

The Machine-to-Machine (M2M) Market's Acoustic Shadow

(Reprinted with permission from *M2M Premier*)

M2M can become an integral part of information management thanks to uncompromising information security

By

Stratton Nicolaides (*)

Summary

An acoustic shadow occurs in an area where atmospheric and/or topographical obstructions impede normal sound propagation. During the American Civil War, acoustic shadows dramatically affected the outcome of battles when commanders, unaware of the merciless fights roaring only a few miles away, failed to send reinforcements.

The author advances that the M2M market is currently in a similar pocket of silence as it undergoes a massive transformation. Powerful forces are reshaping the transport and processing of data bringing about both challenges and opportunities. The raging (and largely unheard or misunderstood) battle rests in security threats to the data or information as it is transported and processed.

Unquestionably, watertight information security is critical to winning this battle. M2M-focused information security with its battery of new weapons such as compliance with the ISO 27001 standard must work to effectively and seamlessly protect host hardware and software. As a result, M2M will move from the periphery to the center and become a cornerstone of an integrated data management system that translates data into meaningful business information.

(*) Chairman and Chief Executive Officer of Numerex.

The Acoustic Shadow and the M2M Market

American Civil War historians consider the “acoustic shadow” one of the conflict’s most baffling, disruptive factors that might have significantly altered its outcome. An acoustic shadow occurs in an area where atmospheric and/or topographical obstructions impede normal sound propagation, creating a pocket of silence. During the Civil War, acoustic shadows dramatically affected the outcome of battles when commanders, unaware of the merciless fights roaring only a few miles away, failed to send reinforcements.

How does this idea of the “acoustic shadow” relate to the Machine-to-Machine (M2M) market? As Peggy Smedley of *M2M Magazine* has repeatedly and accurately asserted, it is not only the existence and impact of M2M (altogether, a *silent revolution*) which is overlooked, but as importantly, its rapidly changing environment, shifting from a *product-centric* to a *service-centric* world, which forces M2M players to redefine themselves if they want to become a critical and seamless ingredient of business management. Undoubtedly, the eye-popping potential of “location- based services,” “real-time location systems,” “radio frequency identification devices (RFID),” “telematics” and the like, seems a potent and positive – if disruptive – force. And, as equally beyond question, the role of M2M continues to mature, innovate and expand. Yet the dynamics of its metamorphosis require a painstaking read of the tea leaves to break through the acoustic shadow – which we could call euphoria or progress or a “boom” – and take on the biggest battle yet in the M2M market: information security.

The Acoustic Shadow In Context

Dr. Charles Cross, professor, Longwood University (Farmville, Va.), and an expert on the acoustic shadow, recounts the story of the Seven Pikes battle in his book *Acoustic Shadows and the Civil War*[1]:

On May 31, 1862, Confederate forces under General Joseph Johnston attempted an attack on Union forces to the east of Richmond. The ensuing battle, known as Seven Pines (or Fair Oaks), was one of Johnston's rare offensive forays during the course of the war. More comfortable with the defensive, Johnston on this occasion concocted one of the most confusing, poorly executed tactical plans of the war.

Meant to synchronize forces on three converging attack routes, Confederate Major Generals James Longstreet, Benjamin Huger and D.H. Hill got their men tangled and then bickered over who had priority on the various routes. Even after this disastrous start, the Confederates still might have prevailed but for an unusual occurrence. Johnston planned to send reinforcements under Brigadier General W.H.C. Whiting on a flank attack whenever sounds of musketry were heard from Hill's troops, two miles southeast of Johnston's headquarters. The attack, if it had occurred in a timely fashion might have created a Confederate victory - but Johnston never heard the sounds of a battle, which was raging in full force.

This is one of the earliest examples in the Civil War of one of a type of acoustical phenomenon that had been noted for two hundred years prior to Seven Pines and given the catchall name acoustic shadows. Though citizens of Richmond could clearly hear the battle five to ten miles to their east, the sounds of musket fire eluded Johnston's ears. Similar scenarios occurred at a number of other important Civil War battles, sometimes with dramatic effects on command decisions.

Why? Importantly, the sea changes that are driving M2M innovation and expansion are not merely cosmetic or “bolt-on.” Collectively, they represent a radical new approach wherein processes are re-designed, partnerships and acquisitions are carried out, and value propositions are adjusted to respond to specific customer demands that aim at blending M2M technology with corporate IT systems. Successful M2M enterprises understand uncompromising customer requirements and become an integral and seamless part of corporate asset management.

