GUARDIANS OF THE ONLINE WORLD

Cyber security is becoming big business. Here's why

BY NIDHI SINGAL
ILLUSTRATIONS BY RAJ VERMA

$4.3 BILLION
Revenue generated by cyber security services industry in India in 2019

$7.6 BILLION
Expected revenue by 2022

21%
Expected CAGR of the industry till 2025

Grocery is a boring, low-margin business. But that did not prevent cyber criminals from stealing data of 20 million customers of online grocer BigBasket and selling it for a staggering $40,000 or nearly ₹30 lakh on the dark web. And that too non-financial data such as name, email ID, PIN, contact number, address, date of birth, location, IP address.

BigBasket had thankfully not stored customers' financial data such as debit/credit card details. But companies and their customers are not always so fortunate. In 2016, security of close to 3.2 million debit cards issued by major banks, including SBI, HDFC Bank, ICICI Bank, Yes Bank and Axis Bank, among others, was compromised. The breach, caused by a malware on an ATM network, resulted in not just financial loss to consumers and banks but also dented people's

trust in digital banking.

"There is always risk of financial loss in a cyber attack. To combat the evolving cyber security threats, banks need adaptive 24x7 methods of detection, defence and counter-attack," says Abhimanyu Bhoan, CEO, New India Co-operative Bank.

With dramatic rise in cyber attacks over the years — they doubled to 6,96,938 between January and August this year — companies, especially those with a heavy online presence, are beefing up their security architecture, creating new business for providers of cyber security and making it one of the fastest growing areas in IT services. As per the India Cybersecurity Services Landscape report by Data Security Council of India (DSCI), the cyber security services industry in India generated revenue of $4.3 billion in 2019 and is expected to reach $7.6 billion in 2022. It will be registering a compounded annual growth rate (CAGR) of 21 per cent till 2025.

Sector Contribution

Going forward, the cyber security market in India will be defined by three key sectors, banking, financial services and insurance (BFSI), information technology (IT) and IT-enabled services (ITeS) and government, which will account for 68 per cent of the market, according to the DSCI report. The BFSI sector's share will be the largest at 26 per cent. Driven by new regulatory norms as more and more businesses go digital, rapid adoption of technology and increased number and complexity of cyber threats, the BFSI sector's spending on cyber security is expected to rise from $518 million in 2019 to $810 million by 2022, a CAGR of 16.1 per cent, led by users such as New India Co-operative Bank, which has adopted IBM's Security Operation Centre (SOC) services for proactive monitoring of threats 24x7,

The User Club

BSE Ltd has deployed next gen SOC & technologies. In next gen SOC (Security Operation Centre), data monitoring extends beyond the organisation into cloud services, key executives' email accounts, mobile devices, and much more

New India Co-operative Bank uses IBM's SOC service for monitoring of threats 24x7, as well as for defence and counter-attack

Panasonic has deployed California-based Fire Eye's solutions at the gateway level to detect embedded malware

Some Recent Data Breaches

At BigBasket, data of 20 million users, including name, email ID, PIN, contact number, address, date of birth, location, along with IP address, available for sale – November 2020

Data breach at Dr Reddy's Laboratories resulted in shutdown of all production facilities across the world for 24 hours – November 2020

Administrative network of Kudankulam Nuclear Power Plant of Nuclear Power Corporation of India in Tamil Nadu was breached in malware attack. However, plant systems were not affected – September 2019

Data of over 100 million users of local search service JustDial was publicly available – April 2019

"Security leaders from SMBs to large enterprises need to continue their focus on the entire threat lifecycle which constitutes planning and detection, in-the-moment response and remediation–recovery"

Prashant Bhatkal, Security Software Leader, IBM India/South Asia

apart from detection, defence and counter-attack.

