



The Insecure Enterprise

With cyber criminals offering ‘fraud as a service’ and malware factories churning out malware designed to steal information, the threat perception for Indian enterprises has escalated to a new level, as organized crime syndicates take over from script kiddies

By [Srikanth RP](#)

[More from this author](#)

- In February 2009, local newspapers reported that the Ministry of External Affairs was examining a security breach on its computer network, after some computers were found to be infected with spyware, which was sending copies of information to an external e-mail address
- In March 2009, Websense Security Labs discovered that the official website of Rajshri Productions, India, had been compromised and was infecting the machines of site visitors with malicious code
- In August 2007, the website of one of India’s leading banks, Bank of India, was hacked, and was found to be distributing malware and Trojans to visitors. In the same month, Websense Security Labs discovered that the official site for Syndicate Bank was compromised with a malicious script
- In December 2006, Kingfisher Airlines was hit by an online e-ticket fraud that cost the airline Rs 17 crore
- CERT-In, the Indian Computer Emergency Response Team’s website, reveals that a total of 4,475 Indian websites were defaced in the year 2008.

What do the above incidents tell us? The fact that even after following the best security mechanisms, all a hacker has to do is to find a single open door or a minor exploit for breaching a network. KK Mookhey, Principal Consultant, Network Intelligence India, rightly sums this up as an asymmetric warfare: “The attacker has to find only one loophole, while the defense has to plug all loopholes.” With multiple threats ranging from Zero day exploits, website vulnerabilities, unpatched software and an ever-growing insider threat, enterprises cannot afford to blink their eyes even for a moment.

Clearly, even as the Internet has leveled the playing field for Indian enterprises, it has also exposed the vulnerabilities of Indian enterprises to global hackers who do not differentiate between boundaries. For example, the Bank of India hacking incident was traced to an ISP in Russia.

Emergence of Fraud-as-a-Service

While, in the past, Indian enterprises needed to guard themselves only against virus attacks and hackers who hacked for fun, today, the same enterprise has to ensure multiple layers of defense against sophisticated attackers whose only motive is profit. Says Vikas Desai, Lead Technology Consultant— India and SAARC, RSA Security, “Earlier fraudsters used to hack for thrill, now it’s a professionally run organized crime for financial gains.”

Desai says that in the next few years, threats will grow both in depth and breadth. Virtual and cloud ecosystems have the possibility of being the new breeding grounds for fraudsters, while threats will become more sophisticated. “We can expect a build-out of the fraudster supply chain—the fraud-as-a-service business model, and an increase in automated attacks.”

The change in motive can be seen from the fact that while hackers were earlier content with defacing a website, they are now targeting users of legitimate popular sites. One popular tactic is SQL Injection, wherein hackers inject malicious code into the website by exploiting a security vulnerability in the database layer of an application. Whenever a user visits such a website, the malicious code is downloaded to the user’s computer. Gradually, the hacker gains control of all the machines infected with this code, and succeeds in creating a botnet used for sending out spam mails or even personal information stored in personal computers.

Says Sunil Rawlani, Executive Vice President and Head, IT, HDFC Standard Life, “Over the years, the nature of attacks has progressed. From networks, the target moved to stealing data. But a step after this is even more insidious: the malicious modification of data—which is making a difference.” In a networked economy, this can have disastrous implications.

The transformation of the nerd into a well-organized adversary, is best summed up by Jim Motes, Chief Information Security and Privacy Officer, Perot Systems Corporation, “Technological advancement, ubiquitous transfer and storage of proprietary corporate information, customer personal and financial data, industry intellectual property, and government technology have led to an evolution of the ‘hacker’ into educated, well-paid, technically proficient individuals sponsored by nation states and organized crime.” The recent Symantec Global Internet Security Threat report mentions such an example, wherein it highlights the role of the Russian Business Network (RBN), an underground professional organization that specializes in the distribution of malicious code and hosting of malicious websites. The RBN has been credited with creating approximately half the phishing incidents that occurred worldwide last year.

