DOI: 10.15849/IJASCA.220328.08

Int. J. Advance Soft Compu. Appl, Vol. 14, No. 1, March 2022
Print ISSN: 2710-1274, Online ISSN: 2074-8523

A Comprehensive Review on the Cyber Security Methods in Indian Organisation

Dr. Deepshikha Bhatia

Sr. Assistant Professor, Department of CS&IT, IIS (Deemed to be UNIVERSITY), Jaipur (Rajasthan)
E-mail: deepshikhabhatia63@gmail.com

Abstract

Cyber security, an application that protects and controls the systems, programs, networks, data and devices from cyber-attacks. This cyber security practice used by individuals and small or large organizations for protecting against unusual data access. A powerful cyber security system provides a great security against malware attacks, viruses, ransom ware, cloud attacks, IoT attacks etc. and it designed for accessing, destroying, deleting and altering these attacks and secure the retrieving data from the server and user's systems. This paper discuss about the importance of cyber security in organizations of India. Surveys of Indian organization's cyber security measures are taken for the evaluation of the methods and challenges of cyber security. This comprehensive review provides insights about securing the data by employing cyber security frame works, risk assessment models and educating cyber security knowledge among public with help of government public programs. With these information this paper helps for overcoming the cyber threats and attacks and created a pre cautionary thought and also made a pre vision for diminishing theft of data among employees and tracking hacker's activities before attacking the organizations.

Keywords: *cyber security, Indian organization, cyber-attacks, cyber security methods, DDoS attack.*

1 Introduction

The present advanced world revolved around digital life and technology forced humans at greatest risk to cybercrimes than before. Cybercrime created a possibility of threat to specific one or firms that leaded to high loss in financially. The violation of data are instantly increased and technological world turned with cyber security for protecting confidential and sensitive data.

Received 26 November 2021; Accepted 22 February 2022

Cyber security had been a practice for protecting servers, computers, electronic systems, mobile devices, networks and data. Cyber security also been a path of defending other electronic gadgets from cyber criminals. It also well known in other words as electronic information or information technology security. The malicious attackers remove, rearrange or leak the valuable data that created an enormous threats to a business organizations or specific individuals. Cyber security helped for protecting data from attackers by ensured morality, availability and confidentiality of data.

The cyber security challenges for securing and safe guarding are

- Data security
- Application security
- Network security
- Disaster recovering for business continuation
- Mobile security
- Identity management
- Cloud security
- Infrastructure and database security
- Operational security
- End user education security

The huge financial loss in cyber security crimes created a necessity of cyber security in organizations and it had become one of the aspects of company's norms and procedures. The hackers had raised their standard for attacking into difficultly solved one and used unique tactics for hacking. It thrown down a risk for maintaining security up to data to organizations (Dixit & Silakari, 2021).

The motivations behind hackers for stealing sensitive data are financial gain by ransom attacks, for damaging the reputation of a firms, political causes, to insisted fear, to take revenge for personal reasons.

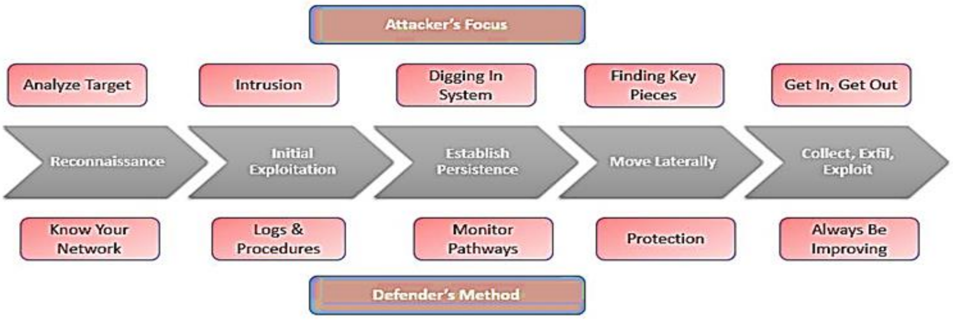


Fig. 1. Cyber security methods for security and defending the attackers

According to attackers motivation point of view cyber-attacks are divided into two types.

1) ***Passive attack***: The attacker's major motivation for retrieving sensitive information without damaging devices or systems and demanding the victim.
2) ***Active attack:*** The attacker rearrange or modified the information that created a threat to system sources and caused morality damage to system (Lezzi, Lazoi, & Corallo, 2018).

