Briefing Paper

Cybersecurity Challenges for Indian MSMEs

Introduction

The advancement in digital technologies has transformed businesses and processes across the globe. More importantly, the shift towards the adoption of digital technologies is prominent in developing countries, such as India.[1] The digital economy contributes about 14 percent to India's gross domestic product (GDP) and is expected to grow up to 20 percent by 2024.[2] Similarly, digital adoption by the people has been growing at an unprecedented rate in all the regions of the country.[3] More importantly, the move towards digital technologies and tools has been significantly accelerated due to the COVID-19 pandemic.

All of these are sustained by an infrastructure called cyberspace, a connected internet ecosystem.[4] As in the offline world, the internet ecosystem also has its vulnerabilities and threats called cyber threats. These vulnerabilities and threats affect individuals and enterprises causing them losses of billions of dollars globally.[5] To this end, cybersecurity[6] strives to protect systems including networks, applications, and resources from cyber threats and cyberattacks.

Importantly, the incidences of cyberattacks have grown exponentially over the years, and particularly in India, the reported cybercrime increased by 121 percent between 2016 and 2018[7] and was also the second most cybercrime-affected country in the world.[8]

This growth in cybercrimes and increasing cyber threats makes it evident that the need for cybersecurity is more prominent than ever, which is further important for vulnerable businesses such as micro, small and medium-sized enterprises (MSMEs) with weak system protection and low awareness. Since many businesses are now engaged in working and operating from home without the comprehensive security framework of a workspace, the need for cybersecurity is further heightened. A study by Cisco indicated that about 73 percent of Indian organisations reported more than a 25 percent rise in cyber threats while working and operating from home.[9]

MSME Classification in India		
Composite Criteria for Manufacturing and Services Enterprises: Investment And Annual Turnover		
Micro	Small	Medium
Investment < Rs. 1 crore and Turnover < Rs.5 crore	Investment < Rs. 10 crore and Turnover < Rs.50 crore	Investment< Rs. 20 crore and Turnover < Rs.100 crore

Source: Ministry of Micro, Small & Medium Enterprise, Government of India[10]

Use of Digital Tools by MSMEs in India

A 2018 survey conducted by Kantar for Tally Solutions revealed that almost 35 percent of MSMEs among 2250 respondents across 34 cities in India including 13 Tier-II[11] cities have adopted business management software.[12]

Almost 40 percent of the respondents were based in Tier-II cities. This signifies the value that the businesses are putting on digital tools for their operations in Tier-II cities. Amongst the businesses that have adopted digital technologies, almost 43 percent of the MSMEs are using online banking and digital payments. Also, almost 80 percent of these MSMEs are using desktop or laptop and 35 percent are using smartphones for their businesses.[13]

However, the adoption of digital tools by MSMEs has increased after the COVID-19 pandemic and has encouraged companies to go digital, inwards and outwards. Inward digitalisation pertains to the efficient management of business processes using business management software and outward digitalisation pertains to making business transactions contactless and increasing quality of service. A report by KPMG estimated that by 2022, about 80 percent of the revenue in a business will be generated online, thus highlighting the increasing importance of digital and online tools.[14] Similarly, adopting digital tools is estimated to increase revenue for MSMEs by 34 percent.[15]

Another report 'Indian MSME Impact Report 2019' by Instamojo highlights some critical challenges that affect MSMEs. The challenges include the absence of adequate bank credit/finance, limited knowledge of business, non-availability of technology support, complex taxation norms, lack of marketing skills, constraints on the expansion of business, non-availability of skilled labour, lack of creating skill development, poor/inadequate logistics infrastructure, and complex legal norms.[16]

Instamojo reports that 47 percent of MSMEs that are using digital payment solutions are only able to manage a few critical challenges. Most importantly, the report mentions that about 20-30 percent of respondents who are able to manage these challenges smoothly are only able to do that by learning new technologies, taking expert help, or gaining considerable experience using the technology. While 75 percent of the MSMEs are optimistic, that technology will help them solve the challenges. This

signifies that MSMEs have limited knowledge of using technology to address some of their challenges, while they are interested to use them. Thus, causing the businesses to be exposed and vulnerable to cybersecurity threats.