Entities such as stock exchanges are also not behind. "When you talk about stock exchanges, speed and accuracy are very important. We are a fully digital platform. Cyber attacks like DDoS (distributed denial of service), malware, ransomware, phishing, social engineering and many more can have a huge impact on BSE's contribution to the financial system of India," says Shivkumar Pandey, Group CISO, BSE Ltd. BSE's robust IT system includes the Next Gen SOC & Technologies deployed by IBM and an array of in-house teams working in areas such as risk, governance & compliance, application security and project management. The systems are designed and implemented based on Zero Trust Security Design & Architecture. They ensure coverage at all levels - endpoint, data centre, network, applications, cloud and more.

The IT/ITeS sector has emerged as the fastest-growing user of cyber security services. Its spending on cyber security is expected to grow from $434 million in 2019 to $713 million by 2022, a CAGR of 18 per cent.

The government sector is not far behind and is expected to spend $581 million by 2022, up from $395 million in 2019, a CAGR of 13.8 per cent. This growth is primarily driven by increased focus on digitisation of government systems and rising cyber attacks on critical state infrastructure. Digitisation of citizen services, consumer awareness and smart city initiatives will also drive substantial investments in cyber security. The cyber security spend in other sectors is expected to grow from $630 million in 2019 to $949 million by 2022, a CAGR of 14.6 per cent, says the DSCI report.

Pandemic Impact

Rise in cyber attacks and changes because of the pandemic are impacting the industry positively. Organisations working with disconnected teams and disparate data are feeling the need for an open and connected platform approach to cyber security. Cyber security is emerging as a business necessity and not just a support function.

With multitude of employees and partners accessing enterprise and messaging applications remotely, Panasonic Life Solutions is doing its best to stay safe. "We have implemented a very strict information security policy, which is regularly communicated and explained to employees and partners. We conduct regular vulnerability tests to ensure safety of our network and have deployed a VPN for closed access," says Dinesh Aggarwal, Joint Managing Director, Panasonic Life Solutions India Pvt. Ltd. The company has been pursuing a large-scale move towards digital technologies for internal and external stakeholders and has deployed Fire Eye at gateway level to detect embedded malware.

Pidilite Industries Ltd, on the other hand, believes in keeping good stuff in and bad stuff out. "We isolate and ring-fence what we consider IP (intellectual property) or confidential information, and implement stringent controls to protect such information. For keeping the bad stuff out, we have adopted an objective

score-based approach that measures our security posture on various parameters and suggests remediation measures to improve the score on an ongoing basis," says Mayur Danait, CIO, Pidilite Industries Ltd.

However, there isn't 'one strategy that fits all'. The approach differs according to the nature of the organisation. "A sound security strategy for remote workforce always includes proactive endpoint protection (or next-generation antivirus) that mitigates attacks before, during and after they are executed. Advanced approaches include automated rollback to return infected Windows PCs to their previously clean state," says Debasish Mukherjee, VP Sales - APAC at SonicWall, a network security solutions provider.

With global growth engine coming to a halt, IT spending will be aligned with business projections. However, allocation for security is expected to increase significantly.

Spending & Impact

Investment in cyber security technologies is an ongoing need. Hence, many organisations in India, even after being aware of cyber security as one of the top five risks to their business, continue to contemplate on the recurring cost involved. "The reason is the dynamic and ever-evolving threat landscape. Security leaders from SMBs to large enterprises need to continue their focus on the entire threat lifecycle which involves planning and detection, in-the-moment response and remediation–recovery. This will help them prepare for additional unforeseen threat scenarios," says Prashant Bhatkal, Security Software Leader, IBM India/South Asia.

Investments will depend on multiple factors such as the nature of the business, the domain it operates in, regulatory compliances, types of risk involved and awareness level. For instance, a financial institution might invest more in security compared to a manufacturing organisation due to the nature of data it handles. As per the industry norms, enterprise security budgets are 8-10 per cent of overall IT budgets, which have been increasing every year. "Security operations itself have become so complex that they involve a significant amount of technology. Of the technology spend of 30 per cent, 15-16 per cent will be on security," says Shree Parthasarathy, Partner, National Leader - Cyber Risk Services, Deloitte India.

