strategy+business

Watching over the Web

by Thomas Künstner, Manuel Kohnstamm, and Stephan Luiten

from **strategy+business** issue 54, Spring 2009

reprint number 09102

booz&co.

Reprint

Watching over the Web

For broadband service providers — and the Internet in general — "digital confidence" pays off.

by Thomas Künstner, Manuel Kohnstamm, and Stephan Luiten

Illustration by Lars Leetaru

The Internet's growth is no longer driven by technology. In much of Europe, more than 70 percent of households have broadband Internet access (along with cable television and wireless access); the same technology is rapidly reaching saturation in Asia and North America as well. No wonder that online advertising is growing at 32 percent per year or that in the business-to-business realm, Forrester Research Inc. estimates Web 2.0–related sales will grow by 47 percent per year, resulting in almost US$5 billion (€4 billion) in growth worldwide by 2013. Moreover, the next-generation networks of digital video and wireless services are expected to accelerate all these trends — at increased broadband speeds, with ubiquitous connectivity, and through many types of devices.

There is a risk, however, that this momentum will founder as the hidden costs and risks of the Internet become more evident. Already, the statistics on fraud, criminal cyber-attacks, and lost business are cause for concern. Twelve percent of Europeans avoid shopping online because of concerns about Internet security. According to Booz & Company analysis, the number of online attacks approximately doubled each year between 2002 and 2005, costing the industry an estimated $1 trillion (€843 billion) in 2005 alone in lost revenue, idle time, repairs, and reputation damage. A separate analysis of Internet scams (in the U.S. in 2007) showed them costing their victims as much as $4,000 each.

In short, for those businesses — and governments — that want to see the Internet fulfill its potential, the single most critical factor is not technology. It is confidence. Digital confidence is the level of trust that consumers place in this emerging infrastructure. Digital confidence is tangible enough that its value can be estimated: In the European Union, for instance, the economic upside amounts to an extra 11 percent growth (about $58 billion or €46 billion) on top of the $550 billion (€436 billion) overall revenue base of the Internet in 2008.

When digital confidence deteriorates, content providers and advertising markets are the most negatively affected businesses. In 2008, in an in-depth scenario exercise for Liberty Global Inc., a leading cable TV company, Booz & Company calculated the difference between "getting digital confidence right" (a best-case scenario for the year 2012) and getting it "wrong" (a worst-case scenario in which many people would curtail their time and activity online because they didn't feel safe). Even in the worst-case scenario, consumers would not abandon the Internet, but they would use it less often and spend less money online. The overall cost in Europe could be $156 billion (€124 billion), or almost 30 percent of the total market at stake — approximately 1 percent of the total estimated European Union gross domestic product. And there would be similar costs elsewhere throughout the world.

In short, for any Internet-based business, digital confidence pays off. That's why many organizations — public agencies, private companies, and not-for-profit groups — have attempted to promote it. But the industry is gradually realizing which organizations stand at the core of the issue: broadband service providers. These telephone, cable, or access companies represent the first line of contact for consumers, typically charging them a monthly subscription fee to connect their computers, entertainment systems, and mobile devices to the Internet.

The senior management teams of those companies are turning their attention to digital confidence. They recognize that they are not just selling access; their customer relationships depend on their ability to provide a reliable and attractive communications marketplace and a medium that is reasonably safe from attack, fraud, and threat. But this type of access has not been easy to deliver, and it will be even more difficult in the future. The complexities are great, and the moral and political issues are tangled and contradictory. Government cannot resolve the contradictions; no matter how enlightened and proactive Internet regulatory agencies may be, regulations in themselves cannot ensure that people trust the online world. Ultimately, the guarantors of digital confidence need to be the broadband providers. And that recognition alone represents a significant step change for the industry. It means that providers will have to see themselves as the critical link in a value chain that includes consumers, the various "suppliers" of Internet services, and the governments in whose jurisdictions the providers operate.

True digital confidence could also transform the way people use the Internet — or, more precisely, it could complete the transformation already begun. Future growth in an Internet-based economy will not be driven by penetration of service; the number of people paying for service is finally approaching a saturation point. Instead, growth in the Internet area will be driven by increases in usage. As people gain the confidence to make more use of online commerce — turning naturally to Net-based software, banking services, catalogs, ticket agencies, publications, music and video download sites, and many more applications to come — the medium will realize its full potential as an enabler of commerce and civilization.