Cyber Threats and MSMEs

Types of Cyber Attacks

Cyberattacks is a significant threat to enterprises and individuals as it takes discrete and disguised forms.[17] The following are the types of common cyberattacks, but not limited, as detailed by Cisco are:

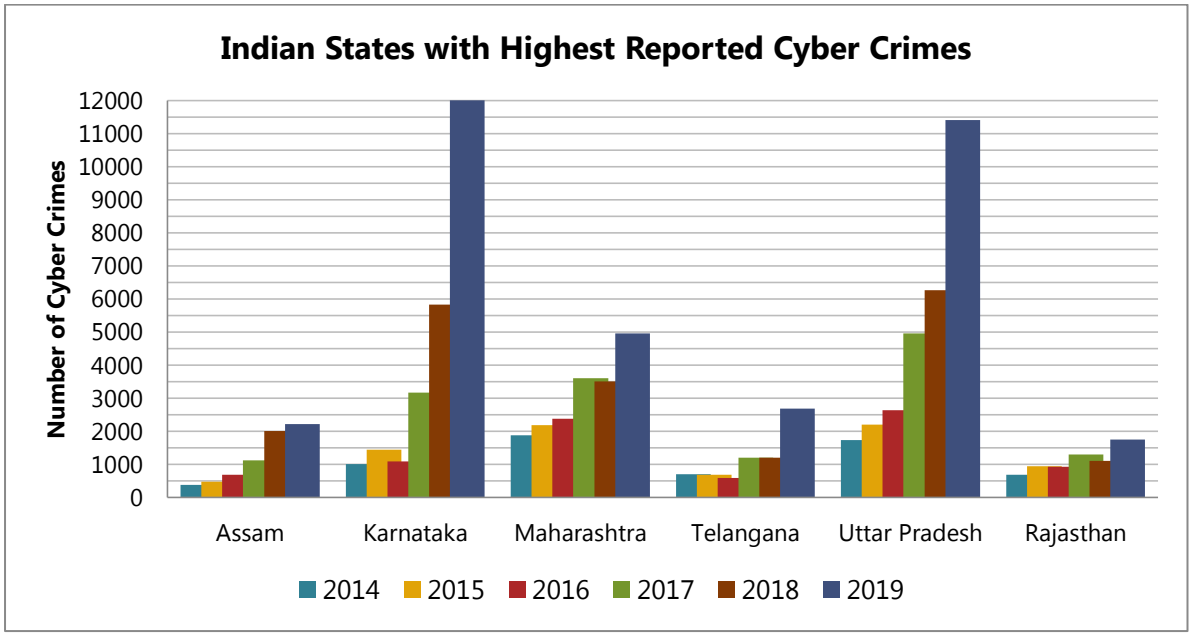
Type of Cyber Attack	Description
Malware	Malware is malicious software that includes spyware, ransomware, viruses, and worms. Generally, malware breaches a network through vulnerability, typically when a user clicks a suspicious link or downloads an email attachment, and thereby installs the risky software.
Phishing	Phishing is a form of fraudulent communication that appears to come from a reputable source. The objective is generally to steal sensitive data, such as credit cards and login information by make believing people in the authenticity of the communication.
Man-in-the-middle attack (MitM)	MitM attacks, also known as eavesdropping attacks, occur when attackers insert themselves into a two-party transaction. Once the attackers interrupt the traffic, they can filter and steal data. This attack is administered most commonly through Public Wifi.
Denial-of-service attack	A denial-of-service attack floods systems, servers, or networks with traffic to exhaust resources and bandwidth. As a result, the system is unable to fulfill legitimate requests.
Ransomware	Ransomware is a kind of malware that first hijacks a computer, then encrypts files and denies access to the user. The attackers then demand ransom from victims to decrypt files.
Structured Query Language (SQL) injection	SQL injection occurs when an attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not.
Zero-day exploit	A zero-day exploit hits after network vulnerability is announced but before a patch or solution is implemented.

Amongst these, phishing is the most common and prevalent cyberattack, next is malware. To give an overview, India witnesses 2nd highest phishing attacks in the world.[18] According to the report – Impossible puzzle of Cybersecurity from Sophos, 59 percent of cyberattacks victims was targeted

through phishing emails and 39 percent by ransomware.[19] This same report also highlights that India is also one of the leading victims of malware attacks.

Increasing Cyberattacks

The Ministry of Electronics and Information Technology (MeitY) has informed the Parliament that in 2020, India witnessed about seven lakh cyberattacks on citizens, commercial and legal entities due to the proliferation of the internet and mobile phone.[20] The following graph highlights the top Indian states with the most number of reported cybercrimes over the last six years:



Source: National Crime Records Bureau

According to a survey by Kaspersky, about 48 percent of MSMEs among 1139 respondents have had data breaches in their businesses in 2019.[21] The primary vulnerabilities for the data breaches were a lack of understanding of threats and the importance of security in the MSMEs.[22]

