

MARCH 2010

INDIA HIT BY A DOUBLE WHAMMY

PUNE & SILDA ATTACKS PROVIDE A WAKE-UP CALL

SHOCK AND AWE: SECURITY TRENDS FOR INDIA

- Providing Complete Security Solutions a Challenge
- Need for More Integrated Solutions
- Traditional Security Solutions Will Become Obsolete
- Corporates become Dark-Cloud-Aware
- Data Loss Prevention to Protect Information
- Security for Cloud and Virtualised Environment
- Antivirus is Not Enough



Tackling Terrorism and Naxalism Head-on

Reform institutions & systems to pre-empt terrorist threats



Redefining Web-Based Video Surveillance

High quality video over the web at a low bandwidth



Best practices for protecting data

Firewalls in a Web version 2.0 world



Managing the Mobile Enterprise

Unprotected mobile devices could lead to data loss



CERT-In – Securing India's cyber space

Responding to cyber security incidents



Company Profile: Gunnebo - Securing Businesses

Providing holistic security solutions



Shock & Awe

Security Trends for India

Integrated Solutions – The Way forward

The security industry is seeing great traction as far as system integration is concerned and other technologies such as IP and wireless technologies are gaining greater foothold. According to Anil Dhawan, Senior Vice President at G4S Security Services, and President of the APSA – India Chapter, “There is more of system integration with emphasis on CCTV



Surveillance based on remote monitoring and a lot more demand on security training and explosive detections.” Nilendu Mitra, Senior Vice President. TopsGrup, adds that, “Globally, the professional security industry is now a Rs. 6,75,000 crore (\$ 150 billion) industry and this is the only industry in the world that is “recession resistant” given the growing rate of urban crime and terrorism.” Mitra bets his money on multi-fold increase in anti-social and terror activities, equally in developed and developing countries, will continue to lead the growing demand for the services of professional security agencies.

Also in 2010, Mitra foresees the emergence in the demand for the following new services:

- High-End security solutions consultancy and advice
- High-End security training to various entities of the Government, including the Homeland Security agencies
- Expert help in preparation of security programs for corporates and large projects, planning and writing SOP (Standard Operating Procedures) including protocol, procedures and implementation guideline

With the ever-increasing terrorist events and cyber crimes, the awareness about security devices and the need to be proactive is increasing. “We expect this trend to continue in 2010. Historically, analog cameras and CCTV solutions have been deployed everywhere”, feels Sanjeev Sehgal, Managing Director, Sparsh Securitech. He believes that the trend is towards digital cameras and adding DVR to CCTV solutions.

“Going forward, we believe that software will play an important role. Software features that enable event-based video surveillance, alarms, motion detection and pattern based video recording. Like other technologies, security devices will adopt IP and wireless technologies. However, analogue solutions will dominate for the time being while digital and wireless technologies mature for security application,” Sehgal adds.

“These are times when terrorism and probably a sense of uncertainty are in the air. The focus is not just on security for corporates but even for individuals,” cites Pushkar Gokhale, GM, Sales and Marketing, Godrej Security Solutions.

According to him, the major drivers for security would be the infrastructure development happening across wide sectors viz:

- Mass transport system projects - Railways (metros)
- Airports and seaport expansion projects
- Commercial (retail, entertainment, hotels, and so on)
- Industrial projects
- Banks

Top 10 Countries Producing Spam

Q4 2009		Q3 2009		Q2 2009		Q1 2009	
Country	% of total	Country	% of total	Country	% of total	Country	% of total
US	15.6	US	25	US	25.5	US	35
Brazil	11.2	Brazil	12.1	Brazil	9.8	Brazil	7.3
India	5.6	India	5.3	Turkey	5.8	India	6.9
Venezuela	4.4	Poland	4.5	India	5.6	Rep. of Korea	4.7
Rep. of Korea	3.8	Rep. of Korea	3.1	Poland	4.9	China	3.6
Ukraine	3.7	Venezuela	3.1	Rep. of Korea	4.6	Russia	3.4
Poland	3.6	Turkey	2.9	Russia	2.4	Turkey	3.2
Romania	3.3	Argentina	2.2	Romania	2.3	Thailand	2.1
Germany	2.9	Colombia	1.9	Spain	2.1	Romania	2
Russia	2.4	Russia	1.8	Czech Rep	1.9	Poland	1.8
Total	56.5	Total	61.9	Total	64.9	Total	70

A little more than half of global spam originated in just ten countries

Source: McAfee

- Hotels
- Residential apartments

One can see more budget allocation towards security equipment, and a shift towards overall ‘comprehensive security’. The electronic security market is poised for a strong, robust growth driven by Electronic security products, need for CCTV (Surveillance systems).

