A Quarterly insight to Cyber Law!

Cyber Niyam means rules of the Cyberspace. This quarterly newsletter aims to create awareness about the rules and regulations of cyberspace, cyber security and data protection. This is also an effort to create awareness about digital safety, trending cybercrimes and effective reporting mechanisms.

Disclaimer

This newsletter does not intend to advertise or solicit work and is for private circulation only. This newsletter is for the purpose of education and creating awareness on Cyber law and its latest developments. It does not intend to be comprehensive nor intends to provide any legal advice. Though every effort is made to share accurate, reliable and current information, Cyber Niyam is not responsible for any errors or omissions in information made available through this Newsletter. Sharing of this Newsletter does not intend to create attorney – client relationship between authors and reader.

CYBER NIYAM

By Adv. Vaishali Bhagwat *www.vaishalibhagwat.com*

Issue 3 of 2025 – October, 2025

In this Issue

CYBER FRAUDS AGAINST MSMEs

Introduction

Cyberattacks against Indian MSMEs are on the rise due to increased digitization and their typically limited budgets for robust cybersecurity, making them vulnerable to cyber-attacks that can halt operations and cause severe financial losses.

Key factors contributing to this vulnerability include a lack of security expertise, inadequate resource allocation, and insufficient security frameworks. Consequently, a single security lapse can impact the entire supply chain and critical infrastructure, highlighting the need for proactive security measures.

Hence, CERT-IN has issued guidelines providing recommendations for MSMEs to safeguard themselves against cyber-attacks.

.....Continued on page 2

Types of cyber attacks

Ransomware Attacks

Ransomware is a type of malware that locks and encrypts a victim's data, files, devices or systems, rendering them inaccessible and unusable until the attacker receives a ransom payment. While some simple ransomware may lock the system without damaging any files, more advanced malware uses a technique called crypto viral extortion

Distributed Denial of Service (DDoS) Attack

A DDoS attack is when a business organisation's server is overwhelmed with excessive traffic, which causes slowdowns or complete shutdowns. A DDoS attach can render a business website offline to legitimate users which affects business operations.

Phishing and social engineering attacks

These attacks involve deceptive emails, text messages or fake websites designed to trick employees into revealing sensitive information like passwords or other confidential data.

Malware and Viruses

Malwares or viruses are infected files or malicious websites which can infiltrate the IT infrastructure of a business organisation and collect data or corrupt files.

Employee practices

Employees can post a threat either due to malicious intent or due to unintentional negligence due to lack of awareness such as clicking on phishing links or not respecting access controls, not keeping sensitive data secure. Such practices can lead to leakage of confidential data or exposing the IT infrastructure of the business organisation to cyber attacks

Data Breaches

Data breach is an unauthorised access and release of secure information. Such data can include business information, personal data, confidential information of third parties. Such data leakage, where it is attributable to weak information security practices leads to business disruption, breach of contractual obligations and can invite penalties from regulatory bodies.

Weak Passwords and Authentication

MSMEs make the mistake of not having a strong password system across all their communication channels. Weak passwords or a lack of multi-factor authentication can make it easier for cybercriminals to get access to sensitive information.

Outdated Softwares

MSMEs lack the resources or awareness to regularly update their software with latest security updates and patches which makes them vulnerable to a wide range of cyber attacks

GOOD TO KNOW!

What is CERT-IN?

CERT-In, an acronym for 'Indian Computer Emergency Response Team', is the National Incident Response Centre for major computer security incidents in its constituency i.e. Indian cyber community. It was formed in 2004 by the Government of India under Information Technology Act, 2000

CERT-In's primary role is to raise security awareness among Indian cyber community and to provide technical assistance and advise them to help them recover from computer security incidents.

It provides technical advice to System Administrators and users to respond to computer security incidents.

It also identifies trends in intruder activity, works with other similar institutions & organisations to resolve major security issues, and disseminates information to the Indian cyber community. It also enlightens its constituents about the security awareness and best practices for various systems; networks by publishing advisories, guidelines and other technical document

RESPONSE TO CYBER FRAUDS

If your organisation has fallen victim to a cyber-attack–

1. Remain calm

Reporting

2. Report on National Cyber Crime Reporting Portal at www.cybercrime.gov.in
3. File a complaint to Local Cyber Crime Cell
4. Report the incident to CERT-IN within
5. Report to Bank in case of financial information leakage

Steps at organisational level

6. Taking steps to ensure stop/.contain the attack
7. Taking steps to mitigate
8. Informing customers in case of breach of their data
9. Taking steps to recover from the cyber attack
10. Cyber Insurance invocation

CYBER SECURITY

Importance of Cybersecurity

Cyber threats are constantly evolving and each organisation faces risks irrespective of its size.
Hence, it becomes important for all organisations to ensure and their IT systems and data are secure.
Cybersecurity is important for a business for a variety of reasons:

1. It helps to keep secure the IT infrastructure of an organisation,
2. Prevent the leakage of confidential data (including financial information, personal data, client data, business secrets etc) which resides with the business organisation.