Loss to Business from Cyberattacks

Cyberattacks expose sensitive personal, financial and business information, disrupts critical operations, and imposes high costs on the economy. Some of the cybercrime costs include damage and destruction of data, forensic investigation, fraud, post-attack disruption to daily business, monetary and productivity loss, embezzlement, reputational harm, and identity and intellectual property theft.[23]

According to a study by Frost & Sullivan for Microsoft, large-sized companies in India lose an average of US$10.3mn annually due to cyberattacks, while mid-sized companies lose US$11,000 annually.[24] The National Cyber Security Coordinator, Lt. Gen. Rajesh Pant stated that India lost about Rs. 1.25 lakh crore in 2019 from cybercrimes. Most recently, a popular food chain Haldiram witnessed a ransomware attack on its servers, where the hackers have reportedly demanded a sum of US$750,000 to release the data.[25]

Vulnerabilities of MSMEs

With lack of awareness, low organisational priority and lack of skilled personnel make MSMEs an easy target, according to a survey by ESET.[26] Indian MSMEs were the most vulnerable to cyberattacks for the consecutive three years leading to 2016.

Some of the vulnerabilities of MSMEs in cybersecurity include a shortage of qualified personnel due to lack of affordability, lack of capital allocation for cybersecurity, using smartphones for business transactions, and employee carelessness. While these are some major concerns, evolving cybersecurity technology has been one of the significant constraints for MSMEs in adapting to a changing world.

Lack of awareness or knowledge is a fundamental vulnerability where the MSMEs do not always know if they have been attacked or breached. Similarly, the business owners may not be aware that the data has been leaked, how much of their data has been leaked and what type of data has been leaked.[27] This is also substantiated because of the lack of cybersecurity personnel in their organisations.

Additionally, MSMEs may also hesitate to report cyberattacks on them to law enforcement agencies as these businesses fear a loss of reputation exposing their vulnerabilities.[28]

Cybersecurity Challenges for MSMEs

According to a survey report by ESET,[29] some of the main challenges for MSMEs in implementing cybersecurity solutions are:

- Cybersecurity is not a priority for MSMEs.
- Capital allocation is a huge constraint for MSMEs. Businesses prefer to use funds for scaling up their operations instead of investing in cybersecurity.
- MSMEs outsource their technology and regulatory compliance to third-party vendors and service providers. Examples include handing out digital signatures to chartered accountants to submit tax/goods and services tax returns. However, the vendors and service providers may not have a comprehensive cybersecurity framework to protect the sensitive information of their clients.
- Lack of skilled and qualified personnel in cybersecurity. MSMEs are averse to making comprehensive investments fearing that the return of safety would be wasted since technology and associated threats are rapidly changing.

- Bringing and using personal devices by the employees to access the workplace network for their personal use may leave the network unprotected.

Cybersecurity Best Practices

The following list of practices may direct the MSMEs towards a basic approach to cybersecurity.

Strategy	Description
Management and Employee Awareness	Awareness is the fundamental key to cyber precaution and protection. Understanding this basic approach, MSMEs should train the management and employees to identify phishing emails and messages, suspicious websites and regulate policy for use of personal devices on the official network.
Unified Threat Management/Firewall	The most primary and basic approach to securing a business is installing a firewall, intrusion detection system and intrusion prevention system.
System and Software Update	MSMEs should regularly update their computer systems, browsers, applications, antiviruses, etc. to patch security vulnerabilities in the system and software.
Paid Softwares and Tools	Free software does not provide comprehensive and multi-layered security and protection for the business. Thus, MSMEs should avoid free security and anti-malware software that are easily available online.
Data Backup	Data backups help safeguard and preserve organisational data, if it is lost due to a cyberattack. Thus, MSMEs should regularly backup data and distribute backup storages between cloud storage and servers including removable media if the data volume is not too large.
Engage IT Expert	MSMEs should employ a dedicated IT department to regularly monitor and review software and security configurations of the business.
Hiring Reputable Service Providers	MSMEs should be cautious and informed while hiring a service provider and assess if the provider invests in cybersecurity management and recovery framework if it loses business data in any cyberattack.
Multi-factor Authentication	To prevent any unauthorised access, MSMEs must add a layer of protection using multi-layer authentication.
Revisit Password practices	Businesses must adopt a password change policy for every device that should be updated every 60-90 days and ensure a policy to encourage creating complex passwords.

The adoption of these approaches is also dependent on some of the challenges that were highlighted above. Overall, there is an increasing immediate need for the MSMEs to prioritise cybersecurity as a business strategy than anything else.