Video surveillance has become the key part of integrated security set up. However, in this segment the focus is shifting from analogue to IP based systems. IP and Ethernet LAN-based installations - although expensive - offer advantages such as scalability, flexibility, functionality. Much more features in cameras like day/night, direction control, backlight compensation, motion detection, weatherproof, tamper resistant, audio detection are gaining popularity.

Gokhale believes that the CCTV market is expected to grow at a rate of 25 per cent. The other segment which is growing at a fast pace is ‘screening equipment’, like walk-through metal detectors and x-ray baggage screening machines. This has been a result of the need for screening individuals and belongings at the entry points of public places. One has seen a drastic change in the user profile of x-ray baggage screening equipment, which was earlier restricted to airports. Today, besides the airports, it is seen in railways (metro rails), hotels, public places like malls and stadiums.

Supporting his reading of the industry, Gokhale says that the department of police would turn out to be one of the major buyers of the screening equipment. One of the major events, which will drive the market for these products in the coming year, is the Commonwealth Games.

According to him, “the market for screening equipment is expected to grow at least at a rate of 50 per cent. Another area of growth would be explosive detection and blast containment devices, essentially an after effect of the Mumbai terror attacks.”

However, he feels that, “The market in India does not seem to be ready for security against the CBRN (Chemical



The market for screening equipment is expected to grow at least at a rate of 50 per cent. Another area of growth would be explosive detection and blast containment devices, an after effect of the Mumbai terror attacks

Pushkar Gokhale, GM, Sales and Marketing, Godrej Security Solutions

Biological Radioactive and Nuclear) threats in the short run, though eventually one would reach a point where one would have to face CBRN threats.”

Meanwhile, Vinay Vashishta, CEO, RBH India again backs integrated solutions as an emerging trend in 2010. “Clearly,” he says, “products which can do total alarm management in single unified form with a strong control and command software is catching up fast. Most of solutions are stand-alone even if it is integrated; it becomes a part of Building Management System where it serves just as a building facility and not a proactive security system.”

Security for cloud and virtualised environment

Can the security industry be complete without an IT perspective?

Vikas Desai, Lead Technology Consultant, India & SAARC, RSA, the security division of EMC, anticipates security spending in 2010 to continue to be strong in India and



more targeted to also address security risks that come with deployment of new technologies within enterprises.

Quoting an IDG research commissioned by RSA in April 2009, it was found that 73 per cent of top IT security decision makers surveyed across the globe reported increased usage of virtualization technology, personal consumer mobile devices and social networking platforms at their companies. Also, just under one-third (31 per cent) of the respondents’ companies are already leveraging the cloud, while 16 per cent have plans to migrate applications and processes in the following 12 months. Among these respondents, a significant two-thirds (66 per cent) do not yet have a security strategy in place.

Desai anticipates remarkable changes in this area in 2010. “We can expect more and more organizations taking a slow and steady approach in leveraging cloud computing and virtualization in 2010. Less critical applications will be migrated to the cloud, and more sensitive company information will continue to reside in local servers. Authentication will also be an imperative measure to ensure that information in the cloud or a virtualized environment does not land in the hands of non-authorized users or fraudsters.”

Issue of Data Loss Prevention

According to Desai, “The hardest risks to detect within an organization are those that are posed by its employees and other insiders.” RSA defines ‘Insider Risk’ as the security risks that an organization is exposed to by its internal users (employees, contractors, business partners) who have access to critical systems and confidential information. The threats can be deliberate (malicious) or unintentional.

Desai feels, “Internal security risk is a complex and difficult challenge facing organizations today no matter what industry or region. Therefore, Data Loss Prevention (DLP) is the only way to protect information in the organization and it is not a surprise that DLP is gaining plenty of ground in the region including India. Companies have already bought in on the value of DLP and are ready to engage; therefore I am anticipating that it will be a high priority for businesses in 2010.”