2 Need of the Study

Cyber security needed for daily working activities that ensures the data available in network when it needed, a small vulnerable caused huge damage to reputations of companies. It protected security, privacy and correctness of data. Basically, cyber security had been most important for military, government, medical, corporate and financial sectors for collecting, storing and processing unusual numbers of data on systems and other devices. (Raghavan, Desai, & Rajkumar, 2017) An important region of data must be with confidential details may be it had been a financial data, intellectual property, personal details or other types of data that cannot be easily accessed which caused unwanted consequences. Firms transmitting data over any networks because of business purpose and here, cyber security described for dedicating full protection on information systems that system used for storing data.

As mentioned above, (Adlakha, Sharma, Rawat, & Sharma, 2019) cyber security had been a significant thing that protect all types of data form stealing and damaging. Without a cyber-security application, organization must not defended oneself to face opposite to data stealing programs and it leaded to easily targeted by cyber criminals. Some advanced business companies installed modern snit virus software and fire walls but, cyber criminals were so smarter, they used difficult tactics for unlocking security. Cyber threats occurred in any stage of organizations so, the companies head must take responsibility for educating cyber security awareness among employees. Some of common attacks they must know about social engineering phishing, ransom ware and other malwares.

2.1 Need cyber security in India

In ancient history India had been a developing country, now in digital and internet systems it also a developing country. The public in India had enough knowledge about internet and web communication systems but not fully aware of cyber security system. The high rate of confidential data and information theft had been occurred in India. The matter of fact that individual, large or small business must relied on internets and systems so, cloud computing services, smart phones, and IoT devices are most probably used for developing technology up to data.

Governments must focus attention on the following instructions to secure data from threats and attacks.

a) Appointing a data protection officer.

b) Communicate data breaches.

c) Guarding data for privacy.

d) Required user permission for processing information

e) Securing measures for alarming those effects as soon as possible.

f) Government must know about those effects as earlier.

g) Paying some fine.

3 Recent Investigation of Cyber Security Methods

The cyber security methods created for overcoming threats and attacks. Some of cyber security methods are DLP (data loss prevention), IAM (identity access management), anti-virus, fire wall, proxies, cyber liability insurance etc. here, this study gone for investigating about new methods in cyber security that are used in recent studies (Uchendu, Nurse, Bada, & Furnell, 2021).

3.1 Latest cyber security measures in business environment

In recent days KM (knowledge management) played a major parts in cyber security. Hence (Wang & Wang, 2019) this study collected the five real time lively cases of KM for the practical implementation of cyber security measurements in business firms. The knowledge management depended on the organizational construction of significant extension. This specific domain focused on KM measurements for cyber security in organizations that revealed the regular particularized construction of three organizational tiers for cyber security of KM are: 1) organizational tiers 2) formal inter organizational tier 3) informal social networks tier.

3.1.1 The organizational tier

Included KM with grouped and specific users of information technology among the limits of business firms.

3.1.2 The formal inter organizational tier

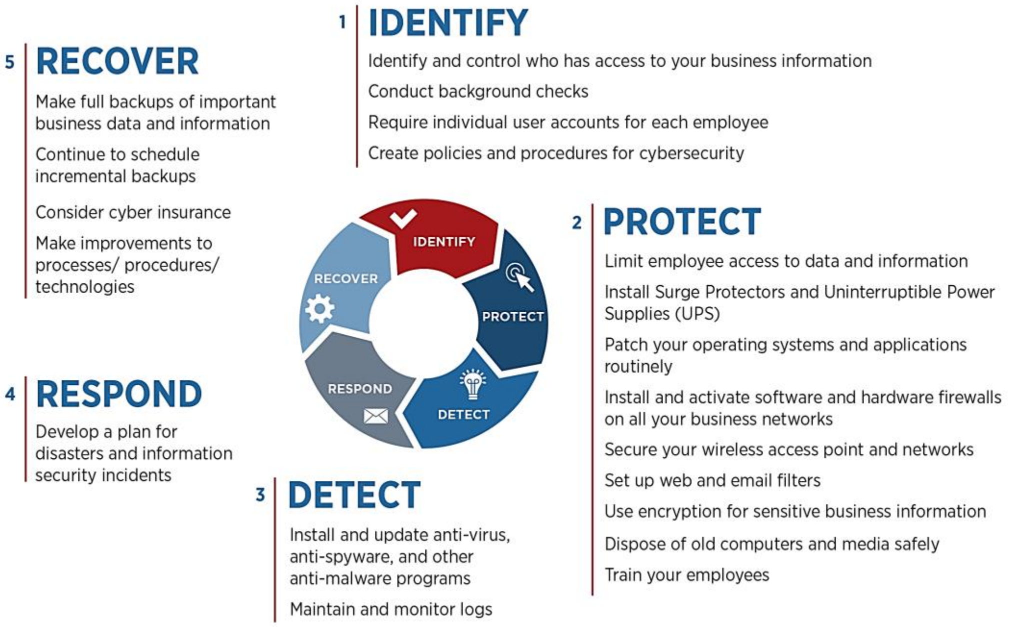
The knowledge management for cyber security involved inter connection between organizations that are combined. A common business firm’s compulsory worked with IT vendors for sharing the knowledge for cyber security.