Reasons for Concern

Most people have had personal experience with some form of Internet

Thomas Künstner
(thomas.kuenstner@booz.com) is a partner with Booz & Company's communications, media, and technology practice. Based in Düsseldorf, he focuses on convergence markets and advises top management teams in the communications and media industry on strategic and organizational issues.

Manuel Kohnstamm
(mkohnstamm@lgi.com) is the managing director of public policy and communications for Liberty Global, a leading international cable operator and provider of telephone and broadband services in Europe, the Americas, and Asia/Pacific. He is also a board member of Belgian cable operator Telenet NV and president of the industry group Cable Europe.

Stephan Luiten
(sluiten@lgi.com) is the director of public policy for Liberty Global. He was formerly the director of Brussels-based E.U. public affairs consultancy European Strategy (now Grayling). He has also worked for the European Commission's Directorate General Internal Market.

Also contributing to this article were Booz & Company Principals Michael Fischer and John Ward. This article was adapted from the 2008 Liberty Global report "Digital Confidence: Securing the Next Wave of Digital Growth," by Thomas Künstner, Michael Fischer, John Ward, Martin Brunner, and Florian Pötscher.

abuse or breakdown, but the problems are so complex and interwoven that few people see their full extent and impact. There are, essentially, four categories of concern:

- **Network integrity and quality of service.** These concerns involve the reliability of the technological platform. Criminal attacks can undermine access to the Internet. Viruses and malware (deliberate attacks through the system on end-user devices and local area networks) take a toll that can include not just inconvenience but also large-scale hardware destruction: Consumers Union found that over a six-month period, spyware infections prompted nearly 1 million U.S. households to replace their computers. Even the ubiquitous, low-level irritation of spam e-mail takes a toll; 55 percent of Internet users say spam has reduced their trust in the integrity of their e-mail, and 18 percent see spam as a "big problem." Finally, peaks in traffic load can lead to slow service or weak connectivity, a problem that threatens to grow as more people download and stream video from the Internet. Network providers have known for some time that about 80 percent of Internet bandwidth is consumed by only 10 percent of consumers, and congestion goes up with use of file-sharing and video applications. For example, when the BBC iPlayer was introduced in December 2007, bandwidth usage surged in the U.K., so much so that Internet service providers (ISPs) tried to get the BBC to partially fund the network upgrades they needed.

Growth in an Internet-based economy will be driven by increases not in the number of people online, but in usage.

- **Privacy and data protection.** The safety of consumers' private electronic information — their identities, passwords, and usage profiles, and even the information they post about themselves — must be ensured. People need to feel secure that their private data won't be published inadvertently or without their consent, and that they won't be vulnerable to identity theft, in which criminals replicate or use their private data for fraud. Most social networking sites allow users to limit access to only friends and trusted individuals, but almost half of the consumers on these sites make their profiles available to everyone. The effects of this choice on personal safety, security, and reputation are still uncertain: For instance, as businesses use Web searches to check the validity of job applications, outdated or fraudulent information about a person may show up, with the applicant having no recourse to delete or change it. Organizations also face data risks: In the United Kingdom, the national revenue and customs department had to apologize to customers of investment bank UBS Laing and Cruickshank after losing a computer disk, sent by the bank, that contained addresses and account details of UBS's Personal Equity Plan investors.

- **The protection of minors.** The well-being of those younger than 18 must be defended in the online world. This includes protecting children from exposure to sexually explicit, violent, and otherwise undesirable content; discouraging cyber-bullying and other hostile behavior (such as the posting of demeaning photographs); preventing solicitation of children by adults; and fighting the sexual abuse of children online, including prosecuting the purveyors of child-related sexual content. The extent of this threat is often underestimated, but it is substantial; almost 25 percent of youths surveyed have been exposed to indecent material, and one June 2008 posting in Australia of sexual content involving children received 12 million hits within 76 hours.