He also says that, “Evolving threat will drive more advanced security measures - As cyber threats become more sophisticated and IT systems more complex, large enterprises will continue to examine ways to improve the performance and responsiveness of IT and security operations.”

He adds a note of caution, “With the critical security challenges that organizations are facing today, organizations must go beyond the traditional understanding of security and look at a more advanced security operations function that can effectively manage risk internally and externally.”

Vineet Sood, Head Channels and Alliances, Symantec India says, “The ever evolving threat landscape and the increasing sophistication of cyber criminals will make security a key area of concern across the world.”

Sood lists out some trends for 2010 that Symantec researchers have identified:

Top 10 Countries Producing botnet - Zombies

Q4 2009		Q3 2009		Q2 2009	
Country	% of total	Country	% of total	Country	% of total
China	12	US	13.1	US	15.7
United States	9.5	China	12.2	China	9.3
Brazil	8.5	Brazil	8	Brazil	8.2
Russia	7	Germany	7.3	Russia	5.6
Germany	6	Rep. of Korea	5.1	Germany	5.3
Rep. of Korea	5	Italy	4.3	Italy	4
Italy	3.5	India	3.4	Rep. of Korea	3.8
UK	3.2	Russia	3	India	3.2
Taiwan	3	UK	2.9	UK	3
Spain	2.6	Spain	2.6	Spain	2.6
Total	60.3	Total	61.9	Total	60.7

Top 10 countries of newly created zombie computers, by quarter. These systems are hijacked to send spam to millions of email addresses

Source: McAfee

Antivirus is Not Enough

With the rise of polymorphic threats and the explosion of unique malware variants in 2009, the industry is quickly realizing that traditional approaches to antivirus, both file signatures and heuristic/behavioural capabilities, are not enough to protect against today’s threats. Verma says that, “We have reached an inflection point where new malicious programs are actually being created at a higher rate than good programs. As such, we have also reached a point where it no longer makes sense to focus solely on analyzing malware. Instead, approaches to security that look to ways to include all software files, such as reputation-based security, will become key in 2010.”

Social engineering is already one of the primary attack vectors being used today, and Symantec estimates that the number of attempted attacks using social engineering techniques is sure to increase in 2010.

Rogue Security Software Vendors Escalate Their Efforts

In 2010, expect to see the propagators of rogue security software scams take their efforts to the next level, even by hijacking users’ computers, rendering them useless and holding them for ransom, warns Verma. “A less drastic next step, however, would be software that is not explicitly malicious, but dubious at best. For example, Symantec has already observed some rogue antivirus vendors selling rebranded copies of free third-party antivirus software as their own offerings. In these cases, users are technically getting the antivirus software that they pay for, but the reality is that this same software can actually be downloaded for free elsewhere,” he adds.

Social Networking Third-Party Applications Will be the Target of Fraud

With the popularity of social networking sites poised for another year of unprecedented growth, expect to see fraud being leveraged against site users to grow. In the same



The ever evolving threat landscape and the increasing sophistication of cyber criminals will make security a key area of concern across the world

Vineet Sood, Head Channels and Alliances, Symantec India

Authentication will also be an imperative measure to ensure that information in the cloud or a virtualized environment does not land in the hands of non-authorized users or fraudsters

Vikas Desai, Lead Technology Consultant, India & SAARC, RSA, The Security Division of EMC

vein, expect owners of these sites to create more proactive measures to address these threats. As this occurs, and as these sites more readily provide third-party developer access to their APIs, attackers will likely turn to vulnerabilities in third-party applications for users' social networking accounts, just as we have seen attackers leverage browser plug-ins more as Web browsers themselves become more secure, Verma adds.

Fast Flux Botnets Increase

Fast flux is a technique used by some botnets, such as the Storm botnet, to hide phishing and malicious Web sites behind an ever-changing network of compromised hosts acting as proxies. Using a combination of peer-to-peer networking, distributed command and control, web-based load balancing and proxy redirection, it makes it difficult to trace the botnets' original geo-location. As industry counter measures continue to reduce the effectiveness of traditional



botnets, expect to see more using this technique being used to carry out attacks.

URL Shortening Services Become the Phisher's Best Friend

Because users often have no idea where a shortened URL is actually sending them, phishers are able to disguise links that the average security conscious user might think twice about clicking on. Symantec is already seeing a trend toward using this tactic to distribute misleading applications and we expect much more to come. Also, in an attempt to evade antispam filters through obfuscation, expect spammers to leverage shortened URLs shorteners to carry out their own evil deeds.

