Network security: Scenarioin India

C.M.Anitha[1], Lecturer in Physics, JMJ college for women, Tenali. Mail ID:cm.anitha27@gmail.com

C.Ratna Mary[2], Lecturer in Mathematics, Noble College, Machilipatnam.Mail ID:cratnamary@live.com

Abstract :

Earlier, Network breaches target only the banking and the IT sectors, but now every organization big or small are affected by the threats. To handle these situations effectively, consumers, manufacturers and organizations are to be prepared and well aware of such threats. With the rapid growing of the 'Internet of Things' in every sector, they are hence forced to deal with the existence of these threats and risks, there is thus an increase in focus among regulators.

Cyber security in India has come a long way in the past few years and has gained huge importance in recent times with the thrust on Digital India, e-commerce and mobile payments. Development in digital sector is possible only with robust implementation of cyber security by Prime Minister Narendra Modi. "Can we secure the world from the bloodless war? I'm talking about cyber security. Innovation should be a tool to handle cyber security in India. Cyber India with proper network security is my dream," he has said recently. With rapidly growing interconnected business operations and increasing digitization, cyber security challenges are bound to intensify. Effective measures need to be taken to ensure protection against cyberattacks and threats. We need to focus on the basics that will help keep the growth story on course. Earlier, Network Security was known to be a concern only for the IT and banking industr y, has now penetrated every vertical as a serious threat to any business or organization. The consumers, suppliers and the manufacturers as well should make the cyber risks and they should be prepared to deal with the same. While every sector is fast embracing the 'Internet of things', they are forced to challenge the existence of cyber threats, risks and malwares;there is thus an increase in focus among regulators.

From the very past, India has been targeted for political reasons primarily through cyber-attacks and this dynamic shifting trend from this landscape can be credited to the newly and gaining sophistication in technology and increasingvulnerability in the complex systems. The market that is driven by varied forces like the rise of analytics of big data, consistent rise in threats, fall in the availability of customer security software and strong regulatory compliances enforced by the Government, has few, yet giant hurdles to cross, namely, technical expertise and lack of awareness of security concerns.

The Market can be segmented on the basis of Segment (Security Information and Event Management (SIEM), Security Web Gateway (SWG), Identity Governance and Administration (IGA) and Enterprise Content-aware data loss prevention (DLP)), Solution (Encryption, Firewall, Web Filtering, Identity and Access Management (IAM), Data Loss Protection (DLP), Risk and Compliance Management etc.), Service(Network Security, Endpoint Security, Application Security, Content Security, Wireless Security and Cloud Security) and Verticals. The technology is widely being used to protect violation in Aerospace and Defence, Banking and Financial Services, Telecom and IT, Healthcare, Retails, Manufacturing, Government and Public Utilities.

Key Words: **cyber security, National Association of Software and Service Companies (NASSCOM), cybercrimes, Organization, National Institute of Standards and Technology (NIST)**

INTRODUCTION

Indian companies are known for their quality deliverables. International certifications like ISO 9000 were attained for establishing this reputation. Likewise following international standards in information security will also help companies build credibility in the minds of their customers. Currently, the information security environment in India is a bit complex.National Association of Software and Service Companies (NASSCOM) is the overlooking and governing body for the IT software and services industry in India. Its 1050-member companies are in the business of software development, software services, software products and IT-enabled/BPO services. Indian companies are known for their quality deliverables.

Cyber security is bound to increase as there is an increase in the number of business interconnections. Effective measures need to be taken to ensure protection against cyberattacks and threats. While the nation focuses on growth, our work as technologists, strategists and captains of industry is clearly cut out. We need to focus on the basics that will help keep the growth story on course.

Indian companies have a dynamic security practices comparable to those followed by western companies. Indian companies primarily comply with BS 7799-a global standard that covers all domains of security.Companies sign Service Level Agreements (SLA), have very strict confidentiality and security clauses built into them at the network and data level. Such SLAs also cover all relevant laws that the companies comply with their providers both domestic and foreign to comply to take action in case of any security breaches.