Amit Nath, Country Manager, India and SAARC, Trend Micro, corroborates this fact, and says that cybercrime has become a flourishing business: “With the increasing use of Web 2.0 technologies, virtualization and a growing internet population in 2009, we will see a lot more information stealing malware geared towards stealing personal data, login credentials and credit card data.”

India – A Magnet for Spam and Phishing Attacks

India is clearly the center of attention, and has seen a rise in phishing attacks, with several Indian banks sending out advisory notes to their customers, cautioning them against revealing personal information related to their accounts. Phishing, which is the art of masquerading as a trusted entity to acquire sensitive information, is gaining significance as a preferred method for fraudsters.

Says Vishal Dhupar, MD, Symantec India, “In the last year, Symantec observed over 600 phishing URLs with IP addresses hosted in India. Many Indian companies, from banks to airlines

and retailers, were the targets. Over 1,000 unique phishing attacks occurred on reputed Indian banks during the past year alone.” Dhupar also points out another interesting fact: India has retained its place among the top countries of origin for spam, across several months. Symantec’s ‘State of Spam’ report for April 2009 showed that India is only behind the US and Brazil in sending out spam messages. This threat takes on a more dangerous dimension when you consider the increasing link between spam and malware.

With spam being the cheapest method to spread information, both analyst firms and vendors believe that call-to-action spam will be the main delivery mechanism used by fraudsters. Last year, specific to India, Symantec observed that malicious activity in the form of worms, viruses and Trojans was on the rise. More than 65 percent of malicious attacks in India was through worms, as compared to the global average of 22 percent. The most recent example is the Conficker worm, which has infected millions of computers worldwide. Malicious code propagation vectors like file sharing/executables were behind the high proliferation of viruses in India. The firm also observed that rampant software piracy in India aided the spread of malware by the file sharing/executables mechanism. In fact, the widespread use of pirated software in India and China was attributed to the large number of computers infected by Conficker in these countries.

Threats Grow in Sophistication and Intent

While viruses are still rampant, they are not the topmost threat. Says Rajendra Deshpande, CTO, Intelenet Global Services, “Security threats to organizations have moved beyond virus and worm attacks and progressed to infrastructure misuse, information theft, phishing, malware, DoS and DDoS attacks.”



In a declining economy, threats have grown manifold as enterprises face intellectual property theft from both insiders and outsiders. Experts such as Desai of RSA, believe that as companies reduce their workforces, insider threats are more probable than ever before. Competitors too are waiting for such opportunities to steal product designs or other forms of intellectual property. This is corroborated by an FICCI-PwC report on security in India, which states that corporate espionage has emerged as one of the leading threats, with 14 percent of the organizations attributing security incidents to competitors.

With profit being the only motive, the mantle has passed on from the script kiddies to the organized crime masters, who have the capability to run specialized operations. The other danger is the fact that with no precedence, the new threat is that of harboring potential cyber terrorists, who look respectable in society, but use their knowledge for wrong means. Navin Agrawal, Executive Director, KPMG Advisory Services, sums up this growing threat for Indian CIOs, when he says, “This is the age of corporate cyber espionage and there is big money involved. There is a generation coming along, which is smooth, well-trained, and also smart enough to hide their real intentions.”

This is supported by the FICCI-PwC report, which states that majority of the organizations which participated in the research study believed that employees or former employees are a major source of security threat. Almost 47 percent of the organizations surveyed believed that employees were responsible for security incidents and 25 percent attributed them to former employees. Only 39 percent companies attributed negative security events to external hackers.

Rawlani of HDFC Life Insurance says that data leakage by employees and partners is a major threat for every enterprise, and organizations need to identify and place appropriate controls to prevent such leakages. In this context, identity, access management and end-point security solutions are crucial in managing these issues.

Even as vendors modify their security techniques to detect new viruses or malware, malware creators are also developing new variants that have the capability to evade scanners. The Conficker worm is such a variant that has consistently been reinvented by its creators. For instance, it copies itself to removable media drives in a way that forces code execution. Manjunath Kashi, Director, Enterprise Computing group, Unisys, shares an interesting insight on 'Conficker': "The new variant of Conficker worm created secure infrastructure for cyber crime, allowing its creators to remotely install software on infected machines. The worm is used by the creator to develop a botnet that is rented out to criminals who want to send SPAM and steal IDs. The worm directs users to online scams and phishing sites."