The number of attacks designed to exploit a certain operating system or platform is directly related to that platform's market share, as malware authors are out to make money and always want the biggest bang for their buck.

Spammers Breaking the Rules

As the economy continues to suffer and more people seek to take advantage of the loose restrictions of the CAN SPAM Act, more organizations will sell unauthorized e-mail address lists and more less-than-legitimate marketers spamming those lists.

Highly specialized malware was uncovered in 2009 that was aimed at exploiting certain ATMs, indicating a degree of insider knowledge about their operation and how they could be exploited. Expect this trend to continue in 2010, including the possibility of malware targeting electronic voting systems, both those used in political elections and public telephone voting, such as that connected with reality television shows and competitions.

CAPTCHA Technology Will Improve

As this happens and spammers have a more difficult time breaking CAPTCHA codes through automated processes, spammers in emerging economies will devise a means to use real people to manually generate new accounts for spamming, thereby attempting to bypass the improved technology.

Symantec estimates that the individuals employed to manually create these accounts will be paid less than 10 percent of the cost to the spammers, with the account-farmers charging \$30-40 per 1,000 accounts.

As cyber criminals exploit new ways to bypass CAPTCHA technologies, instant messenger (IM) attacks will grow in popularity. IM threats will largely be comprised of unsolicited spam messages containing malicious links, especially attacks aimed at compromising legitimate IM accounts. By the end of 2010, Symantec predicts that one in 300 IM messages will contain a URL.

In addition, in 2010, Symantec predicts that overall; one in 12 hyperlinks will be linked to a domain known to be used for hosting malware. Thus, one in 12 hyperlinks appearing in IM messages will contain a domain that has been considered suspicious or malicious. In mid 2009, that level was 1 in 78 hyperlinks.

Challenges of 2010



Protecting and providing complete security solutions will be challenging

India's private security industry, estimated to be over Rs. 10,000 crore today, requires over two lakh security professionals in various installations/utilities in the next coming years. With this huge opportunity comes a great challenge for the industry - to regularize and organize the industry with the implementation of The Private Security Agencies (Regulation) Act 2005 (PSARA) - to ensure uniform standards of professionalism across the country, says Nilendu Mitra, Senior Vice President, TopsGrup.

Adds Mitra, "That apart, there is a range of threats including terrorism and irregular warfare. Terrorists use cyberspace as well as wireless technologies like satellite phones, GPS maps to chart their entry and escape routes. While the country's police and security forces are progressively working towards modernization we are still way behind in technology and training to counter such new-age terrorism. New age chemical warfare will be the next agenda up on the sleeves of terrorists."

The emergency response network to coordinate between victims, ambulances and hospitals during an emergency is still missing in the country and is expected pose a serious challenge in the face of any terror attacks.

According to Anil Dhawan, Senior Vice President at G4S

Security Services, and President, APSA - India Chapter, "The Implementation of PSARA Act for the guarding Industry will be a challenging one. That apart, good security solution for the forthcoming Commonwealth Games in New Delhi 2010 will be another great challenge."

However, according to Vinay Vashishta, CEO, RBH India, "It is necessary to provide total alarm management in a cost-effective manner so that small and medium size companies can afford it. If technology is out of reach of a common requirement (price wise), I personally do not consider it as a good technology. For instance, the Maruti car actually changed everything in car industry in India, so according to me, it is more effective technology than those of other large players in the car industry."

Sanjeev Sehgal, Managing Director Sparsh Securitech, believes that customer awareness about security still remains a key issue in India. "Terrorist events are making customers think about security as a strategic investment to protect their properties and businesses but we still have some ways to go. The second challenge we see is the availability of capital for small and mediumsized businesses to invest in new products and technologies."

On the IT security front, Vikas Desai, Lead Technology Consultant, India & SAARC, RSA, the security division of EMC, lists out some of the challenges below:

Going forward, we believe that software will play an important role. However, analogue solutions will dominate for the time being while digital and wireless technologies mature for security applications

Sanjeev Sehgal, MD Sparch Securitech

Corporate becomes Dark-Cloud-Aware

While the Dark Cloud becomes more corporate-aware, CSOs will seek to gain better visibility into the Dark Cloud of cyber crime infrastructure and feed information such as stolen access credentials and compromised end points directly into their back-end monitoring systems.

