down at the root level, the issue is whether parents can trust the ecosystem of the school where their child is spending a lot of time. How do you make society work when a major crisis like this one says to a parent, “Don’t trust the school’s ecosystem to protect your child.”?

ENDNOTES

1 I remember having to sleep by the telephone while waiting for the requested international connection. The call operator would wait until the person called showed up on the other end of the line at a local post office in India.

2 The complete vision/tagline states: Trust in, and value from, information systems.

3 Horsburgh, H.J.N.; “The Ethics of Trust,” The Philosophical Quarterly, 10(41), October 1960, p. 343-354

4 Schneier, Bruce; Liars and Outliers, Wiley, 2012

5 Ibid. This definition from Russell Hardin was quoted by Schneier.


7 Op cit, Crovitz


9 Op cit, Horsburgh, p. 350

©2013 ISACA. All rights reserved. www.isaca.org