

## **The Will to Regain the Confidence-Trust of Our Customers and Citizens**

Carlos Solari

We live in an age of great uncertainty – a period of unprecedented technical innovation that reshapes our lives. It is innovation that accelerates even as we harbour an unquiet sense that we don't know its destination; where will it take us and what becomes of us in the process? Ray Kurzweil, one of our pre-eminent innovators spoke in a recorded discussion at Harvard University to this point of innovation acceleration. It was February 2005.

Inviting questions, a young student in the audience asked the question that her seniors, the bearded *professerati* also asked, yet not as simply. “What happens to our souls; are we in danger of losing our souls”, she asked in great earnest? His answer, honest and direct was nonetheless the more disturbing. Mr. Kurzweil was “mindful”, he said, of the “intertwined nature of the risks with the benefits”.

What does happen to our souls? Not an easy question to answer; a contrast of science and the existential. Taking liberty to expand on this question we may ask, what happens to our sense of who we are, our humanity and our cultures if we permit innovation to go unchecked even by simple prudence? Can the pace of innovation be slowed enough that we can answer this important question?

If only we could slow it down enough that both its promise and its dangers are better understood – give us time to think through its benefits, assuage our concerns. It cannot be slowed is Mr. Kurzweil's assertion, the bad will come with the good; it runs on its own headlong momentum, fuelled by the competitive global markets – subject to a law that may be as simple as technology begets technology only faster and faster. But was this the question that she was asking or was her question more probative; whether it is worth losing our souls for the sake of innovation; are the benefits really worth the risks?

Actually we do know the answer to this question – it depends. In the most extreme example nuclear power is innovation that gives us the many benefits of electricity but with a price of fear for every generation here forward to grapple with - that in the wrong hands it can also threaten our very existence; our souls are in danger indeed. There are risks and there are consequences of the most severe kind for innovation not fully understood and without the necessary controls.

We accelerate the innovation engine nonetheless with few questioning the consequences. Nowhere is this age of uncertainty more pronounced than in the world of cyber space where it seems that information technology continues to thread into everything and it is all changing so rapidly. In the world of cyber space we enter new ground before we have even begun to figure out how to protect the present – the cyber security dimension of cyber space.

There are already consequences. In 2007 alone just reading from news events there were breaches of information control affecting 162 million people; personal account data that was misplaced, lost, sold or stolen. This compares with 49 million in 2006. <sup>1</sup>In January 2008 the investment firm Société Générale reported that it had suffered a massive \$7.1 billion in trade losses in just two days; the reasons were simple enough, system controls that were not in place, bypassed or ignored.

Governments are awakening to another grim reality, the knowledge that national infrastructures, the very pillars that hold up societies, commerce, the lights, food supply everything that sustains life for seven billion people around the world, they all have a mutual interdependence that cannot be undone and they are all particularly dependent on two of these infrastructures: energy and communications. We who are in the communications business should ask the question; to what extent is the communications infrastructure hardened and are these infrastructures designed robust in balance to the risks that we know exist? The question should be asked for the present and also for its future state, that is, as we change the technologies underlying this infrastructure are we designing them risk-hardened?

To answer this question we begin with one word, *convergence*. Convergence is the global communications transformation; it is happening everywhere around the globe converting from proprietary, separate technologies and infrastructures for voice, video and data to single infrastructures, a single underlying technology. The very same technology that runs the Internet for data is the technology that will soon run voice (telephony) and video in all its manifestations.

And we answer the question with another term – *Web 2.0*. Employees are individually using Web 2.0 and more progressive companies are strategically embracing Web 2.0. Like it or not people are syncing their iPods, using social networking sites, blogging etc. Security purists see Web 2.0 as a threat; CIO's see the great potential that these technologies can create inside their companies breaking down silos, reducing latency. It is the next major thrust of differentiation – those embracing it will compete better in marketing, sales, customer enablement – the possibilities are endless. No doubt about it. Convergence is the principal underlying network transformation and together with Web 2.0 they form the next big promise of the information revolution.

With Convergence and Web 2.0 applications and services we are quickly if not already reaching the point of no return. But do we know the risks involved with the Internet Protocol (IP) based technologies and what about the consequences? Absolutely. Have we mastered how to make this technology less vulnerable? Absolutely not. Have we at least taken pause to slow down this convergence to Convergence until we figure out the measures of protection? Not in the least. And what of the payload, what we call Web 2.0 representing all the new services and applications, the great benefits that will derive from this convergence to IP, have we figured out how to protect them? Not at all – actually

---

<sup>1</sup> [www.attrition.org](http://www.attrition.org)

quite the opposite – Web 2.0 makes the current challenges of security small by comparison.

Tracking back to where we started this chain of inquiry, it was a question of whether we are designing the convergence technologies hardened to the importance that communications has in our national infrastructures – again, with the energy infrastructures, the two from which all other infrastructures depend completely.