- **Piracy and theft.** E-commerce transactions must be protected for all parties. For business and content providers, including video producers, being able to distribute their work safely without fear of copyright violation or theft is a precondition for doing business online. E-commerce services also need protection against consumers' failure to pay or failure to provide agreed-upon goods or services. Users must be sure they are not exposed to criminal prosecution for using legitimate protocols and applications, such as peer-to-peer file-sharing systems.

Piracy and theft can carry immense costs and are difficult to avoid completely. From one country to the next, there is much disagreement about acceptable practices, and great disparity in legislation. At the same time, many individual problems, like phishing (identity theft through online fraud), involve cross-border crimes that require international cooperation to prosecute. Moreover, many of the riskiest aspects of the Internet — such as the anonymity of digital environments and the ability to easily create false identities — are the same elements that enrich digital life and attract participants.

Few regulators can keep up with the speed and scope of challenges in this market. For instance, in the U.K. in May 2008, new laws were announced to close a legal loophole that had unintentionally overlooked drawings and computer-generated images of child sex abuse. Most legal remedies also carry costs; the "three strikes and you're out" rule advocated by content owners to punish copyright violators would require network providers to invest in monitoring and policing activity going through their "pipes." This could lead to a direct overall cost of about $190 million (£130 million) per year in the U.K. alone — in addition to its implications for consumer data privacy. Similarly, just about every "filtering" solution, whether for e-mailed spam or offensive content, also runs the risk of blocking desired content or slowing down the system.

That is why regulators and government agencies are so challenged, and why they often oscillate between heavy-handed, unenforceable rules and a passive philosophy of self-regulation. Commercial firms are thus left to struggle with the same ambiguities. Should a network provider block illegal and undesired Web content, which may mean facing the risk of legal liabilities? If so, who determines what "illegal and undesired" means? Where should the line be drawn? If child sexual abuse content is blocked, what about racist content? And so on.

Four Roles for a Provider

What, then, can a network provider do to lead the way out of this impending crisis? The answer lies not only in meeting legal requirements, but in staying ahead of the curve by adopting proactive policies and practices to drive digital confidence. Case studies around the world show that a "can do" vision is realistic; the answer lies less in technological solutions and more in providers' taking a stand on the role they intend to play. For example, is a network provider merely a conduit, operating the digital highways with no control over content or activity on them? Or can the provider help set the rules for how to travel on these highways — and then help police them?

> The "three strikes and you're out" approach to copyright violators could cost $190 million per year in the U.K. alone.

In reality, network providers have played four different roles on the Internet. They have acted as *teachers,* with no corrective power, educating users about threats and ways to counter them. For example, they may refer patrons to Internet safety information sites like "Web Wise Kids" (www.webwisekids.org) that produce material to help children protect themselves. Network providers have also been substitute *parents,* taking proactive measures to protect users. YouTube thus filters out copyright-protected content. *Referees,* in subsystems where there is self-imposed mutual agreement, help enforce those rules on a case-by-case basis, and often have recourse to real punishment (like removing people from networks). The Dutch cable company UPC NL blocks access to domains that have content with child sexual abuse, using a list provided by the Netherlands police authorities. And sometimes providers play the role of *police,* enforcing mandates with strict rules and some aspect of due process, such as "three strikes and you're out."

Many network providers have learned that no single approach will serve them in dealing with any particular problem. Consider the case of "botnets." These represent a severe form of network integrity infringement for criminal purposes: Personal computers in businesses, universities, and homes are controlled remotely by an unauthorized, malicious third party without the PC owners' awareness. A single botnet can involve as many as several hundred thousand computers. They are used for politically motivated denial-of-service (DoS) attacks, such as the famous attack on Estonia in April 2007 that immobilized the country and the April 2008 attack on Radio Free Europe. They also enable online fraud, and they are responsible for an estimated 80 percent of worldwide spam.

Education is an important measure against botnets: Service providers can teach end-users to safeguard their computers with antivirus and firewall software. But groups that only educate, like Blue Security, a now-defunct small producer of Internet antispam software, are themselves vulnerable to attack. Blue Security was pushed out of business by a massive denial of service attack in May 2006. It is much more effective when service providers combine education with the parent stance — blocking data "packets" associated with botnets — and a police role, usually in cooperation with actual police, to help monitor traffic, trace botnet-related activity, and isolate the servers where the botnet originates.