This article reviews the major trends and challenges tied to the battle behind M2M’s acoustic shadow – the fight for data integrity and information security – that will ultimately shape M2M’s new environment. It also underscores the strategic consequences for M2M players that are trapped – or choose to remain outside – the acoustic shadow and away from the battle. Finally, it also foreshadows one way to ensure that the battle is won and that the M2M landscape is one of opportunities – not casualties.

The Battle Behind M2M’s Acoustic Shadow: Information Security

The first step in overcoming the acoustic shadow comes through defying the convention of the rank and file and search for where the battle’s actually taking place in M2M. Today, marching to the left or right exposes a landscape rife with opportunity – but also mandating that information security be deployed to ensure these opportunities don’t erode into threats. Examining some key trends within the enterprise-meets-information further illuminates the point. They include:

- The Rise of IP as the Dominant Protocol
- The Dawn of Web 2.0/Enterprise 2.0
- The Growing Need for Actionable and Integrated Business Intelligence (BI)
- The Renewed Emphasis on Information Security by Equipment Vendors, Software Companies, and Telecom Operators
- Relentless Regulatory Pressure for Information Security and Privacy
- Escalated Threats to Information

Rise of IP as the Dominant Protocol. Throughout the world, Internet Telephony (IP) is growing by leaps and bounds. Synergy Research's Worldwide VOIP Forecast projected that telephony was to account for 68 percent of enterprise telephony shipments in 2007 [2]. Familiar examples of this upturn such as BT's 21st Century Network (21CN) program and China Mobile's decision to deploy a full-scale, nationwide IP network bear testimony of IP's global ascendance [3]. In the not-so-distant future, the provisioning of M2M applications will, to a large extent, only use IP-based technologies. Some believe it will decrease cost and time for all M2M communication [4]. It is very telling that M2M is often dubbed "The Internet of Things" or "The Pervasive Internet".

However, since telecommunications and data processing are being merged into a single network (the "IT network"), the possible contamination of one side by the other exponentially increases. As Ian Kilpatrick, writing about M2M security risk, puts it in a very succinct and yet concerning way: "Anywhere, anytime, anyhow access is now becoming increasingly achievable" [5]. This increased vulnerability brought about by unlimited access is amplified when wireless, in fixed or mobile forms, is considered.

As users of the Internet conduit, M2M solution providers must protect themselves from data corruption and other malicious interferences. However, and perhaps more importantly, as trusted suppliers of services through that conduit, they must ensure, whether on their own or following their customers' requirements, that they are not themselves "pollution agents." As a case in point, companies are increasingly drawing up their service-level agreements (SLAs) with their telecommunications carriers with additional security requirements [6].

The Dawn of Web 2.0/Enterprise 2.0. In the last few years, terms like "Web 2.0" (Tim O'Reilly) and "Enterprise 2.0" (Professor P. McAfee) have emerged to describe the impact of many recently-developed concepts and technologies on enterprise system and management. Call them buzzwords or fads, but these terms encapsulate profound changes that cannot be ignored by the M2M community because what they represent will shape the way business is done in the years to come. The Web as a platform and the

multidimensional network effects brought about by an “architecture of participation” are main characteristics of Web 2.0.

At the corporate level, open-source programming; utility computing, defined as the provisioning of IT-based functionality on demand (e.g., Software-as-a-Service [SaaS]); and Service-Oriented Architecture [SOA] represent catalytic elements facilitating the application of Web 2.0 concepts in the enterprise. Within this framework, new software is being developed in the open, and constantly modified and improved (hence a new term: “perpetual beta”).

SOA is often presented used in concert with phrases such as “game changer,” or the “next disruptive force.” Volumes have been written about SOA’s attractiveness for a heterogeneous environment of systems, software and applications. It allows the introduction of new capabilities without starting from scratch, and, therefore, the protection of IT infrastructure investments. Concurrently, oft-touted SOA flexibility and reach contain inherent security issues. Concerns are starting to be heard about securing M2M connections in organizations that have deployed SOA. As Eric Pulier and Hugh Taylor pointed out in an early *Developer Magazine* piece framing the issue, “The machine-to-machine interactions have received less attention...If organizations begin deploying an SOA without giving due consideration to alternative security mechanisms, unauthorized users may find it simple to penetrate and evade detection because the systems are now directly exposed in a standards-based manner and the security mechanisms used are either nonexistent or very simple and ‘large-grained [7].’”