With organized criminals taking over from nerds, threats have become more refined and customized. Elaborating on the challenges faced by Indian CIOs, Murali Venkatesa, Product Specialist- Security Services, Sify Technologies says, "Today the biggest challenge faced by organizations is the evolution of Zero day exploits and threats. Security is a moving target and its mitigation requires continuous attention and action."

Mobility, Virtualization and Social Networking Present New Issues

While organizations have given employees laptops and smartphones as a means to improve their productivity, this also presents immense risks, as these devices carry critical business information. However, what is shocking is that data on most of these devices is not encrypted. This can be a security disaster that is waiting to happen.

To prevent the misuse of data in case a laptop or device is stolen, some organizations have made it a policy decision to encrypt data. Says Anita Pai, Executive Vice President, Customer Service and Technology, ICICI Prudential Life Insurance, "We have taken adequate steps at a policy level to encrypt our data. This is applicable for data in transmission, as well as for information residing in laptops or smart devices."

2008 Rank	2007 Rank	Item	2008 Percentage	2007 Percentage	Range of Prices
1	1	Credit card information	32%	21%	\$0.06-\$30
2	2	Bank account credentials	19%	17%	\$10-\$1000
3	9	Email accounts	5%	4%	\$0.10-\$100
4	3	Email addresses	5%	6%	\$0.33/MB-\$100/MB
5	12	Proxies	4%	3%	\$0.16-\$20
6	4	Full identities	4%	6%	\$0.70-\$60
7	6	Mailers	3%	5%	\$2-\$40
8	5	Cash out services	3%	5%	8%-50% or flat rate of \$200-\$2000 per item
9	17	Shell scripts	3%	2%	\$2-\$20
10	8	Scams	3%	5%	\$3-\$40/week for hosting, \$2-\$20 design

Goods and services available for sale on underground economy servers

Source: Symantec

Virtualization, the new favorite of Indian CIOs, is increasingly being adopted by enterprises to cut costs, through consolidation of servers. However, virtualization makes security more complicated because it introduces another layer that must be secured. When there are multiple virtual machines running on a hypervisor, a compromise of the hypervisor can compromise all those machines. Explains Rawlani, "The easy portability of virtual images presents a security issue. With modern virtualization technology, virtual machines can be easily cloned and installed

to a different physical machine. The ability to go back to ‘snapshots’ of past images can inadvertently wreak havoc with patch management.”

In the case of thin clients, since all applications run on the server, one successful break-in can expose an organization to more confidential information, than say a PC attack. Says Ratnesh Sharma, Director, Product Management and Marketing, Citrix R&D, India, “A man-in-the-middle attack can be done on a thin client, as it cannot figure out whether the server it connects to is an authentic or a spoofed malicious server.” Sharma says that, as the server is the central point of failure, organizations need to follow a bottom-up security procedure for server security. This must start with hardened physical security around server infrastructure, followed by network or communication security.

