



Keeping a digital vigil

As online transactions grow and businesses take the digital route, the market for security solutions in India is expected to grow at a rate of 28% from a base of \$291 million in 2007

Archana Rai

Bangalore: India's home-grown start-ups are emerging as potent players in the information security solutions market that was dominated until now by global corporations such as **Symantec Corp.** and **VeriSign Inc.** They have clinched a few contracts from government agencies and business houses in the country, and are looking to expand the market for digital security solutions.

As online transactions grow in India and businesses take the digital route, these new ventures—with help from evangelists and business incubators—are developing unique data protection and recovery technologies targeted largely at banks and business process outsourcing (BPO) firms.



Do-it-yourself test: (from left) iViz Techno Solutions co-founders Nilanjan De and Bikash Barai and iViz director Reuel Ghosh. Photograph: Indranil Bhoumik/Mint

Founded in 2005 at the Kharagpur campus of the Indian Institute of Technology, **iViZ Techno Solutions Pvt. Ltd** has developed the world's first artificial intelligence-based tool that simulates an intelligent human hacker. "Conventional penetration testing products can be a very messy affair," says Bikash Barai, co-founder and CEO, iViZ. "At iViZ, users have to just log on to our website and schedule a test on their own."

Another start-up, **Aujas Networks Pvt. Ltd**, focuses on the \$17 billion (around Rs72,760 crore) global management security services market with four

distinct lines of service, ranging from software application security, identity and access management to helping corporations identify and buttress vulnerable points in their networks.

International Data Corp., or IDC, which tracks the information technology (IT) sector, estimates that the market for security solutions in India—which includes security appliances, software and services—will grow at a rate of 28% from a base of \$291 million in 2007—at a time when the market for such devices is slowing in developed markets.



Managing solutions: (from left) Aujas Networks co-founders Sameer Shelke, Srinivas Rao and Manjula Sridhar. Photograph: Kiran/Mint

It is a view echoed in a report by the Asia Pacific Research Group—a research firm which tracks information and communication technology trends in the Asia Pacific—that rates China and India as the fastest growing markets for information security solutions, with a combined industry segment that is expected to be valued at \$1.2 billion by 2012.

“Securing the digital infrastructure is now a business driver for all Indian corporations as the threat to information security rises,” says Vishal Dhupar, managing director, Symantec Software

Solutions Pvt. Ltd, the Indian arm of Symantec Corp. He says an inability to secure information can have a severe impact on business credibility.

The banking sector typically uses digital security to maintain competitive advantage, build brand image and, most importantly, meet statutory regulations.

“Irda (Insurance Regulatory and Development Authority) regulations are required to be met, and can be effectively managed by having a comprehensive security system,” says Ravishankar Subramanian, director of IT and corporate services at **ING Vysya Life Insurance Co.Ltd**. The company uses a digital security system with software drawn from various vendors such as Symantec, **McAfee Inc.**, **Cisco Systems Inc.** and **Checkpoint Systems Inc.**

It is always a cat and mouse game in the world of digital security, with new challenges emerging constantly.

Shekhar Kirani Vice-president, VeriSign Services India This is a space that other start-ups, such as Bangalore-based **Paladion Networks Pvt. Ltd**, are also eyeing. Focused on the IT security services market, Paladion’s major customers include banking and financial institutions as well as IT and IT-enabled services firms. “We took some time to build momentum, but in the last three years, we have posted a year-on-year growth of 300%,” says Rajat Mohanty, CEO, Paladion, citing the company’s presence in Deloitte Top 50, the annual listing by Swiss consulting organization **Deloitte Touche Tohmatsu** that identifies the top revenue grossers in the start-up arena.

Although the start-ups say it is too early to talk about revenues and profits, they are happy with the way the order books are being filled up.

Hyderabad-based **Synoro Technologies Ltd**, a four-year-old firm, recently won an order for communication security chips from the government of India (GoI). "Just the GoI alone has an outlay of Rs4,000 crore for this programme," says Rajkumar K., director of Synoro, which plans to tap the global market for its product. Rajkumar, however, declined to name the ministry.

In India, top users of Brahmastra, the code name that iViZ uses for its penetration testing product, include media houses such as the Times Group, Web18 (the Internet venture of the Network18 group), television news channel CNN-IBN (owned by **Global Broadcast News Ltd**), credit rating agency **Icra Ltd**, and the Indian defence sector. The product, which can determine security threats in any network and suggest remedies, is being used by more than 30 e-commerce, banking and financial institutions.

Synoro's hardware appliance can provide encryption facilities for a host of digital communication modes. "Our communication security technology is distinctive in that it offers a choice of ciphers (algorithms) that can address sensitive issues such as homeland security," says Rajkumar.

"Earlier, it was enough for firms to secure themselves from threats on the outer ring of their networks. Now, with increased mobility and work-at-home options, security threats are more at end points, of individual users," says Bhaskar Bakthavatsalu, country sales manager, **Check Point Software Technologies Ltd**.