According to the industry analyst firm The Gartner Group, 80% of all software development is to be based on SOA by 2008 [8]. Therefore, as security concerns prompted by the SOA pervasiveness will be heightened, partners and suppliers will be required to measure up to newly-defined information security standards.

The growing need for actionable and integrated Business Intelligence (BI) through a variety of data centralization approaches such as Master Data Management (MDM), Customer Data Integration (CDI), Data Warehousing and Mining (DWM), Business

Process Management (BPM) and Enterprise Decision Management (EDM) Companies are moving beyond simple data collection tied to production processes and customer behaviors. They want to exploit the prodigious amount of information they have to extract meaningful insight into their business. These decision makers seek to ferret out sensible statistics and other types of hidden patterns to better manage risk and uncertainty.

This demand for immediate problem identification and resolution has given rise to “real time business intelligence” (a.k.a. “Business Intelligence 2.0”) which is “the process of delivering information about business operations without any latency” (Wikipedia). M2M technologies are an important arm of such BI 2.0-based systems. While the Gartner Group confirmed as much in early 2007 by touting the new years as “business intelligence 2.0 time,” it also delivered this ominous warning:

“one of the most important points that organizations had to understand was the issue of ‘dirty data’, or information that was added incorrectly to begin with or had been corrupted. While it is acknowledged as an issue, according to [Gartner vice president of research Andreas] Bitterer, organizations “underestimate the size of the issue. ‘Dirty data is not an exception,’ he said. ‘There is not a company on the planet that does not have a data problem.’” [9]

Consequently, M2M service providers are expected to meet stringent security requirements if they want to move up the value chain (i.e., through translating dumb data into business intelligence).

The renewed Emphasis on Information Security by Equipment Vendors, Software Companies, and Telecom Operators. Recently, a re-orientation of priorities among communications players followed customers’ growing concerns related to a rise in information security breaches.

As a result, the IT security industry has undergone a consolidation phase. In June 2006, storage specialist EMC bought authentication security-software company RSA for \$2.1 billion. Two months later, IBM purchased security Internet Security Systems (ISS) for \$1.3 billion, while Check Point announced in December 2006 that it had signed an

agreement to acquire intrusion detection analyst NFR Security for about \$20 million, and in January 2007, that it had acquired Protect Data for over \$500 million.

At about the same time, Cisco made public its intent to buy IronPort for \$830 million in cash and stock. On November 1, 2007, IBM launched a “major initiative” to drive sales in the data security market, including \$1.5 billion in spending in 2008 (much more than IBM ever spent in this area) on marketing and product development [10]. By the same token, the rumor mill is filled with speculative scenarios about moves from HP and others into the data security arena to round out their products.

As far as telecommunications carriers, some large operators have begun buying out technology specialists that can provide them with the necessary tools to compete. For example, in October 2006, London-based BT announced that it had purchased networks security specialist Counterpane for an undisclosed sum [11]. In May 2007, Verizon acquired Cybertrust, a privately held provider of global information services and now claims to be the “No 1 Global Information Security Player” [12] in direct competition with AT&T, which is also promoting its security portfolio as a differentiator to ‘pull through’ the sale [13].

Again, it bears repeating that these consolidation moves stem from increasing customer requirements around security. The M2M customer is no exception: they are aware of potential security battles, the pressures it brings to bear, the mounting regulations seeking to address it.

Relentless Regulatory Pressure for Information Security and Privacy. Whether in the United States or abroad, and as a result of highly publicized scandals and unjustified invasions of privacy, regulators are increasingly concerned with protecting corporate and personal information. Laws and regulations have been enacted and put in place to provide the legal framework for that purpose. For instance, depending on the type of organization, the location or specific markets, companies may have to comply with regulations and standards such as:

- Sarbanes-Oxley Act of 2002 (SOX);

- Health Insurance Portability and Accountability Act (HIPAA) of 1996;
- Gramm-Leach-Bliley Act of 1999;
- California Security Breach (CA SB) 1386 of 2003;
- Federal Information Security Management Act of 2002;
- Federal Information Processing Standard (FIPS) 140-2, FIPS 199, FIPS 200 and NIST Special Publications 800-53, 800-59, and 800-60;
- Department of Defense Information Assurance Certification and Accreditation Process (DIACAP);
- Payment Card Industry (PCI) Data Security Standards (DSS) of 2004;
- International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC) 27001:2005;
- Basel II (International Convergence of Capital Measurement and Capital Standards – A Revised Framework) of 2001 – 2008;
- Personal Information Protection and Electronic Documents Act (PIPEDA) of 2000, Canada;
- Federal Freedom of Information Act of 2002, Mexico;
- Directive 95/46/EC on the Protection of Personal Data of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000, European Union.