Mobile banking fraud

More customers enroll for mobile banking, and more services are offered via mobile channels. Banks in Asia and Europe are already experiencing mobile Trojans and SMS redirection attacks. Banks will start funding the extension of their online banking protection to the mobile channel.

Corporate Web 2.0 based social engineering attacks

The enterprise develops Web 2.0 functionality in order to support a growing internal demand, but this makes them an easier target for social engineering attacks that are combined with malware. We predict that cyber criminals will use Web 2.0 applications for various objectives such as collecting corporate data, infecting multiple PCs within the network, and stealing employees' private information in order to do identity theft.

Infection intensifies

The rate of the malware infection of personal computers was 10 times higher during 2009 compared to 2008. We project infection rates to further grow in 2010 as cyber criminals' scale up their attacks and adapt to emerging

attacks towards Indian enterprises has risen considerably during the past year and we expect to see this trend even this year.

Meanwhile on the software side, Ajay Verma, Director, Channels and Alliances, Symantec India, says, "Rogue or fake security software will be a significant challenge in 2010. In fact, a Symantec study conducted between July 2008 and July 2009 found that cyber criminals are employing increasingly persuasive online scare tactics to convince users to purchase rogue security software. Rogue security software, or "scareware," is software that pretends to be legitimate security software. These rogue applications provide little or no value and may even install malicious code or reduce the overall security of the computer."

To encourage unsuspecting users to install their rogue software, cyber criminals place website ads that prey on users' fears of security threats. These ads typically include false claims such as "If this ad is flashing, your computer may be at risk or infected," urging the user to follow a link to scan their computer or get software to remove the threat.

According to the study, 93 percent of the software installations for the top 50 rogue security software scams were intentionally downloaded by the user. As of June 2009, Symantec has detected more



Clearly, products which can do total alarm management in single, unified form with a strong control and command software is catching up fast
 Vinay Vashishta, CEO, RBH India

defences. Drive-by-download (taking over legitimate websites; routing visitors to an infection server) will continue to be a primary infection method, but social engineering attacks (e.g. spamming a victim's entire social network "friend list" with links to infection servers) will intensify.

Trojans will become corporate-aware

Today, Trojans designed for financial fraud already record a massive amount of enterprise data siphoning off infected PCs. In 2010, we project that the Trojan operators will become more corporate-aware, and build specific triggers for recording sensitive corporate data, files and emails for future trade.

Hackers diverting their attention towards Indian Enterprises

More and more Indian enterprises are coming under the fraudster's radar with focused attacks designed by the fraudsters especially on them. The number of such targeted

than 250 distinct rogue security software programs.

The initial monetary loss to consumers who download these rogue products ranges from Rs. 1350 to Rs. 4500. However, the costs associated to regain ones' identity could be far greater. Not only can these rogue security programs cheat the user out of money, but the personal details and credit card information provided during the purchase can be used in additional fraud or sold on black market forums resulting in identify theft.

To make matters worse, some rogue security software actually installs malicious code that puts users at risk of attack from additional threats. As a result, installing these programs can lower the security posture of a computer while claiming to strengthen it. For example, rogue programs may instruct the user to lower or disable any existing security settings while registering the bogus software or prevent the user from accessing legitimate security Web sites after installation. This, in turn, leaves users exposed to the very threats the rogue software promised to protect against.



- Increase knowledge base of the industry
- Look at security as a strategic investment
- Products / solutions still at a nascent stage
- A good, up-to-date security suite is a must

Recognition and pricing: Crucial factors

The Indian security industry is certainly on the same wicket regarding on some of the issues concerning the industry. To begin with, it seeking industry status under relevant sections of the Income Tax Act.

According to Anil Dhawan, Senior Vice President at G4S Security Services, and President, APSA – India Chapter, "There is a strong need to recognize the private security solution providers by the Government based on well-defined standards."

Says Vinay Vashishta, CEO, RBH India, "We have to work on increasing the knowledge base of the industry for designing effective and proactive solutions."

Sanjeev Sehgal, Managing Director, Sparsh Securitech, feels that businesses need to start looking at security as strategic investment providing return of investment and not just as a cost. The opportunity cost of lost time, property damage, and lost revenue can be very substantial if a security breach occurs – whether it is physical or logistical in nature. With government support and growing awareness, the future of the security industry is very bright in India.