Mobile transactions: Abhijit Bose, vice-president, JiGrahak Mobility Solutions. Photograph: Hemant Mishra/Mint

That is one security gap that mobile commerce enabler **JiGrahak Mobility Solutions (P) Ltd** has tried to bridge with "ngpay"—a mobile money transfer platform that allows transactions over GPRS-enabled handsets. "We released the ngpay platform to the mass market after a one-year beta (testing) to ensure performance, reliability, security, and scalability," says Abhijit Bose, vice-president of the Bangalore-based start-up. Ngpay boasts an application layer security with 128-bit encryption provided by VeriSign and Paladion. "Security audit firms, including Paladion, have rigorously tested and certified

ngpay's end-to-end security," he adds. HDFC Bank uses ngpay to offer financial transaction facilities to customers over the cellphone.

Currently, threats to corporate email security centre around spam or junk mail, phishing—where fraudsters fish for personal information—and viruses that range from being a mere nuisance to malicious ones such as Trojans, which appear as legitimate files.

In India, one in every 30 emails is listed as spam by Internet security firm

MessageLabs Ltd. Security solutions from global companies span identity and access management to data-leak prevention and one-point solutions such as unified threat management appliances, all of which, say security experts, are considered “hot” in the Indian market today.

“The Indian security services market is driven by the increased sophistication of threats and complexities in IT infrastructure,” says Praveen Sengar, senior analyst, software and services, IDC India.

The IT sector is another major user of digital security systems. Product engineering firms, such as **Aztecsoft Ltd**, have adopted ISO 27001 compliance norms, and regularly conduct risk assessments and business impact analyses. “We use digital security products and services from a host of providers such as **Microsoft Corp.**, Cisco, **Blue Coat Systems Inc.**, **Trend Micro Inc.**, McAfee and **Websense Inc.**,” says N. Nataraj, chief information officer, Aztecsoft.

Topping the list of digital threats Indian firms currently face are Zombies—personal computers (PCs) in diverse locations controlled by hackers through files which appear legitimate but are actually computer viruses that hijack a firm’s IT backbone. Targeting specific entities, these Zombie PCs are networked and used to send thousands of messages.

A BPO firm, which did not want to be named, was recently the target of an extortion threat by these Zombies, with its IT network threatening to crash under the weight of unwanted traffic.

“It is always a cat and mouse game in the world of digital security, with new challenges emerging constantly,” says Shekhar Kirani, vice-president of VeriSign Services India Pvt. Ltd, the Indian arm of the US-based firm, which provides digital security solutions such as secure certification of websites and identity verification.

Along with the BPO sector, domestic businesses, too, are looking to grow their online offerings as more Indians transact on the Internet. And as e-commerce grows, so does the need to police the digital network. Despite the global investment in bolstering information security, incidences of breach in digital security worldwide are growing by 300%, according to Cert—the computer emergency response team at Carnegie Mellon University that coordinates Internet security issues.

“The most important aspect of online security is for customers to know that payment gateways on online shopping sites are secure,” says K. Vaitheeswaran, co-founder and chief operating officer of Indiaplaza.in, an online retail company. “We now use a 3D (three-dimensional) secure system that takes customers directly to the bank website. Once that payment is authorized by the bank, we process the order,” says Vaitheeswaran, who feels that a customer is far safer using a credit card on a secure online website than using it offline. Indiaplaza.in uses 128-bit encryption for all payment transactions; in addition, it is authenticated by VeriSign.

“Indian businesses increasingly rely on technology to reach out to staff, partners and customers. Securing this organizational information and the systems that are used to manage and transmit such data is a high-profile function,” says

Symantec's Dhupar. The firm operates a 24-hour response laboratory in Pune that monitors online information security threats on a real time-basis.

Symantec gathers data from more than two million decoy email addresses, 150 million desktop anti-virus sensors, and 40,000 intrusion-detection and firewall sensors worldwide. "We deal with an average of a few hundred threats every day," says Shantanu Ghosh, vice-president, India product operations, Symantec.

All this action has seen venture capital funds pumping in money to fuel new ventures in this niche space. In December, **IDG Ventures India** invested \$3 million in iViZ. Three months later, it invested another \$3 million into Aujas, which had its origin in an entrepreneur-in-residence (EIR) programme set up by IDG Ventures.

EIR programmes are led by experts in a particular domain and perform due diligence on potential deals.

Six-year-old Paladion had earlier raised seed funding from **Nadathur Holdings and Investments Pvt. Ltd**, the investment firm started by N.S. Raghavan, a member of the founding team of **Infosys Technologies Ltd**.

"We were passionate about the managed security services space and were very keen to fund a company in that spot but, as there were no ready business plans, we set out to build an EIR programme," says Sudhir Sethi, chairman and managing director, IDG Ventures India, who leads a team that is managing a corpus of \$150 million for early-stage venture capital investment in India.

Paladion currently earns about 35% of its revenues from the Indian market, and aims to build a global footprint. Aujas, too, has similar plans. "We expect education and training, which is our consulting arm of the business, to be a significant revenue contributor here," says Aujas co-founder M. Srinivas Rao, who expects his firm to initially derive more than half its revenue from the Indian market. It is, clearly, boom time for companies in the digital information security market.