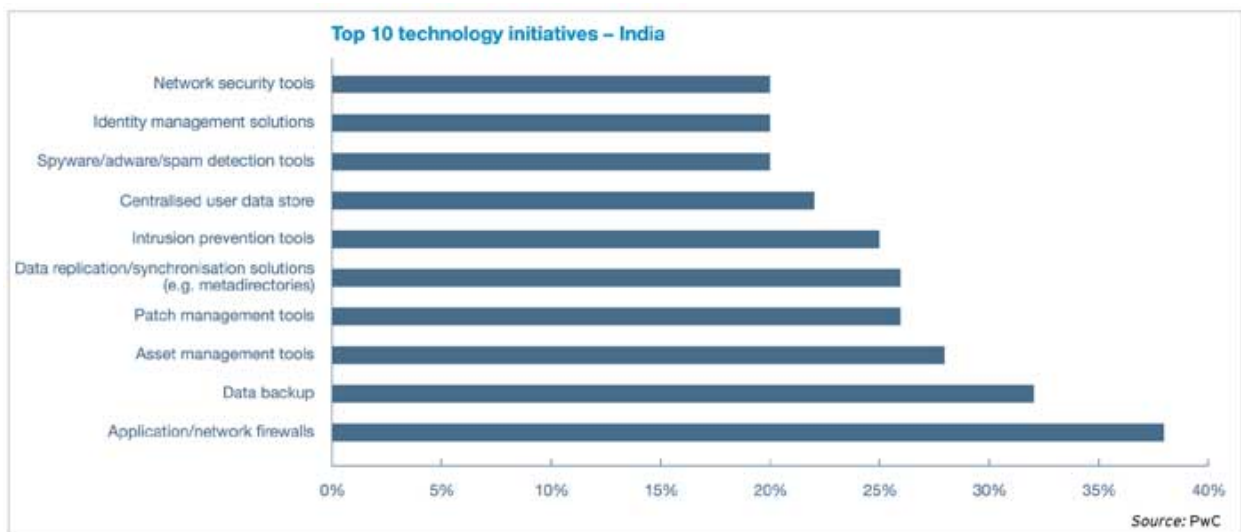
As more applications move to the cloud, security-related aspects will be put to the test, as more and more access points increase management challenges. In this context, Rawlani asks a question that is perhaps playing on the mind of every CIO today, “Cloud computing means we will all use inexpensive terminals to access our resources that are located someplace ‘out there.’ But when the data is ‘out there,’ how can anyone be sure that it’s protected from everyone else ‘out there’? In fact, the biggest obstacle to moving to the cloud, for many companies and individuals, is the security question.”



Cloud computing also highlights perceived issues that CIOs have in terms of data loss or data theft. Says Navin Agrawal, Executive Director, KPMG, “The key threats are in terms of security of data at rest, compliance requirements due to outsourcing of data, recovery of data across the cloud in the event of an issue, and support for investigation of data within the cloud.”

The Antisocial Element of Social Networking

Social networking sites, which have become so popular with youngsters, are a nightmare for CIOs – especially when it comes to ensuring security. Says Rawlani, “Web 2.0 technologies when combined with our ‘work-from-anywhere’ lifestyle have begun to blur the lines between work and private life. Because of this psychological shift, people may inadvertently share information their employer would have considered sensitive.” This is still a grey area for many CIOs, who are grappling with addressing the challenges of preventing confidential information-sharing by employees.



Traditional tools fall short of this aspect, as this requires solutions, with the ability to appropriately classify content. Manish Bansal, Marketing Manager, Websense Software Services India, raises an extremely pertinent point, when he says that Indian organizations have to start looking beyond the traditional solutions, as employees themselves are no longer restricted by boundaries. Says Bansal, “In the Web 2.0 world, effective protection requires the ability to analyze Web content in real time to recognize threats and inappropriate content ‘on the fly’, even content that has never been classified before.”

Locking the Door But Leaving A Window Open

With the advent of Zero day exploits, and attacks coming in from a variety of sources and media, enterprises have to move beyond the notion of just firewalls and antivirus solutions. Says Govind Rammurthy, CEO and MD, MicroWorld Technologies, “Indian enterprises are still ignorant about the importance of security solutions. Having an antivirus solution or firewall will not suffice, as almost everyday there is a new threat emerging, making the software deployed by the enterprises vulnerable to attacks.”

While organizations in sectors such as banking and IT pay more attention to security, due to regulatory norms and customer requirements, organizations in other sectors are far behind. Says Chandrasekhar Balasubramaniam, Country Manager-Infrastructure Risk Management Services, IBM India, “Most Indian CIOs do not look at security in a holistic way, and end up buying point solutions. This trend is seen more among SMBs—most of whom are not knowledgeable enough to understand the importance of looking at security in a holistic manner.” Balasubramaniam says that unless Indian organizations have proper processes, controls and policies in place, security breaches will continue to happen. However, Indian enterprises are realizing the strategic importance of security, and are outsourcing their security-related requirements to firms such as IBM, who provide managed security services. To encourage adoption, IBM is even offering its clients a money-back policy, if the client organization is compromised by a security threat.