3.1.3 Informal social networks tier

The explanation and skilled conversations by unofficial networks ride the learning of cyber security and knowledge sharing. The outcome of KM are frequently hard for measuring and it had been a constant and long run processes hence it hard accessing intermediated results.

3.2 Risk assessment in cyber security

The travel and tourism organizations sector had emerged in developing technologies that recreated services, consumer experiences and products, and also the cyber system increased vulnerability in security measures and risks. In past years this high profiled organizations created a negative impact of not showing any attention towards the risks in cyber security. Here,(Georgiadou, Mouzakitis, Bounas, & Askounis, 2020) some of attacks and threats that impacted negative feedback in travel and tourism sector are POS (point of scale) attacks, third party attacks, malware attacks, ransom attacks, cognitive hacks. Therefore, (Paraskevas, 2020) examined the cyber security measures an risks driven approach and it concentrated mainly on three areas for eliminating risks and implementing cyber security protected systems a) likelihood management b) consequence management c) organization’s human element.



1 IDENTIFY

- Identify and control who has access to your business information
- Conduct background checks
- Require individual user accounts for each employee
- Create policies and procedures for cybersecurity

2 PROTECT

- Limit employee access to data and information
- Install Surge Protectors and Uninterruptible Power Supplies (UPS)
- Patch your operating systems and applications routinely
- Install and activate software and hardware firewalls on all your business networks
- Secure your wireless access point and networks
- Set up web and email filters
- Use encryption for sensitive business information
- Dispose of old computers and media safely
- Train your employees

3 DETECT

- Install and update anti-virus, anti-spyware, and other anti-malware programs
- Maintain and monitor logs

4 RESPOND

- Develop a plan for disasters and information security incidents

5 RECOVER

- Make full backups of important business data and information
- Continue to schedule incremental backups
- Consider cyber insurance
- Make improvements to processes/ procedures/ technologies

Figure 2: Self-assessment tool for risk assessment for cyber security

(Toth, 2019) Study made cyber security assessment tool for identifying, protecting, detecting, responding, and recovering the business organization. Using these strategies risk assessment was created to eliminate cyber security threats in organization. Similarly, (Alali, Almogren, Hassan, Rassan, & Bhuiyan, 2018) described the effects of offender actions that based on the practical nature of offense and victim and on the basis of long term or short term impacted offended cyber-crime on internet world. Most recently many countries in world faced various types of cyber-attacks and threats like website defamation, denial of service (DoS), malware, phishing and spam email threats. Hence,(Humayun, Niazi, Jhanjhi, Alshayeb, & Mahmood, 2020) come into existence developed a unique cyber security risk assessment model for tackling the threats and attacks. Here, an FIS (Fuzzy inference model) produced risk assessment based model that used for the treating threat, vulnerability, used for particular order of risks that mistreated the complete entity and tried to resolve the problems in likelihood.

The sugeno type and mamdani type FIS techniques are used for assessing the risk calculations. However the resulted measurement earned only medium of 53.89% so it to be treated for further improvements.

3.3 A modern method for cyber security

The (Jeyaraj & Zadeh, 2020) present investigation examined in what way firms cyber security reactions became isomorphic over the period of time. Structuring on organizational theory, this study explained about the coercive pressures, mimetic pressures, and normative pressures were impacted in cyber security feedback and reactions. The inputted data had been collected from annual report of 10k organizations and it explained about reactions and responses of cyber security that controlled on the regard of previous security violations and accesses for sources of slackness.

The calculated measurements offered an initial proof of isomorphism in cyber security reactions and responses of firms but the sample space or size may examined as less.