Highlighting other factors, Pushkar Gokhale – GM, Sales and Marketing, Godrej Security Solutions, states: "In terms of challenges, India is a market where there is a high amount of price preference dominating over quality. It is a highly price-sensitive market. While the volumes could be really in bulk, the prices need to be highly competitive." Second is that in terms of the customer's awareness on the products/ solutions

is still at a nascent stage, because of which the customer is not in a position to make out the difference between chalk and cheese when it comes to identifying a competent system integrator. The number of competent and professional system integrators is very few in India compared to the other markets. However, due to the unorganized nature of the industry in this market, especially the electronics security market, CCTV, the low-end suppliers who are less competent tend to spoil the party.

On the IT security front, Vikas Desai, Lead Technology Consultant, India & SAARC, RSA, the security division of EMC, believes that the rise of targeted attacks on Indian organizations and increase in the use of social networks to exploit/defraud users would be the two issues that needs to be highlighted. Vineet Sood, Head Channels and Alliances, Symantec India feels that cyber criminals today no longer operate for fame, but for financial gain. "There is a highly organized cyber mafia at work, creating new pieces of malicious code every second and conducting highly targeted attacks on internet users." In fact, according to Symantec's Underground Economy report, the total value of goods and services advertised on the underground economy services was over Rs. 1240 crore (\$276 million).

In such a scenario, users should defend themselves with a good, up-to-date security suite from a reputed vendor who can protect against not only known threats, but also from never-seen-before attacks.

Innovations changing market dynamics

Innovations change the security landscape. In fact, innovations push the industry to perform at a higher level. Although India is yet to see great innovations in the security space, the trends are encouraging. Sanjeev Sehgal, Managing Director, Sparsh Securitech, believes that natural progression is for cameras to get digital and smart so that security can become more proactive and security devices can be used not only for performing post mortem of events to track miscreants but also to prevent events from happening.

According to Anil Dhawan, Senior Vice President at G4S Security Services, and President, APSA – India Chapter, the Government of India is working towards setting up some standard operating procedures (SOP) to define security standards. “This would make the security requirements mandatory for shopping malls and public places. It will improve security protection for the common person and also bring new opportunities for solution providers,” he said.

However, Nilendu Mitra, Senior Vice President TopsGrup, has a different take. According to him, “Any one innovation cannot alone change the security landscape. Risk management is always holistic and enterprise-wide.”

On the IT security front, Vikas Desai, Lead Technology Consultant, India & SAARC, RSA, the security division of EMC comes up with innovative options that are indeed revelations.

Invisible Authentication

Consumers today are on the lookout for better ways to protect their online accounts and identities, and companies, hoping to avoid some of the potential financial losses associated with identity-related crimes, are turning to proven authentication technologies - that have been fine-tuned to provide users with secure, simple-to-use Internet identities.

RSA® Adaptive Authentication is a comprehensive authentication and fraud detection platform that monitors and authenticates customer activity based on risk levels, institutional policies, and customer segmentation.

Adaptive Authentication is powered by risk-based authentication, an intelligent system that authenticates all users behind-the-scenes by measuring a series of risk indicators. This transparent authentication provides for a superior user experience as customers are only challenged in the highest risk scenarios.

Adaptive Authentication Offers Remote Channel Protection Through the Following Modules:

- **Web Protection:** Protects online customer activity at both the login and transactional levels
- **Phone Protection:** Protects the IVR (Interactive Voice Response) systems and CSR (Customer Service Representative) applications that organizations use within their Call Center operations

• **Context/Identity Sensitive Data Protection:** Not all data in an organization is of equal importance from a security perspective. The first step in preventing enterprise data loss is to determine which data is most sensitive – or at highest risk – to your business. Then, you can prioritize your efforts and define appropriate policies.

Nevertheless, how do you know which data is most sensitive to your business?

To answer the question, one needs to understand the business structure, examine the various departments and lines of business across the organization, and identify both the regulatory and non-regulatory security drivers for each department.

Once the regulatory and corporate compliance universe is understood, one can prioritize data by grouping information into various ‘classes’. For example, one might create three classes of information from the most restricted and sensitive (e.g., data relating to the company’s unannounced financial results) to the least sensitive (e.g., data pertaining to vendor shipping rates).