Benefits at organisational level

This security in turn helps the organisation

1. To adhere to the applicable laws of the country,
2. Ensures that the business operations run smoothly without disruptions,
3. Support the digitisation of business processes of the business organisation
4. Ensure confidence of customers in the business organisation

all of which in the long run help to the business efficiently and thereby maximise the profits if the organisation.

CERT-IN recommendations

CERT-IN has provided certain recommendations for MSMEs in order to ensure their organisations is secure from a cybersecurity perspective. While the documents is not mandatory in nature, it would be highly beneficial to MSMEs to implement the recommendations to ensure smooth business operations and continuity.

Recommendations

1. Management of IT assets
   - maintenance of inventory of all hardware, software, data
   - Ensuring the inventory is updated from time to time
   - In case of sensitive assets (core software, databases etc) there should be proper identification, labelling and classification
   - Tracking of the entire lifecycle of the IT assets which shall include acquisition, secure disposal of the asset, change of location or condition

2. Network security
   - Deployment of firewall software
   - Wi-Fi networks should have WPA2/WPA3 encryption standards
   - Strong passwords
   - Hidden SSIDs (The wifi network does not appear in the list of wifi networks. To connect, you need to manually enter the network name (SSID) and password)
   - Segregation of networks used by third party/guests from internal network systems (Wi-Fi or LAN)
   - Devices should not automatically connect to public WI-FI networks
   - Enforcement of secure wireless configurations across all devices so that every device connecting to the business organisation's Wi-Fi is secure

3. Emails
   - Protection of Email systems from phishing, spoofing using Sender Policy Framework, DomainKeys Identified Mail and Domain based Message Authentication, Reporting Conformance. All these systems help to provide proof of the sender's authenticity.

4. Computers or mobile phone devices
   - Installation of antivirus on all devices
   - Using licensed versions of antivirus software (as against pirated software) and ensuring it is regularly updated
   - Using built in security features of the operating system
   - Installation of anti-virus software by authorised persons only
   - Onboarding with CERT-IN's Cyber Swachhta Kendra which is a Botnet cleaning and Malware Analysis centre to receive alert and advisory on Malware and Botnet infections
   - Controlling and regulating use of external devices such as USBs/ Harddisks as they can be a source of malware

5. Secure configurations /settings
   - Implement set of minimum security settings for server (eg. admin password), devices (eg. antivirus, screenlock), internet browsers (disable unsage plugins), off the shelf software (disable unnecessary features)
   - Disable feature, services, ports which are not necessary for functioning of the hardware or software
   - Remove softwares, applications which are not being used
   - Change all default settings and passwords

- .... continued on page 5

6. Patch Management
   - Regularly applying security patches (software updates issued to fix vulnerabilities) and regular updates to softwares used by the organisation such as the operating systems, applications and firmware
   - Monitoring of security notifications/advisories from various entities such as the vendor, CERT-IN and any other relevant sources in order to remain informed regarding the latest patches and vulnerabilities affecting the IT infrastructure of the business organisation

7. Management of Cyber security incidents
   - Preparation of plan to deal with a cyber security incident which shall include reporting, containment, investigation, recovery from the incident and communication procedures
   - Conducting regular testing of IT infrastructure based on the plan to check its effectiveness
   - Ensure adherence to the directions issued under the IT Act relating to information security practises, response and reporting of cybersecurity incidents. CERT-IN directions require the reporting to CERT-IN of cybersecurity incidents within 6 hours of detection or notification of such incident.

8. Monitoring of systems
   - Enabling comprehensive logging (capturing wide range of events such as logins, file access, changes , errors, admin actions etc.) on all key Information and Communication Technology (ICT) systems (servers, databasese, applications etc) to ensure traceability and accountability
   - Retaining system logs (from servers, operating systems, network devices) and application logs (from business apps, databases, email systems etc) for a minimum period of 180 days with secure storage within Indian territory
   - Continuous monitoring of network activity and privileged user actions which will help to detect suspicious behaviour and unauthorised access attempts
   - Installation of security tools which will continuously monitor systems, analyse logs to enhance system and application logs automatically, detect threat quickly and help respond to them before damage occurs

9. Awareness and trainings
   - Conducting comprehensive cybersecurity awareness trainings regularly for all employees and contractors
   - Participating in cybersecurity workshops conducted by CERT-IN

10. Third Party Vendors
    - Conducting due diligence of third party vendors so as to ensure their systems and IT infrastructure is secure
    - Requiring third party vendors to apply, at a minimum, the same security standards as applied by the MSME business organisation

11. Data management
    - Regular backing-up of data (daily or weekly)
    - Storing of copies of back-up data in encrypted format on other networks/ devices
    - Testing of back up procedures to check recoverability
    - Preparing a business continuity plan
    - Ensuring secure disposal of both physical and digital media

12. IT Governance
    - Appointment of a point of contact to oversee all InfoSec activities and for coordination with regulators including CERT-IN
    - Prepare an information security policy which shall deal with data protection, access controls, incident response management, password policies, third-party management and audits
    - Regularly reviewing Information security policies
    - Ensuring adherence with guidelines and directions issued by regulators from time to time (including CERT-IN)