Cyber security in nuclear power plants had been increased in recent times and also in related firms like manufacturing industries, regulators, operators and research institutes that considered with lots of concerned efficient applications of cyber security for difficult digital assets in nuclear power plants.

It had been an important for analysing and researching that how efficiently it applied for NCS (nuclear cyber security) needs. The supplementary points of NCS technology had been evaluated by various cyber security methods like assessments, SDL (software development lifecycle) and cyber security assurance. (Son, Choi, & Yoon, 2019) This paper implemented above methods effectively for applying, developing, regulating and evaluating cyber security nuclear power plants and its digital systems.

A socio-technical framework was utilized to identify and respond to any type of vulnerabilities which reduced the gaps between existing social and technical in information and cyber security solutions which shown in figure 3.

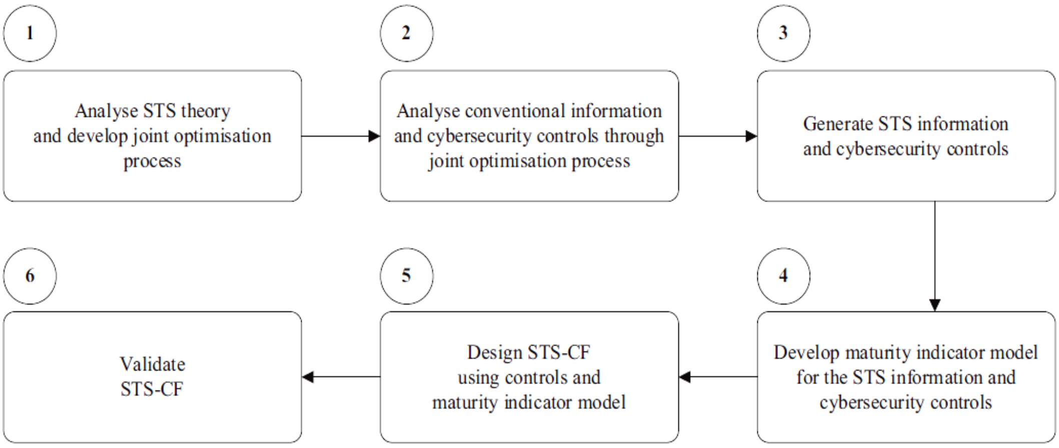

1
Analyse STS theory and develop joint optimisation process
2
Analyse conventional information and cybersecurity controls through joint optimisation process
3
Generate STS information and cybersecurity controls
4
Develop maturity indicator model for the STS information and cybersecurity controls
5
Design STS-CF using controls and maturity indicator model
6
Validate STS-CF

Figure 3: STS-CF (Socio-Technical systems – Cyber security Framework) (Malatji, Von Solms, & Marnewick, 2019)

Thus, the followed theories examined about how new methodologies protected the security systems and how it controls cyber threats and attacks in cyber security technology.

4 Implementation of Cyber Security in Various Organizations

The system should be secured and well maintained, cyber security had been a significant method for securing and sustaining the data and network area in organizations. Some of various organizations that implemented cyber security in firms and examined how it controlled organizations threats.

4.1 Cyber security in railway industry

The railways included a complex construction in transport industry and influenced importantly among public in society. Whereas railway had been pillar of society, the data driven techniques ensured the regular operation, planning, potential future investments and effective maintenance. The important objective of (Thaduri, Aljumaili, Kour, & Karim, 2019) this paper for risk management techniques for securing data in the infrastructure of railway E-maintenance. The followed threats that suppressed in this suggested paper are: snooping, scavenging, tapping, traffic analysis, DoS, procedure violation, eavesdropping, jamming telecom, programming errors, failure from omitting errors in data and maintaining data entry systems.

The ongoing cyber security systems in railways are CYRAIL43 project and a shift 2 rail project (Kour, Aljumaili, Karim, & Tretten, 2019). The researchers suggested a technique for extreme, high level security and risk assessment based on the IEC 62443 standard in railway domain. The internet based railway E-

Maintenance solutions are migrated along with cloud computing area and big data analytics used for analysing and visualizing the high quantity of data in cloud platform. Hence, cyber security hindered the enhancement of cloud platform on the basis of big data for maintaining purposes. Additionally, (Kour, Karim, & Thaduri, 2020) theory explained and developed a maturity model for railway organizations, C2M2 (cyber capability maturity model) had been picked up for accessing the cyber security capacity of railway industry. This method implemented by followed instruction, a fresh maturity level maturity indicator level (MIL4) had been suggested in C2M2 model. Then, C2M2 model supported by modern security analytics and created a threat intelligence for developing the R-C2M2 (railway cyber security capability maturity model).