Laws such as the IT Act 2000, Indian Copyright Act, Indian Penal Code Act and the Indian Contract Act, 1972 are passed in order to safeguard the companies operating offshore. Almost all of the companies comply with the standard of the UK Data Protection Act 1998 (DPA) through contractual agreements for the smooth transaction of the company. Companies dealing with US clients have to undergo stringent compliance based upon the segment of the industry. E.g.: Healthcare requires compliance with HIPAA;financial services require compliance with GLBA

Many companies in India go through a SAS 70 Audit. SAS-70 assignments serve as a catalyst for the companies in India to improve the security internally and externally for minimal disruptions from auditors.

Role Of NASSCOM

NASSCOM and ITES BPO industry are working together to create an information security culture in various levels. Indian companies have been escalating to meet the international demands.NASSCOM has not conducted any research on this, but here are a few links, which you may want to independently evaluate and draw conclusions. However as per some independent studies.The ITRC Breach List is consolidated reporting and citing from various media sources and/or notification lists from variousagencies. There are 5,029 reported data breach incidents since 2005which has been tracked since 2005 which involves 675 million records as per estimation. With an average of 45.2% breaches in 2016, there is a need forawareness about such identitytheft among the individuals.

NASSCOM and its member companies are had been striving hard to uphold the data privacy inlegal and enforcement framework to attain data protection. This threat for the breach in data security is not limited to a nation alone, it can affect any nation in the world and the judiciary and any governing bodies has the responsibility to identify and punish the criminals. India is one of the countries where judiciary rules are strict and restricted. We have seen a few cases in the past year, where almost all the accused have been arrested within 24-48 hours of the crime being reported.

NASSCOM has been working hard to amend and enforce the following acts:

1. Assisting the government to take proper action against the culprits and to make laws for the cyber and network breaches accordingly.

2. Providing assistance and training to the Indian law enforcement agencies to deal with the cybercrime and criminals as per the law.

3. To train and create a stream of IT professionals who are suitable for working in the industry.

The Indian IT companies do not want to merely match worldwide standards in security. They want to set the highest standards.

Current Aspect:

Year after year, cyberattacks continue to escalate in frequency, severity and impact. The age-old methods used for the preventing and detecting the assaults by highly trained and skilled aggressive cybercriminals and many organisations are not equipped with the resources to combat the same. The asymmetric nature of cybercrime incentivises it; the cost of committing cybercrimes to intercept and/or modify information, degrade performance of assets, gain unauthorised access to systems, obtain the information from the organisation for either bringing harm or for any personal agenda is very minimal damage compared to the investments required equipping the safeguards against the attacks.

Underestimating the level of risk an organisation is exposed to is usually a fatal mistake. Cyber security impacts all organisations, from fledgling start-ups to billion-dollar multinationals. Over the most recent years network incidents such as WannaCry virus, the compromise of over 10 million user records by the breach of an Indian music streaming service and vulnerability of the routers causes the spying and assaults in popular network companies. Notable cyber incidents over the past year, such as that of the Indian music streaming service that compromised the records of more than 10 million users, or the vulnerability found in the routers of a popular networks company which allows attackers to spy on traffic, testify this. Indian organisations detected 117% more incidents over the previous year, shooting up from an average of 2,895 incidents to 6,284 incidents a year. This is a sharp deviation from the global trend, which saw a 39% increase in security incidents over the previous year.

Financial Aspect:

There is a critical economic loss as the network incidents increased by 135% over the previous year which is much more compared to 20-30% over the years before. Not only has the number of incidents increased, but the average loss resulting from an incident borne by an Indian organisation has also increased by close to 8%. Handling the losses caused due to cyber incidents and evaluation of the factors casing those has been a daunting task for the organisation, and hence, the true cost of cyber incidents is hard to calculate. Some factors that are typically used to estimate the financial loss from cyber incidents include loss of customer business, legal defence services, court settlements, investigations, forensics, and deployment of detection software, services and policies among others.

External& Internal Breach Aspect:

External factors dominating the news headlines are playing a vital role in the attacks relating to the network. Agents like terrorist hacks, hacktivists, etc. have been all over the media over the previous years. However, it is important to understand that security breaches by insiders—employees, vendors and business partners with authorised access—can be even more harmful. Though several organisations are not ready to deal with these threats.

The trend over the years also shows the same results as security incidents caused by insiders have dominated those caused by external actors. Though the trend has been declining over the last three years due to improvements in internal access controls, it appears that in the last 12 months, the number of incidents caused by insiders have once again increased due to the inability of the existing basic identity and access management controls to prevent modern techniques like social engineering used by attackers to exfiltrate confidential information.