The next step is to determine the data categories, elements, and owners for each class of information. For California SB 1386 compliance, for example, non-public personal information – government identification numbers and citizenship status, for example – are critical pieces of the compliance puzzle. One might classify this information as ‘restricted.’ Then,



The Government of India is working towards setting up some standard operating procedures (SOP) to define security standards. It will improve security protection for the common person and also bring new opportunities for solution providers

Anil Dhawan, Senior V P, G4S Security Services

it should be determined which elements of the information are most critical and which department or business unit within the company owns this data. Finally, after it has been classified, one can then define the policies – the rules for appropriate handling of the data – including which employees and applications are authorized to access this data and how, when, and from where they are allowed to access it. For example, an organisation might allow all employees in R&D to access the information pertaining to the company’s products, but only certain employees to view the data about new, unreleased products – and only during specific hours and from within the corporate firewall.

Traditional Security Solutions Obsolete

On the software side, Vineet Sood, Head Channels and

Alliances, Symantec India believes that, “The explosion of malware variants and the increasing sophistication of cyber criminals have rendered traditional security solutions obsolete. In such a scenario, where new threats are emerging every second, internet security solutions need to keep up with the increasing sophistication of cyber criminals. Symantec believes the industry has reached an inflection point where more new malicious programs are being created than good programs. At this point, given the sophistication of the threats, a new, hybrid approach to virus detection and protection is necessary.”

Sood is of the opinion that, “Traditional blacklisting and whitelisting work well for prevalent malware and goodware, such as a malware file that is on thousands or millions of computers across the Internet. However, these techniques are much less effective at addressing the Internet’s “long tail”—the tens of millions of files that are each on just a few computers in the world. That’s why Symantec has developed a new file-based reputation system that leverages our huge opt-in user base—currently around 35 million users—to anonymously collect application usage data.”

He adds that the system uses this data to derive highly accurate application reputation ratings. All this happens behind the scenes; users are never prompted to submit information or provide input, and participation is voluntary, requiring an initial opt-in when the software is installed.

Reputation-based technology tracks files and applications and dozens of attributes such as age, download source, digital signature, and prevalence. These attributes are combined using numerous algorithms to determine a reputation. As a file is distributed across the Internet and these attributes change, the technology updates the reputation of the file. This is especially important when a file is new, likely to be a threat,

and traditional defenses are not likely to detect it.

The reputation-based technology leverages millions of users who choose to anonymously contribute data about the applications running on their systems. This data is fed into a reputation engine where dozens of attributes for each file, such as age, download source, digital signature, and prevalence are combined to determine its reputation. Without ever having to ask the user, Symantec can infer with an extremely high degree of accuracy the likelihood of an unknown application being good or bad.

Since the traditional blacklisting and whitelisting approaches no longer work against the ever-evolving cyber criminal, this reputation-based technology will provide users with more protection and more confidence that their online interactions are secure, Sood adds.

Indian Security Industry: Gaining Maturity

The Indian security industry has been growing at the rate 25 per cent for the last couple of years and projected to grow manifold in next 4-5 years to meet up with its security requirements. The size of security business in India is currently estimated at Rs.22,000 crore, which according to trade body Assocham may cross Rs.50,000 crore in next few years. Nevertheless, where is it headed?

According to Anil Dhawan, Senior Vice President at G4S Security Services, and the APSA – India Chapter President, “It is getting matured by way of better understanding of its customers. The industry is acknowledging the requirement of security standards and associations for better representation of its demands. It will develop into a major market for security solutions in Asia.”

Agreeing with Dhawan, Vinay Vashishta, CEO, RBH India says, “Certainly getting matured in coming year I believe seller will know what he is selling and buyer will know what to purchase and why.”

Says Nilendu Mitra, Senior. VP & Owner - Marketing & Corporate Communication, TopsGrup, “Security is no longer being viewed as expenditure, but as a long term investment. Mushrooming of shopping malls, special economic zones, self contained townships, IT parks and other exclusive facilities will only continue creating strong demand for private security services in India.”

The industry is constantly transforming and players in this space have started to get into the M&A mode acquiring international security service providers, a trend which was started by Topsgrup, when it acquired 51per cent strategic stake in UK’s The Shield Guarding Company in 2008. The future will see many more such acquisitions in coming years.