.... continued on page 6

14. Password Management
    - Use of strong and unique password
    - Locking of account after 3 to 5 failed login attempts
    - Enabling multi-factor authentication (eg. Password and OTP for allowing access) for all critical IT assets, administrative account and remote access tools

15. Access Controls
    - Assigning unique user IDs to all individuals and personnel within the organisation
    - Access to different email inboxes, servers etc shall be determined based on the nature of the persons role such as administrative, financial, data function etc.
    - Periodic review of access privileges

16. Physical Security of IT assets
    - Implementation of physical access controls for critical infrastructure systems
    - Security guards, electronic badges and biometric access (for sensitive areas including server rooms, areas hosing network equipment and other sensitive areas.
    - Monitoring entry and exit to the sensitive areas using CCTV
    - Maintaining comprehensive asset return checklist for every employee exit

17. Audits /Assessments
    - Conducting vulnerability assessments through independent parties of critical IT infrastructure at least annually
    - Remedying any vulnerabilities identified by such assessments
    - Performing periodic risk assessments to identify threats which are specific to the organisation

NEWS CORNER
Notification of DPDP Rules

The DPDP Act and its upcoming rules establish a framework for processing digital personal data, applying to all organizations that process the data of individuals in India.

The rules for India's Digital Personal Data Protection (DPDP) Act, 2023, are finalized and were sent for legal vetting as of early October 2025. While the full text of the final rules is not yet public, key aspects are known from the draft rules that were open for public consultation in early 2025.

NEWS CORNER
Pune's MIT World Peace University Duped of Rs. 2.46 crore in Fake Government research grant scam

Pune's MIT World Peace University (MIT-WPU) recently succumbed to a ₹2.46 crore cyber fraud where scammers impersonated high-ranking academics and tempted the university with the offer of the government-approved research funding. Pune Cyber Police has filed an FIR and started an investigation.

NEWS CORNER
Data Breach at Indian Council of Agricultural Research

A cyber-attack on the ICAR led to a major data breach that disrupted key recruitment processes and agricultural research projects across multiple institutes, though the identity of the threat actor remains unknown

GLOSSARY OF TERMS

What is a MSME

MSMEs are Micro, Small and Medium Enterprises which are classified as follows:

(i) a micro enterprise, where the investment in Plant and Machinery or Equipment does not exceed one crore rupees and turnover does not exceed five crore rupees;

(ii) a small enterprise, where the investment in Plant and Machinery or Equipment does not exceed ten crore rupees and turnover does not exceed fifty crore rupees;

(iii) a medium enterprise, where the investment in Plant and Machinery or Equipment does not exceed fifty crore rupees and turnover does not exceed two hundred and fifty crore rupees.

Under the provisions of the MSME Act 2006, an "enterprise" has been defined to means an industrial undertaking or a business concern or any other establishment, engaged in the manufacture or production of goods or engaged in providing or rendering of any service or services. MSMEs can also obtain UDYAM registration in order qualify as a MSME.

Cyber Insurance

Cyber insurance (also called **cyber liability insurance**) is a type of insurance policy that helps organizations **manage financial and operational risks associated with cyberattacks, data breaches, and other digital threats**.

ABOUT THE AUTHORS

Adv Vaishali Bhagwat

Vaishali Bhagwat is a practicing lawyer with 25 years of experience in civil and cyber litigation and advisory practice in Pune and Mumbai.
Vaishali has a prior degree and work experience in the field of Computer Science, a Post graduation certification in Cyber Security and Information Assurance and is a certified Privacy Lead Assessor.

She is an advisor to several companies on Cyber law and privacy compliance and advisor to various educational institutions on Protection of children from sexual offences.

She has successfully conducted several prominent cases for corporate espionage and Data theft, Data Privacy, Digital Financial Frauds, Cyber-crimes against women and children, take down orders and IP infringement in cyberspace.

Vaishali is a *TCS Chevening Scholar on "Cyber Policy and Cyber Defense" and has earned the Post Graduate certification from Cranfield University UK. She is also a Disha Alumni which is a prestigious program of the British high Commission on Innovative Leadership chaired by UK PM David Cameron and PM Manmohan Singh*.

www.vaishalibhagwat.com

Adv Kunal Gokhale
BSC. LLB (Hons.) (Business Law) Degree

Advocate Kunal Gokhale is a legal professional with nearly fourteen years of post-qualification experience. He is a graduate from the National Law University, Jodhpur and holds a BSc LLB (Hons.) (Business Laws) degree. Advocate Kunal Gokhale has significant professional experience in handling civil litigation matters with focus on commercial matters. He also provides advisory services in relation to drafting of various types of agreements and has been associated with firms such as Vaish Associates, Advocates (Delhi), Ernst & Young, India (Mumbai) and Luthra & Luthra Law Offices (Mumbai) in the past.

Mrudula Arjunwadkar
BSc., LLB, MPM

POSH Consultant
Helping organizations in end to end POSH Compliance, External member to IC, POSH trainings

V.P SHINTRE & ASSOCIATES