Unintentional breaches can be avoided by ensuring that employees are aware of the organisation's security and privacy policies, procedures and consequences of not adhering to them. Employee training and awareness is an important component and should be carried out by the organisations.

Year over year there is a swift increase of the nature of the cyber threats evolution. Criminal organisations are expected to become more sophisticated, mature and be able to migrate their activities online at a greater pace. Outsourcing activity among Indian organisations is also expected to rise with more and more organisations focussing on their core business, thereby creating more complex and interconnected networks with suppliers, vendors, partners and other third parties, making them more prone to cyberattacks and data leakages.

And hence, it is imperative for Indian organisations to gear up for the cyber security challenge by formulating security strategies and implementing technology solutions to monitor and manage security risks.

Development Aspect:

Recent advances in computer science and technologies are providing powerful opportunities for organisations to transform their cyber security programmes and create a holistic system of integrated safeguards. It all starts with a strategy and an underlying foundation based on risks. A vast majority of Indian organisations (81%) have adopted a security framework or, more often, an amalgam of frameworks, mostly with very good results. The two most frequently implemented guidelines are ISO 27001 (53%) and the US National Institute of Standards and Technology (NIST) Cyber Security Framework. These guidelines enable organisations to identify and prioritise risks, detect and mitigate security incidents, gauge the maturity of their cyber security practices and better communicate and collaborate internally and externally. At the same time, around three-fourths of the respondents said that their organisations have an overall information security strategy in place.

Frameworks such as the NIST Cyber Security Framework and ISO not only bring together leading practices from across industry sectors and serve to improve risk-based security, but alsoprovide a platform for internal communication and external collaboration. Organisations are also leveraging risk based guidelines to improve the security performance of third-party partners, which is a keyconcern. They have found that frameworks can enable companies to more easily exchange information with business partners and suppliers, and communicateexpectations and concerns about the services they provide.

Current Situation:

In today's rapidly evolving threat landscape, threat actors are becoming more sophisticated, breaching the defences of business ecosystems and leaving reputational, financial and competitive damage in their wake. Organisations recognise its importance and have invested accordingly in the technological advances. Vulnerability scanning tools have seen an increase in adoption and are up from 57% to 62%. Intrusion detection tools have increased from 55% to 62%. Other major categories which have gained importance are malicious code detection tools, malware software and use of virtual desktop interface (VDI). Some organisations are exploring the use of data analytics for identity and access management to monitor employee usage patterns and flag outliers. In this scenario, the data analysis solution looks for patterns around the employee access entitlements and then identifies unwanted access. Organisations are already realising the benefits of advanced technologies to improve their information security environment and a sizeable number of them (53%) have listed implementation of newer technologies as their top priority in the next 12 months.

In today's interconnected ecosystem, the compliance of third parties to relevant security policies and procedures is important to maintain the overall security posture of the organisation. Surprisingly, we noted that 50% of companies do not ensure that third parties comply with their privacy policies, and around 40% of total organisations do not have established baseline standards for third parties.

As more businesses share more data with an expanding roster of partners and customers, it makes sense for them to swap intelligence on cyber security threats and responses. Indeed, overthe past three years, the number of organisations embracing external collaboration has steadily increased. These collaborations have proven to be highly beneficial for all parties. Most organisations say external collaborations allows them to share and receive more actionable information from industry peers, as well as government agencies such as CERT(Computer Emergency Response)-In.

Counter Measures:

Many say that information sharing has improved their threat awareness and intelligence. Organisations that do not collaborate often cite the lack of information sharing framework and standards as well as incompatible data formats and platforms among public and private entities as the reason. Another weakness is that cyber security updates are not communicated at network speed. Policies and regulations on data privacy

vary widely across the globe, and some organisations also worry that sharing certain types of data can violate the privacy of customers, employees and other individuals. And, of course, validation of intelligence is a concern for all. In India, the CERT-In function at the national level to coordinate cyber security emergency response and facilitate communication between other CERTs. CERT-In also issues guidelines, advisories and vulnerability notes to help organisations strengthen cyber security. The National Cyber Coordination Centre (NCCC) was recently approved by the government to coordinate intelligence gathering between agencies and handle issues related to national security.