However, there is a shift in how the budget allocation takes place. "While earlier, security was a percentage of IT spends, security spend is now being considered as part of the overall organisation budget separate from IT. This is primarily due to growing regulations, increase in number of attacks and larger impact to businesses," says Tony Velleca, Chief Executive Officer, CyberProof and CISO, UST Global.

A cyber attack can have grave consequences for the enterprise. It may suffer financial losses either due to legal troubles such as class-action suit or loss of clients/customers. "A company may also have to spend millions of dollars in reparation for damages as well as investment to prevent future attacks. This was exemplified in the Target data breach where the company spent more than $100 million in upgrading systems to prevent another breach, besides suffering a 46 per cent drop in profits after the attack," says Nilesh Jain, Vice President, Southeast Asia and India, Trend Micro, an American-Japanese cyber security software company with global headquarters in Tokyo, Japan, and Irving, Texas, United States.

A breach may also lead to stringent penalties with increasing number of companies adopting legislation such as EU's GDPR (General Data Protection Regulations). There are cases of espionage and sabotage too. "Proprietary information, such as formulas or trade secrets, can be targeted in an attack to eliminate competitive advantage. In case of sabotage, disrupted operations can give a competitor, or even another country, an advantage in the market," says J. Kesavardhanan, Founder and CEO, K7 Computing.

QKD – The New Frontier

Quantum Key Distribution (QKD) is proclaimed to be the ultimate technology for keeping information-sharing safe over the network. It uses photons, particles of light, to generate a random secret key. Using this key, the messages can be encrypted and decrypted. In case of any interference from an unauthorised third party, the composition of photons is altered, rendering the randomly-generated keys inoperable. Toshiba has successfully deployed the technology in partnership with Quantum Xchange to enhance capacity for the first quantum-secured network in the US. Toshiba QKD technology can detect if somebody is eavesdropping or attempting to steal information.

"We are a fully digital platform. Cyber attacks like DDoS, malware, ransomware, phishing, social engineering and many more can have a huge impact on BSE's contribution to the financial system of India"

Shivkumar Pandey, Group CISO, BSE Ltd.

"Security operations itself have become so complex. They involve a significant amount of technology. Of the technology spend of 30 per cent, 15-16 per cent will be on security"

Shree Parthasarathy, Partner, National Leader - Cyber Risk Services, Deloitte India.

In certain cases, recovery can take long, impacting business operations. Some organisations may never be able to recover. A cyber attack is an existential threat for an enterprise, and investing in effective cyber security makes sense for any business that wishes to remain in business. "Cyber security is not an extension of IT but core to our digital strategy. It is essential to retain customer trust and build business process resilience," says Bharat Kalia, Co-founder and CEO, LifeLong Online Retail. The home-grown white goods company has partnered with a specialised cyber security partner which helps it monitor, backup and restore the company's core assets.

Regulatory Issues

While India will soon have a robust cyber security policy, current laws do not mandate notification of data breach to customers. However, there are sector-specific regulations on this. For example, companies in the financial sector like banks and NBFCs are required to notify cyber security incidents to the Reserve Bank of India. Further, certain types of cyber security incidents need to be reported to the Indian Computer Emergency Response Team ("CERT-In").

"India should fast-track enactment of the Data Protection Act and set up a strong and effective Data Protection Authority. This regulatory framework will provide for appropriate consents to collect and process data and prescribe penalties for non-compliance. Since the draft Bill already provides for high fines (₹5 crore or 2 per cent of worldwide turnover), it is expected to usher in a strong compliance culture," says G.V. Anand Bhushan, Partner at Shardul Amarchand Mangaldas & Co.

Recently, though, with launch of Indian Cyber Crime Coordination Centre and a dedicated National Cyber Crime Reporting Portal, India has taken a firm step towards reporting and acting on such incidents. BT

@nidhisingal