The notion that security is confined to certain limits is gone today since the perimeter, as it existed earlier, is non-existent today. This makes most traditional approaches to security look irrelevant. Explains Sivarama Krishnan, Executive Director, PwC, “As businesses in India open their applications and networks to customers, suppliers, partners and remote users, they open themselves to a myriad of threats and vulnerabilities that the ‘hard outer shell’ can no longer address.” The biggest challenge that these firms face is in ensuring seamless security by combining solutions across people, processes and technology.

While most companies have well-documented security policies in place, the gaps are present in execution. Agrees Murtaza Bhatia, National Manager, Professional Services Security and iBOSS for Datacraft India, “Security controls are difficult to implement and once implemented, are even more difficult to maintain. The addition of mobility and wireless infrastructure has added oil to this burning issue.”

The most common mistakes in security include using default or weak passwords, and not updating patches regularly. For example, the key reason why Conficker spread so quickly was due to a vulnerability that Microsoft patched in October 2008. However, as organizations did not keep their software updated, the Conficker worm took advantage of the vulnerability, and ended up infecting close to 10 million PCs. Proactive security management is another area where Indian enterprises have huge gaps to fill. Most firms have robust policies, but if they are not properly implemented, the impact is lost. Navin Agrawal of KPMG, points out the example of an Indian organization, where in the absence of proactive



monitoring, a firewall rule on an internal machine that was created for temporary web server access, was kept open.

Another big area which most organizations are not paying heed to, is in the area of application layer security. Says Ajay Soni, Vice President, IMS, Patni, “With application development being more focused on design, security aspects such as access control list (based upon segregation of roles as well as interfaces between applications) are only partially checked for information security issues.” Soni says that vulnerabilities arise as the functionality of the application undergoes customization, and is different from the environment in which it was originally conceived. More importantly, he says, that at times, his firm has observed that as soon as the application is released, the application goes into an extraordinarily hostile environment.

Towards An Integrated Model

While in the past, a major percentage of Indian organizations looked at piecemeal point-to-point solutions, today, the trend is slowly shifting to an integrated model. Says Subashini Prabhakar, Chief Technology Manager, Dax Networks, “The Indian security market is undergoing a paradigm shift evolving from the product to the service model. Businesses are also turning to Unified Threat Management (UTM) devices rather than standalone systems because of their capabilities to address multiple threats, as well as for the tangible benefits of reducing costs and improving efficiencies.”

Due to the low cost of maintenance and deployment, integrated devices have seen good acceptance among Indian enterprises. Agrees Sanjay Virnave, President-Sales, Tulip Telecom, “There has been a surge in the adoption of integrated threat management solutions as it is a comprehensive approach to network security that addresses multiple types of malware, blended threats and spam.”

The demand for integrated threat management solutions can be seen from the sales of UTM devices from vendors such as Elitecore Technologies and Fortinet. For example, Elitecore has more than 1500 clients today in India, for its UTM product, Cyberoam. While a bulk of its clients are from the SME segment, it also counts among its clients, names such as Asian Paints, Mudra Communications, Angel Broking and Hero Honda.

Says Tushar Sighat, Vice President-Operations, Elitecore Technologies, “From our own research, we have observed that point solutions such as firewalls are not experiencing growth. Our success in this space shows that SMEs want an integrated solution, which is simple to use and maintain.” The firm’s flagship product combines features such as intrusion prevention, antivirus, content filtering, firewalls and bandwidth management in one device—which translates into a lower cost of ownership. A case in point is Gujarat Alkalies and Chemicals Limited (GACL), which wanted a single solution for its security, productivity and connectivity needs. The firm chose a UTM appliance from Elitecore, and used it to block spam and viruses, besides using it for prioritizing bandwidth to users.

