# The WannaCry Ransomware attack: Raising the stakes of Cyber-Security in India

*Image: Reuters*

***By Nandavarapu Kiran, Blueocean Market Intelligence***
**Published date: June 8, 2017**

The ‘WannaCry’ ransomware struck in May 2017, to once again remind countries of the importance of Cyber Security. First identified in UK, it later spread to Russia, Ukraine, India, Taiwan, Tajkistan, Khazakhstan, Luxembourg, China, Romania etc., to about 150 countries that have faced the severity of the attack. Being highly destructive and infectious, it has affected more than 10,000 organizations and 2,00,000 individuals worldwide. India has been one of the worst victims of this cyberattack, being the third largest country to be affected, and about 48,000 computers being hacked. West Bengal, Maharashtra, Gujarat, NCR (Delhi) and Odisha were the top five states with the maximum number of detections. It has been found by cyber security experts that only those computers running Microsoft Windows, which have installed neither the security

patch that the company released in March 2017, nor the emergency patch it released for older Windows systems in May 2017, have been affected.

To accommodate the growing needs of globalization, digitization has become inevitable. Especially with regard to a workforce that is scattered and disconnected, the rise in the number of devices (BYOD), has in fact made life easier, through greater accessibility, collaboration, engagement and productivity. This is slowly progressing, to make the devices feel connected, dependable, complex and vulnerable as well. Unconsciously an alarming threat has crept in, and this is undoubtedly going to increase. While we embrace fast paced innovation, and digitization, “sustainability” has to be kept as top priority. Only by being proactive, aware, and communicating a culture of being ethical in handling devices, can an organization remain protected.

Globally, the US, China, Germany and Britain are the countries typically prone to cyber-attacks, including the most recent ones on Walmart, Sony, Yahoo etc. However, over the recent couple of years, India has been emerging as an attractive destination for malicious activities too. It has never been targeted, or exposed to attacks before, as much as it is being now. This is mainly because of the growing digitization, resulting in India facing higher visibility, thus increasing the chances of attacks. The attack at Zomato, ICTC Hack, and Bangladesh bank hack, are some of the attacks, which recently made headlines in the sub-continent. The maximum risk prone countries such as the US, have already begun exploring the reasons behind the attack and taking measures to resolve the issue. It is now India’s turn, which has now begun experiencing the criticality, and the necessity to think seriously about the problem and a solution to minimize the impact.

On further analysis of the attack in India, the incident has revealed that a majority of those affected are government bodies, a few notable ones being Andhra Pradesh police, the computers at panchayat offices of Kerala’s Wayanad and Pathanamthitta districts, West Bengal Electricity Distribution Company, Gujarat government’s WAN, Southern Railway Divisional Office in Kerala’s Palakkad district, and Tirumala Tirupati Devastanam (TTD). This clearly reveals the tendency of the victims to ignore, and of being careless with regard to cyber security and its implications. While on the one hand,

the Government emphasizes on digitization, cashless economy, smart cities etc., on the other, the most important ‘security’ aspect of it is being overlooked. The incident has also exposed the ‘’vulnerability’’ of India to such types of attacks, and has additionally brought out in the open, the numerous pirated software and outdated licenses present in the market.

One major reason behind the occurrence of these attacks is that, most of the companies are still not very serious about the allocation of a substantial security budget. Businesses are more concerned about aspects related to revenue generation and business expansion. The overall spending on cyber security is quite low, an average of about 5.6% of the overall IT budget. This leads to a security department being formed ‘’for the sake of existence’’, with several loopholes. And hence, when an attack strikes, or such a need arises, companies only think of a temporary solution to resolve it internally. This has exactly been the case with the WannaCry attack as well.

Furthermore, reporting of a cyber-breach has not become mandatory for a corporate firm, which tries to conceal it fearing damage to their reputation and image. This entire mindset has to undergo a radical change, and a serious realization has to set in. Cyber Security awareness has to be ‘thought of’, ‘endorsed’ and ‘addressed’ with equal priority, as that of any other business division. A Chief Information Security Officer (CISO), with a solid cyber security team should be made mandatory in every organization, driving the entire process and establishing it as significant component of every stakeholder in every company.

It is unfortunate that organizations don’t make it stringent to follow even the minimal security measures or practices those are required. It is high time that every company realizes the importance of cyber security and starts to ‘Act’, instead of ‘React’ after every adverse occurrence. It becomes very essential to get at least their first line of defense in order, such as, installation of Anti-Virus with firewalls in every system, efficient Data backup system, Authentication, proper encryption at the user end, and creation of specific access controls. Once this preliminary set up is in place, there has to be diligent maintenance of up to date versions of all software, operating systems and antivirus packages. Regular maintenance of security patches has to be strictly ensured

as well, and any data that is accessible through the public domain has to be doubly secure, and ensured that it is not compromised.

In the case of small and medium businesses, managing the resources, cost and time, can be quite challenging.  Cloud computing technologies can be the best alternative to handle in this situation. In addition to efficient resource utilization, Cloud also helps in saving maintenance, management and monitoring costs, as the responsibility lies with the service provider. The data also becomes more secure as it is maintained in a separate network, outside of the office network, which can be easily disconnected in case of any attack.  Periodical reviews, audits and awareness, can guarantee a safe and defensive organization.

Cyber Security attacks in the form of ransomware, malware, phishing, etc., are definitely nothing new. Hackers keep on trying to find an opportunity from within the smallest loophole existing in the system. Several Threat intelligent systems are still nascent and are still emerging to defend and help organizations safeguard their data and resources. Deception and Diversion tools and technologies is another innovative weapon that is emerging to counter the attack from hackers. Gartner predicts that by 2018, 10 percent of enterprises will use deception tools and tactics, and will actively participate in deception/diversion ions against attackers. Cyber situational awareness and Cyber-crime training can be periodically fed into the minds of the all the stakeholders across businesses. India may still have a long way to go before it catches up with the advanced countries in terms of the volume of data generated, but it has already begun to emerge as a threat prone market. Hence it is essential to address the issue at this stage, as an early and combined effort of both the public and private sector could help save the situation, before things get totally out of hand.

*The author is the Director of Hi-Tech Practice at* ***Blueocean Market Intelligence***

**Source:** *http://tech.firstpost.com/news-analysis/the-wannacry-ransomware-attack-raising-the-stakes-of-cyber-security-in-india-381327.html#disqus_thread*