www.iirisconsulting.com

Subject: IIRIS Weekly Brief: India: A Cyber Crime Every Ten Minutes

INDIA: A CYBER CRIME EVERY TEN MINUTES

Introduction

Cyber crime is defined as “any illegal activity or unlawful act wherein the computer is either a weapon or target or both”. The range of incidents this year include, ransomware attacks like WannaCry and Petya targeting organizations, and the hacking of government websites such as those of the National Security Guard and the Union Home Ministry. This brief analysis looks at cyber-crime in India, its impact on business, response measures, levels of preparedness and future trends. It rounds up with a perspective on how cyber warfare affects national security.

Cyber Crime In India

As the risk of cyber threats looms over enterprises, a Symantec study in 2016 revealed that India ranks fourth when it comes to online security breaches, accounting for over 5% of global threat detections. The US and China occupy the top two slots and together make for almost 34%, followed by Brazil and then India.

According to the Computer Emergency Response Team (CERT-In), in July 2017, a total number of 44679, 49455, 50362 and 27482 cyber security incidents were observed during the year 2014, 2015, 2016 and 2017 (till June) respectively. From the global ransomware attacks that hit hundreds of systems to phishing and scanning rackets, at least one cybercrime was reported every 10 minutes in India in the first six months of 2017.The types of cyber security incidents include phishing, scanning/probing, website intrusions and defacements, virus/malicious code, ransomware, Denial of Service attacks, etc.

In May 2017, a ransomware called WannaCry targeted thousands of public utilities and large corporations globally, including affecting Indian companies. Then in June, another ransomware built upon this version with greater lethality. The ransomware went by many names such as Petya, NotPetya, Nyetya and Goldeneye. It infected networks in multiple countries including operations at the Jawaharlal Nehru Port Trust in Mumbai and the Pipavav Port in Gujarat.

The Ministry of Corporate Affairs and the Andhra Pradesh Police were also affected, along with several large organizations. According to some experts, Indian companies lose approximately INR 400 billion due to cybercrime every year. India is among the top 5 countries today in terms of the frequency and the number of cyber-attacks and is ill-prepared for such attacks, as loopholes continue to exist despite the patches for vulnerabilities.

Impact On Corporate Sector

The financial loss suffered from cyber incidents can be substantial. It can also lead to bigger risks such as disruption in business continuity, loss of reputation and customer trust, which can be detrimental, especially for industries that rely heavily on data and intellectual property. These sectors include Information Technology (IT), E-Commerce, Financial Services and Pharmaceuticals. The country is rapidly moving towards a digital economy and is increasingly being targeted by cyber criminals around the world. Increasing adoption of digital banking, wallets, mobile banking are some areas that might attract targeted attacks from cyber criminals.

According to an industry study, some of the weaknesses that have led to a rise in cyber-crime include:
Lack of processes to deal with cybercrime incidents. Inability to detect incidents effectively and being held back due to low understanding of the motive of the attack. Approaching an easily accessible team for help against contacting a cyber-crime specialist.

The weakest link in the cases of cyber-crime in corporates are the employees themselves. According to one report, employees are the second largest source of incidents after unknown hackers. This is because employees have not been trained to practice safe browsing habits and/or have been careless in handling sensitive data.

A key exploit used by hackers are the social media pages of employees. It is a veritable data bank, with several employees posting extensive details regarding their work profiles and personal information which enables a breach. Firewalls against such sites on corporate systems are not an effective deterrent, especially as information posted during non-official hours or divulged during online interactions cannot be monitored by firms.

As opposed to a wide field attack, latest cyber-crime attempts have become increasingly focused with targeted attacks becoming the norm. At least 26% of total cyber-attacks in 2016 were reportedly aimed at the technology, media, and telecom sector. The financial services sector has seen around 24% of all cyber-attacks. This has led the Reserve Bank of India (RBI) asking banks in February 2017 to report any cyber security incident within two to six hours. One of the more dramatic incidents involved an oil and gas company in 2015, where the email ID of a senior official was spoofed in order to get a client to transfer billions of rupees to the hackers account.