Threats to information are not going to go away; their acceleration has become a fixture of the business environment. This last trend, which might be ignored because it is not tangible – but rather a constant of our insecure world – overshadows the M2M market. The permanence of innovation and adaptability by nefarious minds in the area of information security must be integrated in M2M activities. It is a challenging endeavor. Elusive and diffuse, “threats are evolving fast, but by the time you read about them in your paper or news brief, you are already behind the curve.” [14] Therefore, it is not enough to recognize that threats do exist. Being effectively alert to their "metastatic" proliferation is becoming a condition of the M2M evolution into maturity. In December 2007, Cisco released its first annual report on the global state of security. The report's findings are an eye-opener and reinforce the fact that security threats and attacks have become more global and sophisticated [15]. Heretofore unheard or unseen threats are unfolding before us. It behooves the M2M player to be wide awake, constantly vigilant and nimble enough to adjust within a potentially uncomfortable, menacing environment.

Consequences of Staying in the M2M Acoustic Shadow

Incantations around Total Quality Management (TQM), which seem to have peaked in the mid-1990's, have been useful in emphasizing what should have never been forgotten in the first place: businesses are to provide quality products and services. This is their *raison d'être*. Quality requirements were never codified in a widespread set of mandatory and regulatory rules the same way information security requirements are, for in instance in the SOX or HIPAA frameworks (Six Sigma set of practices that bend toward quality aside). One good reason might be that there are gradations in quality levels ("more or less good") and, in the final analysis, quality is in the eye of the beholder. This is not the case with security and privacy. There are no two ways to look at a security breach: either the data is corrupted/stolen or not. The financial consequences could be far reaching in addition to potential civil and criminal liabilities. Therefore, it would be a fatal mistake to construe the security-related regulations as the "new fad," bound to vanish with time. They are here to stay, and the M2M industry must move beyond the acoustic shadow and begin proactively identifying and playing close attention to them.

Breaking from the M2M Acoustic Shadow Requires Sensory Development

For the shrewd M2M company witnessing this evolution, the logical conclusion is that thriving in such a demanding environment requires adaptation. However, others could see these constraints as a sign to wax conservative, falling back on traditional activities and avoiding the challenging unknown. Still others, more optimistic, could rather see them as a bountiful source of opportunities.

It is not novel claim that the future of the M2M market lies in unified data integration, meaning a graduation from peripheral, basic-sensor networks to more holistic information platforms. UK-based Juniper's recent report on M2M is quite explicit in this regard: "information transmitted from remote devices is of no value unless it is integrated with the host back-office systems and used to help the organization to become more profitable." [16]

Breaking through M2M's acoustic shadow and fighting the security battle requires full "sensory" development. Any basic M2M system consists of detection, transmission, analysis and response. Whether it is automatic meter reading, alarm monitoring, or GPS tracking, a simple M2M service acts like a reflex that triggers a specific response to a specific stimulus without reaching the level of consciousness, from the sensory neurons to the effector cells. Yet this is not enough – M2M players must take these basic principles and hone them into fully developed networks and systems that can be trusted to remain secure. This requires growth and maturity on the part of companies themselves.

Developing these sense and moving down a path of security growth is really a journey that starts with survival reflexes and hopefully blossoms with what Harvard Professor Robert Kegan calls "Social Maturity" [17]. The point here, of course, is not to discourse on developmental psychology, but to propose a parallel with the ongoing maturing of the M2M industry. The same way we would want to be able to depend on "socially mature" individuals, i.e., those who can be trusted, M2M customers are looking for such partners that can help them move beyond the mere collection of data and provide an environment that is safe while ensuring that they function outside the acoustic shadow.

Beyond The M2M Acoustic Shadow: Opportunities For The Secure Player

The aforementioned market trends delineate the new M2M landscape: fertile, protean and open ground that will yield a wide array of profitable opportunities if an unwavering commitment to tight information security is demonstrated.

The industry is steadily and silently coming of age. Some M2M-related firms at the vanguard of this evolution understand the compelling case to be made to their customers if they can clearly show that secure processes are in place. Consider the strategic intent of some recent acquisitions and partnerships in the space: obtaining the missing links in the value continuum in order to offer end-to-end solutions that can securely and harmoniously mesh with their customers' management systems. It is a marked transformation from the past. Successful M2M companies are moving from data

transport to information creation. Security through and through is the “Open Sesame” of the proverbial next level. It is no longer enough to be fast, extensive, versatile, advanced, and friendly – trust and security are the new prerequisites.