Technological change continues to disrupt how organisations compete and create value in ways that often alter operating models. Some of the most significant business trends today, including the explosion of data analytics, the digitisation of business functions, and a blend of service offerings across industries, have expanded the use of technologies and data that is creating more risk than ever before.

The ecosystem of Internet-connected devices, operational tools and facilities is poised to soar in the coming years. Research firm IDC(International Data Corporation) predicts that the number of devices connected to the Internet will reach 30 billion in 2020, up from an estimated 10.3 billion last year. The Government of India recently launched the Digital India Programme and the Smart Cities Mission. Digital India aims at transforming India into a digitally empowered society while the smart city concept aims at developing 100 smart cities in India. These initiatives will boost the IoT(Internet of Things) industry in India. Citizens and business leveraging this technology will serve as a fillip to this industry. IoT has indeed come a long way from being a futuristic concept just a few years ago to transforming into real products, services, and applications. Smart watches, fitness bands and trackers, smart glasses, self-driving cars and drones are just the beginning of the endless possibilities.

As IoT continues to expand, analysis of machine-to-machine (M2M) data will become critical. In this type of data-centric environment, the importance of strong encryption cannot be underestimated. The security and privacy risks have been highly publicised. Hackers can hijack connected cars and control them remotely; digital snoopers can infiltrate home surveillance systems and monitor the behaviour of residents; and threat actors can compromise connected medical equipment and potentially impact the health and safety of patients. Vulnerabilities left unattended can result in grave repercussions from business losses to catastrophic establishment attacks.

Conclusion

An advanced and enhanced information security programme will not only enable companies to better protect themselves against cyber threats in the future, but also help create competitive advantages and foster trust among customers and business partners. The challenge, of course, is that it is exceedingly difficult to predict the future of cyber security when many aspects of its present state are uncertain and continually shifting. Nonetheless, we believe there are some assumptions that organisations should consider while preparing to enhance their cyber security over the next five years. First, any discussion of the future should be predicated on the premise that personal lives will be increasingly digitised, creating even greater avalanches of data that can be collected, analysed and potentially compromised. Businesses too will continue to generate and share more information about people and processes, and IoT will unleash a torrent of (M2M) data. Amid this escalation of data, individual and corporate identity, and privacy will begin to converge. In this type of data-centric environment, the importance of strong encryption cannot be underestimated. It's safe to assume that future threat actors will wield an attack kit of technically sophisticated tools and tactics. For governments and businesses, espionage and political hacking will merge as hacking techniques will become highly nuanced and aggressive. At the same time, increasingly brazen attacks by nation-state and politically motivated hacktivists will result in economic sanctions or possibly even cyber warfare. In fact, it's not entirely unlikely that a catastrophic cybersecurity incident will precipitate demand and support for government-controlled identity management. Furthermore, governments are working to improve their ability to trace and directly attribute intrusions to responsible threat actors. An empty indictment of individual cybercriminals or governments hasn't worked in the past and similarly will be ineffective in the future. Enforceable international treaties will be a necessity. Authentication and identity management are the juggernauts that pose the greatest perils to cyber

security and promise the greatest payoffs. Mustering the right defences will require new solutions based on big data, cloud computing and heuristic approaches. Forward-thinking companies are already shifting away from traditional perimeter defences in favour of cloud-enabled cyber security based on real-time analysis of data and user-behaviour patterns. Thinking ahead can help organisations stimulate discussion, explore possible scenarios and develop a strategy for cyber resilience. Doing so will help businesses build a forward-looking cyber security programme that is based on the right balance of technologies, processes and people skills—all supplemented with an ample measure of innovation. With these components in place, organisations are likely to be better prepared for the future of cyber security.

References

FORTNIGHTLY MAGAZINE Sept 30 - Oct 14 VOLUME 17 ISSUE 18 / 2016 NO. OF PAGES - 32 15 GLORIOUS YEARS OF SERVING IT INDUSTRY (SINCE 1999) www.ncnonline.net

Network Security and Cyber Risk Management Market in India PUBLISHED AUGUST 2016 www.mordorintelligence.com

https://www.wiseguyreports.com/sample-request/473959-network-security-and-cyber-risk-management-market-in-india-trends-and-forecasts-2015-2020