While SMEs may be driving the UTM market in India, large enterprises are also gradually realizing its immense value. Says Vishak Raman, Regional Director, India and SAARC, Fortinet, “In the current economic environment, we are seeing a number of enterprise customers adopting UTM devices for the high ROI and value. Today, nearly two-thirds of our customer base is made up of carriers and enterprise customers.” In India, the firm has clients such as GMR Group, TAFE, and Cambridge Solutions.

For customers who do not want to consolidate their security-related requirements in a single device, firms such as Fortinet are offering customers the flexibility to later add more

functionality by just turning on the features in the device rather than having to purchase new solutions.

The move towards integrated security can also be seen in the strategies of firms such as Cisco and Juniper Networks, which have embedded security-related features in their networking devices. Says Mahesh Gupta, Business Development Manager—Network Security, Cisco India and SAARC, “A self-defending network can help enterprises identify, prevent, and adapt to both known and unknown security threats.”

Similarly, Juniper Networks has a solution called the ‘Adaptive Threat Management,’ which is meant to overcome all the weaknesses associated with point tool-based network security architecture. Says Sanjay Jotshi, Director of Enterprise and Channels, India and SAARC, Juniper Networks, “Enterprises today need an integrated set of tools that link networking and security solutions together to prevent, detect, monitor, and react to ever-changing security threats. Adaptive threat management architecture can adapt to changes in the threat landscape based upon rules and policies.” Jotshi claims that when the architecture senses an attack in one area of the network, it can adapt by strengthening access policies in another. “Network elements, security policy engines, and enforcement points all coordinate together to monitor, enforce, and audit security policies,” Jotshi says.

Integrated solutions are also vital for preventing data loss due to security-related incidents. Current Data Loss Prevention (DLP) offerings are available as integrated solutions that protect confidential data wherever they are stored. DLP solutions leverage a common foundation with the same policy management, detection, incident response workflow, and reporting capabilities across network, storage, and endpoint systems. Explains Dhupar of Symantec, “A unified approach to enforcement enables the organization to write a policy once and automatically enforce it throughout the enterprise.”

Security – A Moving Target

In an age where threats are dynamic in nature, and attackers are using creative methods to get past security systems, it is vital that organizations step up their level of alertness. In domains such as IT and healthcare, this is even more crucial. For example, at Omega Healthcare Management Services, an offshore provider of healthcare revenue management solutions, the IT team has set up controls at multiple levels which start from end points to the gateway level. Being an HIPAA compliant organization, the organization has to take extra care to protect health-related information. “I constantly tell my security team to think like a hacker. It is imperative that we shift our primary focus on internal security breaches rather than always looking at our firewall to protect our network,” says Kamalraj Chandrasekaran, Associate Vice President – Technology, Omega Healthcare Management Services.

The seamless combination of security controls that encompass people, process and technology is a must today, and any gap in any of these elements can lead to a security breach. Most organizations make the mistake of viewing security only as a technology issue, and end up paying for it. “Security is more than passwords and lost devices. Above all, it means creating an internal culture of responsibility. As more workers leave the physical confines of their company's premises, the devices they use expand the boundaries of the corporate network, making it a challenge for the CIO to ensure application security,” says Saurabh Sanghoo, Head, Consulting and Solutions Integration, Orange Business Services, India. It is apparent that until all stakeholders in the process take complete ownership for security, gaps will be imminent.

Sanghooe says that for sectors such as the BFSI segment, where information security is extremely critical, organizations must go beyond the usage of the standard username and password mechanism. He says, “For such environments, authentication applications such as biometrics, fingerprints, and the use of a token key or smartcard, will help create an additional layer to confirm the authenticity of each user. Automatic deactivation of e-mails when an employee quits and auto-rotate passwords are other measures that would prevent a breach of security.”



While new technologies that promise to provide complete security will always look attractive, it is important to focus on the basics. Says Anita Pai of ICICI Prudential Life Insurance, “Simple things like ensuring that employees use their access cards without fail, reviewing CCTV footage on a regular basis, or deciding how one gets access to information, can go a long way in ensuring security.”

In conclusion, security must be treated as a journey, and not a milestone, as organizations need to continuously evaluate and modify their policies on a regular basis, to ensure that they remain secure in today’s world which has no boundaries.