A New Weapon for Information Security: ISO/IEC 27001:2005

Numerex is no stranger to this transformation. We are carrying out a number of strategic initiatives aimed at strengthening our information security coast-to-coast, and offering secure services that facilitate a “safe partnership” with our customers. Our recent ISO/IEC 27001:2005 certification (i.e., compliance with the information security management system (ISMS) standard published in October 2005 by ISO, the Geneva, Switzerland-based International Organization for Standardization) speaks to our commitment to delivering “clean” data. Essentially, this internationally-accepted standard, commonly referred as ISO 27001, gives entities and governments a set of strict criteria that facilitates a solid information security framework. This is not a simple endeavor as it entails compliance within many business aspects such as equipment, software and overall processes. Its adoption is rapidly spreading throughout the world. Well-known institutions or companies such as the World Bank, the United Nations, regional Federal Reserve Banks and major telecommunications operators have been awarded this certification.

ISO 27001 is touted as the overarching or umbrella standard that could harmonize the current, disparate regulatory information security requirements with which organizations in respective geographies and/or industries have to comply. It is favored to become the default IT security architecture. In Japan, ISO 27001 is a basic requirement for public contracts. In the United States, it has been recently proposed in a testimony presented to Congress that the government “lead the drive toward a common global standard for the public and private sector to secure information systems by accepting ISO 27001 as equal to FISMA [i.e., the Federal Information Security Management Act of 2002]. In addition, acceptance of ISO 27001 certification would improve transparency of Federal information security and reduce the bureaucracy and costs associated with current FISMA compliance procedures.” [18]

Of course, ISO 27001 compliance does not guarantee that the certified organization has mutated into an impregnable fortress. It states, however, that a rigorous and careful approach in data handling is followed from end to end. Accordingly, best practices are used and utmost respect and attention are given to ensuring data confidentiality, integrity and availability. However complex the undertaking, there is no other valid option: it is what the M2M customers need, and it is what they should get.

Unlike other management improvements that could tolerate a “second best” position, e.g., formal training that could be replaced by on-the-job experience, information security, by definition, must be as airtight as it can be; with the acknowledgment that perfection in this domain can only be approached asymptotically. As Bruce Schneier, one of the world’s foremost experts in network security, reminds us: “There is no such thing as absolute security” [19]. Human frailty notwithstanding, every effort must be directed towards ensuring an optimal security level for both the service provider and its customers. One must see to it that security is deployed thoroughly and completely. There is no room for half-baked expedients: “The sad truth is that bad security can be worse than no security; that is, by trying and failing to make ourselves more secure, we make ourselves less secure...We deceive ourselves by believing in security that doesn’t work.” [20]

This means that partners, suppliers and other contributors to the business’ activities must be “on board” with a proactive security posture. Service Level Agreements (SLAs) must be drawn accordingly and the security vision must trickle down and be shared throughout the organization.

Back office integration through M2M is predicated upon M2M’s ability to be secure all the way. Financial services, health care and government are examples of sectors that require this type of protected connections. We can already see M2M forces vying for position in those sectors without much fanfare.

One might contend that the demands caused by security issues could perhaps be of little interest to the traditional M2M business such as an alarm monitoring company, indifferent to the attractiveness of integration's promise land. This irresponsible neglect could be lethal. For instance, because the Internet is increasingly used to transmit alarm signals, any related business is inherently vulnerable to network intrusion. There are many forms of attack, among them "the specter of Distributed Denial of Service [DDoS] should be of great concern" [21]. In a DDoS attack, hackers have control of an army of computers on the Internet, which they have infected with bot ("robot") software and which can be directed to bombard a targeted alarm central station with meaningless and paralyzing requests. Once under attack, the station no longer can look after the unsuspecting customer who is now open to all kinds of sabotage and various pernicious actions.

Overlooking the immediate seriousness of the threats posed by hackers, data thieves and other malevolent pranksters is needlessly risky, and, as pointed out in the previous discussion of threats, fecklessly ignores that: "They're already here!" (quite fittingly, the movie buff might recall one of the last scenes of the 1956 original classic movie, *The Invasion Of The Body Snatchers*, in which the local doctor, scared out of his wits, yells in the middle of traffic, "They're already here. You're next! You're next! You're next!").