According to Sanjeev Sehgal, MD Sparch Securitech, “Awareness about security products and need to have adequate security measures in place to secure their businesses. The rapid economic growth will fuel the growth in security industry and we expect Indian market to continue growing at over 30 per cent for the foreseeable future.” He feels that, “Technology adoption in India is a lot quicker

than most other countries. Digital cameras are the preferred solutions in the developed countries and we expect similar trend in India over the next couple of years. Analog cameras are still the preferred devices due to their flexibility and reliability but digital cameras will become preferred devices in next few years.”

Sehgal is very optimistic, “Majority of the products sold in India are still imported. Very few firms develop security products in India. India has the talent to develop these products. We have made it our mission to make India a recognized leader in design and manufacturing of security devices. Easier access to capital and government policy support are needed to ensure support for local firms. We expect more firms to take our lead and start developing these products in India.”

Vikas Desai, Lead Technology Consultant, India & SAARC, RSA, The Security Division of EMC dishes out facts to buttress his optimism, “The total information security market in Asia Pacific was said to be worth \$420 million in 2006, and APRG predicts it will grow to nearly \$1.1 billion by 2012. The Indian security market has been growing rapidly at double digit Annual Growth Rate and Gartner is forecasting a CAGR of 16.4 per cent for the Indian security market from 2008-2013.”

According to him, “The potential of the security market in India is huge as most organizations still do not have a complete understanding of various risks of fraud faced by them nor they have an efficient strategy

for investing in securing this information across verticals and consumer groups,” says Desai.

Vineet Sood, Head Channels and Alliances, Symantec India summed up by saying, “With growing broadband adoption, India is becoming a hub and a target for malicious activity. However, awareness and adoption of security solutions is rather low. In fact, according to a Symantec report, adults in India rank the highest when it comes to not having the basic security measures. 33 per cent of adults in India do not have security software.”

This is despite the fact that India had the third highest volume of malicious activity in APJ, according to Symantec’s Internet Security Threat Report XIV. Furthermore, in the APJ region, India ranked first on worms and viruses attacks prevalence chart. Nine of the top 10 malcodes found in India consisted of worms (55 per cent) and viruses (15 per cent) that disabled security related processes, downloaded additional threats and stole confidential information.

The report also revealed that India had an average of 836 bots per day during 2008 and there were 103,812 distinct bot-infected computers observed in the country during the period. This was a staggering increase of nearly 250 percent from the previous Internet Security Threat Report.

Furthermore, 12 per cent of spam detected in APJ in 2008 originated in India, making it the third-ranked country for this category.

While these threats are set to increase rapidly, with the increasing internet penetration, they also signify the heightened vulnerability of India to online threats, and the growing need for security solutions in the country. Therefore, the market for internet security suites in India shows tremendous potential.



Any one innovation cannot alone change the security landscape. Risk management is always holistic and enterprise-wide

Nilendu Mitra, Senior. VP & Owner – Marketing & Corporate Communication, TopsGrup

in place to manage these risks.”

One major point that was however clearly agreed upon by most organizations, especially in the BFSI, telecom sectors, was to have risk based “information centric” approach towards security as all agreed that information/data is vulnerable not only during transit but also when it is residing at a datacenter. Besides, security is no longer a hindrance for businesses, but it is critical to have a robust security policy and infrastructure in place to accelerate business productivity.

“As more of our personal and business information is getting connected through technology drivers like social networking, cloud computing, mobile business applications and online banking, risks of misuse of this information are also on the rise. Therefore, we see a heightened awareness

Symantec has the advantage of its Global Intelligence Network, which captures worldwide security intelligence data that gives Symantec analysts unparalleled sources of data to identify, analyze, deliver protection and provide informed commentary on emerging trends in attacks, malicious code activity, phishing, and spam. The Global Intelligence Network enables Symantec to detect and remediate threats in real time, allowing us to protect customer information as well as interactions over the internet.

In the context of the malware explosion that India, along with the rest of the world, is witnessing, Symantec believes vendors who can provide complete protection against new, never-seen-before threats, will be the preferred choice of customers.

- **Security is no longer being viewed as expenditure, but as a long-term investment**
- **Industry players getting into the M&A mode acquiring international security service providers**
- **Technology adoption in India is a lot quicker than most other countries**
- **India has the talent to develop products**
- **Easier access to capital and government support needed**
- **Growing need for security solutions in the country**