Many would answer this question with an optimistic “yes”. A more sanguine answer is made obvious by another series of questions: a) do we have a systematic and generally accepted standard way with which to measure security, b) are we using these metrics broadly across the industry and in a transparent way that we can take a look and answer them independent of the vendor community, c) are the laws and regulations of nations that provide governance for the information communications technology in parity with these metrics and with the pace of change? With these three simple questions, all with the same answer, no, no and no, we don’t have to ask for opinions. It is clear enough.

If we don’t measure security, then our working assumption cannot be that security happens by chance. Take a look inside the complex networks that make up convergence and we get the confirmation. The many incidents of compromises in cyber-security provide further indicators that no, we have not yet mastered how to secure the information, the systems and that there are consequences. What are we to do?

First we recognize that the situation is not all doom and gloom – there is much that already exists and much forthcoming in technical capability, security models and processes. Second, we must recognize the need for urgent corrective action as the timeline is tied to the pace of transformation – the converged next generation networks getting installed around the globe. It’s not too late, but it won’t stay this way much longer. Loiter too long undecided and without the necessary resolve to action, the time will come quickly when our only recourse is to slap on patches on top of patches. Sound familiar? Third, we must change how we view and adopt security in complex systems. We must resolve to change how we develop the information technology - telecommunications systems, how we acquire them, manage them and how we serve our customers. We must stop the nonsensical notion that if we only train our end-users with how to be good security engineers we can improve the state of security. In an ideal world, security is systemic and part of basic system design.

As the suppliers of the information technology - telecommunications systems it takes a commitment of will, resolve and action to recover the confidence and trust given to us by our customers, our citizens and governments. Conversely as buyers, if we blindly accept these systems without asking how well they are designed hardened to mitigate the risks then we should not be surprised to find out that they are delivered without the necessary protections. We become co-conspirators in the current failing model - trying to protect inherently vulnerable systems accepting a share of responsibility that belongs not with the buyers but squarely with the system developers and suppliers. It is time to change our behaviour as well as our methods.

There is good news to encourage our action. In 2003 the ITU/T X.805 security standard conceived at Bell Laboratories was proposed as a model for how to design in the security in a repeatable, rigorous and consistent way. This model allows the measurement of security in complex systems, a missing part of our overall formula for correcting our course. It allows us to be prescriptive and to use a common language between the system developers, the manufacturers and the companies-agencies making the IT purchases. It allows a purchasing agent to make a single statement in a request for proposal (RFP) and so communicate the basis for evaluating the degree to which the vendor has applied security. For the vendor, it removes the element of ambiguity and provides the inducement to make security a prime consideration in the system design – one that pays for itself as security becomes a differentiator in system selection.

Just as importantly, this standard coupled to the developing ISO 27000 series standards and IT management methodologies give depth to what have been here-to-date standards with much in process and policy but poor in the detail for how security is designed. By adopting this standard as the framework for security, we can create the transparency needed so the market can self-correct and reduce the burden of poorly conceived legislation and burdensome regulation that, rather than improve security, simply adds cost overhead that we can ill afford.

From 2003 to the present, much transpired with the evolution of the X.805 security standard in Bell Laboratories. It went from a good theory to the tools and methodologies that are now serving within Alcatel-Lucent to take the necessary steps for designing-in the security. The decision was made, the will and resolve taken with action. The first steps are in place to take this theory and put it into practice. Clearly, these are but initial steps and though important as they are, by no means is the practice in one company sufficient to change what is an industry malaise. It needs help from governments, academia and the industry at large to take this small instance and transform it into an industry practice. There is no gain if we don't do this together.

So it is that innovation accelerates as Ray Kurzweil says, a march forward to the world of Convergence and Web 2.0 while present networks remain unprotected; our mastery of the security paradigm an elusive target. There are always consequences; some we can see today, others remain to be seen and to be felt. The fact that all infrastructures have a co-dependency to the communications infrastructure requires that it have a commensurate level of protection to the importance of its role in our lives.

To correct our course we must build foundational constructs that can be measured and apply a common language that transcends from the technical to the policy. We need better models such as the X.805 security standard and we need better communication between the policy makers and the engineers. Absent these, we see the result that is today - policy disconnected from the reality on the ground, knee-jerk reactions that exacerbate rather than remedy - a spiral of increasing cost in bureaucracy that detracts rather than improves cyber security.

We consider three key points already stated but worth repeating: first is that we don't have much time – we cannot afford to wait a few years to begin embedding security in the systems of convergence and Web 2.0. Point two is that we need models that allow us to measure security – measure it in the design stage, in deployment and in the operational stages. This simple attribute will transform cyber-security from the mystic art that it is today to the science of metrics, baselines, and business-rational remediation. This is the language business executives expect and understand. The X.805 standard can be such a model available in the present time to help us make this transformation.

In truth, the stakes could not be higher and the problem of cyber security could not be more serious. This is the third point. Information communications technology is in everything and becoming more so with each day that we automate to improve operational efficiency and compete in the global markets. When the convergence to Convergence is done, when Web 2.0 is deeply rooted in a few years time, it will be too late and too expensive to redesign these systems making them hardened against a hostile environment of hackers in league with crime syndicates or authoritarian governments unwilling to align to the principles of individual privacy. It matters in the utmost that we get the security right and in time to make a difference.