Whether information security is perceived as a springboard to larger markets, or as a Chinese wall protecting the business integrity, it is becoming a primary strategic consideration in the M2M industry. Unfortunately, it's a consideration that for many is behind the acoustic shadow of the industry's rapid growth and proliferation. Those M2M leaders that are quietly harnessing its resources to do battle with its many dimensions will become an inherent part of their customers' integrated data management.

Sources:

- [1] Ross, C. D., *Acoustic Shadows in the Civil War*, Acoustical Society of America 136th Meeting Lay Language Papers, October 13, 1998, <http://www.acoustics.org/press/136th/ross.htm>
- [2] Avaya Press Release, *Avaya and Lenovo to Provide Customers Enhanced IP Communications on ThinkPad Notebooks*, March 6, 2007, <http://www.avaya.com/gcm/master-usa/en-us/corporate/pressroom/pressreleases/2007/pr-070306.htm>
- [3] In the United States, the following report echoes the same observation: IEC North America 1Q06 Report, *IP Telephony's Dominance of Business Communications Market is Accelerating*, July 2006, <http://www.prwebdirect.com/releases/2006/7/prweb413273.php>
- [4] Singer, Alan, *Internet Protocols Ease Development Cost and Time for M2M Communication*, June 2006, <http://www.rtcmagazine.com/home/article.php?id=100683>
- [5] Kilpatrick, Ian, *Is Machine-to-Machine the Gap in Your Security?* April 2005, <http://www.creativematch.co.uk/viewnews/?90897>
- [6] Hines, Matt, *Carrying the Load for Security – Companies ask providers to take more responsibility for protecting networks*, November 21, 2006, www.eweek.com
- [7] Pulier, Eric, and Hugh Taylor, *Security in a Loosely Coupled SOA Environment*, May 2006, <http://www.developer.com/security/article.php/3605836>
- [8] Cited in AJAXWorld News Desk, *Technology Viewpoint: Is Web 2.0 The Global SOA*, February 17, 2006, <http://webservices.sys-con.com/read/164532.htm>
- [9] Barker, Colin, *Gartner: It's business intelligence 2.0 time*, January 30, 2007, ZDNet.co.uk, <http://news.zdnet.co.uk/software/0,1000000121,39285700,00.htm>
- [10] Bulkeley, William M., *IBM Sets Major Data-Security Project*, Wall Street Journal, November 1, 2007, <http://online.wsj.com/article/SB119388138081578621.html>
- [11] Hines, Matt, *Carrying the Load for Security – Companies Ask Providers to Take More Responsibility for Protecting Networks*, November 21, 2006, www.eweek.com
- [12] Verizon Website, *Verizon Business Completes Cybertrust Acquisition - Surpasses Competition to Become No. 1 Global Information Security Player*, July 09, 2007, <http://www.verizonbusiness.com/us/about/news/releases/>
- [13] Scalet, Sarah D., *Introducing AT&T, Your Internet Security Company*, CIO.com, May 17, 2007, <http://www.cio.com/article/110250>

- [14] Tom Patterson and Scott Gleeson Blue, *Mapping Security: The Corporate Security Sourcebook for Today's Global Economy*, Addison Wesley Professional, 2004, p. 79.
- [15] Cisco 2007 Annual Security Report, December 2007,
http://www.cisco.com/web/about/security/cspo/docs/Cisco2007Annual_Security_Report.pdf
- [16] Cory, Therese, *Wireless Telematics & Machine to Machine – Entering the Growth Phase*, Juniper Research Limited: Basingstoke, UK, November 2006, p. 107.
- [17] An enthusiastic summary of Dr. Kegan's ideas can be found in Dombeck, Mark, *Robert Kegan's Awesome Theory of Social Maturity*,
http://www.adultandchild.org/poc/view_doc.php?type=doc&id=11433
- [18] Paul B. Kurtz, *Federal IT Security: The Future of FISMA*, Testimony before the Subcommittee on Government Management, Organization, and Procurement and the Subcommittee on Information Policy, Census, and National Archives of the House Committee on Oversight and Government Reform, June 06, 2007
<http://www.riskbloggers.com/wp-content/uploads/2007/06/kurtz-fisma.pdf>
- [19] Schneier, Bruce, *Beyond Fear*, Springer, 2006, p. 17
- [20] Schneier, Bruce, *Beyond Fear*, Springer, 2006, p. 14
- [21] Engebretson, David, *Why Security Must Protect from DDoS Attacks*, January 1, 2007,
http://www.sdmmag.com/CDA/Articles/Security_Networkings/BNP_GUID_9-5-2006_A_1000000000000032355