In the past, the natural role for ISPs has been that of teacher. After all, their core business purpose has been, and still is, to provide a secure, reliable, and powerful network for Internet traffic, without engaging in what happens over its network. This has helped them limit risks and liabilities in areas where they have no responsibility or control — for example, the nature of the content being transmitted.

But consumers are demanding a higher level of trust online. And the payoffs for providing it are becoming clearer. For example, when parents are comfortable with the level of protection provided for their children, they allow them to use the Internet more. When traffic management is robust enough to provide consistent speeds, more people turn to the Internet for videos and entertainment. The extent to which a network operator is able to guarantee a high quality of service and optimal broadband experience for all users is a major competitive edge in infrastructure competition, and playing the role of teacher alone will not be enough. Providers will end up expanding their roles.

When parents are comfortable with the protection provided for their children, they allow them to use the Internet more.

That does not mean taking on a major policing role. Consumers use the Internet precisely because they want choice and interactivity; providers that are too restrictive may risk losing a competitive edge, as consumers seek out alternatives.

The answer is for network providers to see their primary role as providers of digital confidence. This means not just declaring, but internalizing, confidence-building procedures and protocols, and making them part of the organization's culture.

Thus, if you are an executive at an Internet service provider, you need to deliberately choose the combination of roles to play for each area of concern, with an eye toward safeguarding the entire system to which you provide a gateway. As a teacher, for example, start by building customer awareness. Develop well-conceived and continually improved programs on such threats as identity theft, piracy, and online behavior (including addressing bullying, restricting solicitation, and defining what constitutes unacceptable content). Target your messages to specific user groups, including parents and children. Also target business clients with education on spam filters and protection against DoS attacks. Do not delegate this job to other groups; you can partner with others, but you must be seen as the source of digital confidence.

As a substitute parent, provide the tools and resources needed to back up your education — for example, make high-quality content- and spam-filtering software easily available. Even more importantly, be as transparent and consistent as possible in your communications with consumers. Let them know exactly what your policies are, and make sure, if you promote a form of protection, that people at every level of the company understand it and can help consumers adopt it.

As a referee, be prepared to step away from your home ground when you can do so transparently. Contrary to some perceptions, consumers accept restrictions — but only when those restrictions are enforced with clear statements and a consistent, reliable framework. For example, if a consistent, high-quality user experience, without perceptible delays requires active traffic management, consumers will accept that, so long as it is fair and transparent.

And when you take on the policing role, recognize that you cannot act alone. For example, blocking (or reducing the speed of access to) some Internet sites can place a company at legal risk. Only if you are mandated by law to block certain Internet sites owing to content concerns will you be less vulnerable to accusations of infringement of copyright, civil liberties, freedom of speech, and Net neutrality.

The Internet industry as a whole, sooner or later, will have to demonstrate that it is serious about digital confidence by developing coherent solutions. Network operators and ISPs will need to work closely with each other, and with regulators around the world, to build collective confidence in the Internet. They will need to address all areas that clearly fall outside an individual service provider's activity: for example, blacklisting illegal content, enforcing laws against spamming, and preventing large-scale DoS attacks.

The most effective solutions will have the commitment of all players, and they will proportionately allocate the cost of implementation and the resulting financial rewards. Regulators must allow industry to develop such solutions and foster stakeholder cooperation and financial support programs while allowing competitive pressures to work, rather than applying regulation that may be counterproductive from a consumer point of view and may cause economic damage. For example, our analysis shows that a strict quality-of-service regulation banning most forms of traffic management could increase the capital expenditure requirements of network operators across Europe by up to $8 billion (€6 billion).

In the meantime, network operators are increasingly aware that they need to build and invest in their customers' digital confidence to grow new advanced services. Their reputation, their competitive advantage, and the overall growth of the medium depend on it. Nothing, not even their technological edge, is as critical to their future success. ✚

Reprint No. 09102

strategy+business magazine
is published by Booz & Company Inc.
To subscribe, visit www.strategy-business.com
or call 1-877-829-9108.

For more information about Booz & Company,
visit www.booz.com

booz&co.