Response Mechanisms

The government is implementing a Crisis Management Plan for countering cyber-attacks, including mock cyber security drills, empaneling security auditing organizations to disseminate best practices, holding trainings for IT and cyber security professionals, launching the Cyber Swachhta Kendra (A Botnet And Malware Analysis Centre), and issuing advisories and vulnerability notes on the relevant websites. A National Cyber Security Agency would be helpful to let India respond to cyber attacks. However, while some progress has been made in India, including a law regulating the cyber-space, there is lack of any operational manual which describes the methods of investigating relating to cybercrimes. A Standard Operating Procedure (SOP) must be set so that the present force can conduct its investigation without any ambiguity.

Companies will have to work on their cybersecurity defense models on the following basis: Proactively identify current or future risks associated with an organization. Identify potential hacks based on cyber threat intelligence. Provide consistent and reliable response to the incidents. Investigate the incident and identifying the root cause. Incorporate assessment or investigation findings to the existing information security procedures.

Level Of Preparedness

Indian companies will have to be well equipped to be able to deal with cybercrime going forward. Recognizing the serious threat India faces, the Government announced an investment of INR 4 billion for a cybercrime control hub “Indian Cyber Crime Coordination Centre” (IC4), which will be set up to check cybercrime. One of the priorities of IC4 will be to check attempts by international gangs to penetrate the Indian Government’s official communication network and hack them.

According to experts, the vast majority of organizations are looking at cyber security as a compliance task and thus do the minimum possible to achieve that. According to a recent survey, less than half of Indian companies are planning to increase cyber security spends, indicating that incident response is still not on the priority list. Organisations need to understand that the quantum of losses suffered because of a cyber breach will continue to escalate in future, and there is a heightened need to make investments in building robust cyber diagnostic programmes, provide remediation approach, cyber threat intelligence and incident response.

Where We Assess It Is Likely To Head

Cyber crime in the near future is likely to head in several directions:
Targeting of organizations, particularly C-suite executives by ransomware in order to exchange the encrypted data for money Hijacking of smart devices connected to the internet in order to create massive networks that aim to disrupt web facing services Phishing and spoofing emails using social media information to breach organizations, steal personal information or perform identity theft Hacking mobile devices for credentials that can grant access to an organizations internal networks and data from anywhere Theft of cryptocurrencies that are independent of central banks and governments Targeting individuals and digital payment service providers in the current move towards a cashless society by taking advantage of loopholes and a lack of awareness

Cyber Warfare And National Security

India is extremely vulnerable to cyber-attacks on its national economy and infrastructure. This is highlighted by the fact that the Aadhar database, the Union Home Ministry, and the National Security Guard have already been hacked. All current technology being used by the government and the military are sourced from external vendors and have long been penetrated by other intelligence agencies. Officials in the government have previously claimed that hacks on the networks on India's National Security Council have originated in China. Chinese hacking capabilities are well known as shown be the targeting of Australian government networks, corporate espionage in Canada, hacking of South Korea over the US supplied missile defense, and even some speculations by experts that WannaCry originated in China and not North Korea.

In March 2009, a Canadian research team published a study of the GhostNet cyber espionage network that targeted over 1,300 hosts around the world including the German, Indian, Pakistani and Portuguese embassies globally and the Tibetan government in exile in India. M.K. Narayanan, the former National Security Advisor of India, stated that his office and other government departments were targeted on December 15, 2009 - the same date on which Google reported sophisticated cyber attacks from China. In March 2011, the government of India asked mobile operators to change the SIM cards of all mobile phones to indigenously made SIMs, as foreign SIMs could contain embedded worms which could adversely affect the functioning of cellular networks.

Over 700 websites of various central and state government departments have been hacked in the last four years, according to official data. India faces a multitude of challenges related to hardware, software and cyber literacy in order to be secure against criminals, nations and organizations that aim to exploit the vulnerabilities that currently exist.

In order to further enhance India's digital security credibility, it is recommended that the existing IT laws be revised to cater for newer dynamics on data integrity, push for speedier investigations and more international cooperation on cyber-crime. The need of the hour is for corporates to band together to present an alternative digital security framework to the government which could assist. One recommendation is the creation of a National Cyber Security Agency (NCSA) as an answer to the challenge. An NCSA would improve India's resilience and defense systems. It would also be responsible for a wide range of cybersecurity transformations in the area of policy formulation and its implementation at the national level.