Way Forward

The role of MSMEs is critical to the growth of the economy and employment. As businesses are turning to use more digital and internet tools for their operations and otherwise, it is very critical that organisations also take initiatives to protect against the prevalent cyber threats. The number of cybersecurity incidents is rapidly increasing over the years as individuals and companies are migrating online.

MSMEs are very prone to cyberattacks as they have a shortage of qualified experts and personnel due to lack of affordability, inadequate capital allocation to cybersecurity, low cybersecurity prioritisation, negligence by their employees in accessing and using the internet. The literature on cybersecurity challenges for MSMEs and point towards a need to conduct capacity-building workshops, to make them aware of the cyber threats and enable them to take proactive actions against increasing cyber incidents.

---

1 https://meity.gov.in/writereaddata/files/india_trillion-dollar_digital_opportunity.pdf

2 https://economictimes.indiatimes.com/tech/internet/why-cybersecurity-should-be-indias-foremost-priority/articleshow/71843562.cms

3 Supra Note 2

4 https://niti.gov.in/sites/default/files/2019-07/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf

5 https://assets.kpmg/content/dam/kpmg/in/pdf/2017/12/Cyber-Crime-Survey.pdf

6 International Telecommunication Union (ITU) defines cybersecurity as "collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies to protect the cyber environment and organisation and user's assets. https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

7 http://164.100.24.220/loksabhaquestions/annex/173/AU1384.pdf

8 https://inc42.com/buzz/cyber-attacks-india/

9 https://ciso.economictimes.indiatimes.com/news/indian-companies-reported-over-25-jump-in-cyber-threats-while-wfh-cisco/78806763

10 https://msme.gov.in/sites/default/files/AtmanirbharPresentationPart-1BusinessincludingMSMEs13-5-2020_0.pdf

11 The Reserve Bank of India classifies cities in Tiers based on the city population. Tier 1 city is population 1 lakh and above, Tier 2 is between 50 thousand and 1 lakh, Tier 3 is between 20 thousand and 50 thousand, Tier 4 is between 10 thousand and 20 thousand, Tier 5 is between 5 thousand and 10 thousand and Tier 6 is below 5 thousand.

12 https://www.cii.in/webcms/Upload/63349Statesman.pdf

13 *Ibid*

14 https://inc42.com/resources/adoption-of-digital-tools-by-smaller-businesses-is-not-a-second-option-anymore/

[15] https://yourstory.com/smbstory/mastercard-msmes-digital-payments-india-covid-19

[16] https://www.instamojo.com/instamojoebooks/indian-msme-impact-report-2019/?utm_source=blog&utm_medium=interlink&utm_campaign=instamojo

[17] https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html#~types-of-cyber-attacks

[18] https://www.business-standard.com/article/news-ians/india-2nd-in-list-of-top-phishing-hosting-nations-report-119052300970_1.html

[19] https://secure2.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-impossible-puzzle-of-cybersecurity-wp.pdf

[20] https://www.hindustantimes.com/india-news/nearly-7-lakh-cyber-attacks-in-2020-it-ministry-tells-parliament/story-bOv6SuWSP9XxUwtF9uBTvK.html

[21] https://www.kaspersky.com/about/press-releases/2019_third-of-small-companies-suffered-a-data-breach

[22] *Ibid*

[23] Ahmad, Tabrez, Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity (April 5, 2020). Available at SSRN: http://dx.doi.org/10.2139/ssrn.3568830

[24] https://www.pymnts.com/news/security-and-risk/2018/microsoft-india-financial-loss-cyberattack/

[25] https://ciso.economictimes.indiatimes.com/news/noida-cyber-cell-probing-haldiram-ransomware-attack/78760860

[26] https://economictimes.indiatimes.com/tech/internet/heres-why-indias-small-businesses-are-sitting-ducks-for-cyber-criminals/articleshow/60921023.cms?from=mdr

[27] http://www.iiakm.org/ojakm/articles/2019/volume7_1/OJAKM_Volume7_1pp14-26.pdf

[28] *Ibid*

[29] https://economictimes.indiatimes.com/tech/internet/heres-why-indias-small-businesses-are-sitting-ducks-for-cyber-criminals/articleshow/60921023.cms?from=mdr

This Briefing Paper is an output of the project 'Cyber Safe East India – Workshops on Cybersecurity for E-Businesses' being implemented by CUTS International with support from the U.S. Consulate General, Kolkata and is authored by Kapil Gupta, Assistant Policy Analyst, CUTS International. The author acknowledges the valuable inputs from Udai S Mehta, Arnab Ganguly and Sumanta Biswas from CUTS International and Raymond Tavares and Jaidev Dhavle from UNIDO, towards finalising the paper.

February, 2021