4.2 Cyber security in marine organizations

The hackers are decently increases the awareness of cyber-attacks and vulnerabilities among the marine sector hence, the existed risk assessed system tools that may not sufficiently represented the special nature of marine cyber-attacks and threats. Therefore, (Tam & Jones, 2019) this paper introduced model-based framework for MaCRA (marine cyber risk Assessment) which considered a consolidation of marine and cyber factors with the challenges of configurations, ship functionalities range, environmental and user's factors. The current study aimed for presenting intensively marine cyber risks factors and informed to marine community while taking decision in cyber security systems. Thus it provided the necessity profiles for marine cyber risk factors and supported for increasing insurers, operators, mariners, regulators all over the world marine cyber security measures. For the further research MaCRA had been suited for practical application in real world usage and increased its usability on the basis of software tools. (Hopcraft & Martin, 2018) suggested international maritime organization, to create resilient and robust cyber security regulations. This study also created an advanced standardized cyber code for legal binding instrument. This instrument will face cyber threats in maritime networks. (Das & Morris, 2018) a midstream marine organization oil terminal tested five system models for strengthening cyber security in the maritime organization.

- Strong physical system
- Cyber-physical system link
- PLC (programmable logic controller)
- Cyber security network
- HMI (human machine interface)

To assess the challenges in maritime navigation (Androjna, Brcko, Pavic, & Greidanus, 2020) this study suggested to implement multiple PNT (positioning, navigation, timing) systems on maritime vessels for complementing navigation through GPS. In addition to, (Progoulakis, Rohmeyer, & Nikitakos, 2021) this study intended to use API STD 780 SRA (security risk assessment tool) and bow tie analysis for assisting maritime assets owners with cyber security measures.

4.3 Cyber security in health care system

In recent days cyber security had been violating in health care systems that stick patients into privacy risk and caused to lost faith in management of health organizations. Although these threats added extra danger to patients health safety and also financial safety to organizations of health system.

Therefore, (Bhuyan et al., 2020) explored the main type of cyber security in health organizations by selecting four players that contributed for cyber-attacks and security in this particular organizations for identifying the mistakes and eliminating threats in it.

1) Cyber attackers: These attackers constituted the major threat for cyber security.
2) Cyber defender: The cyber defender was a generic name that adopted for large array of separate one, which strongly worked for ensuring cyber security.
3) End users: End users played an important part for safe guarding cyber systems.
4) Developers: These developers are needed for assuring security and eliminating mistakes and problem that attacks cyber systems.

The following cyber threats that attacked health care systems in recent days are privilege escalation, MITM (man in the middle), cryptographic attack, structured query language injections exploit, Trojans, and worms. Hence this study explained about the pre cautionary measures that had been taken for cyber security systems and identifying attacker’s path and blocked it. (Askar, 2019) suggested STAMP (System-theoretic accident model and process) for finding hazards and system safety measurements, and analysing loss in physical system. (Jalali & Kaiser, 2018) encouraged to move health care system into cloud based hosted services. Using latest technology with strong cyber security measures for detecting unauthorized access on devices. Strong firewall network for staff, patients, medical devices. Strict policy for technology procurement.

5 Cyber Security Methods in India

In past decades the security in cyber systems had gained more importance in international agencies and governments. Cyber space had been an emerging technology in growing economic conditions as well as also to citizens in world wide.

5.1 Country level frame work in cyber security

For generating assurance, activities that had been taken by a country for encountering cyber threats that essential for maintaining perfect secured systems. Hence, (Bahuguna, Bisht, & Pande, 2020) this aimed for offering a fresh and new aspects that focused on country wide's cyber security bench marking and its assurance. The above presented an analysis technique for adopting countries cyber security assessment and generating a great assurance of cyber quality measures. The data gathered from 37 different countries including India and learned knowledge about worldwide scenario of security measures by adopting cyber security methods.

The experimental results differentiated by i) types of actions in cyber security pre-process of bench marking ii) special tools and techniques for implementing bench marking iii) bench marking's frequency actions iv) bench marking had been implemented by it type and name v) bench marking's output procedure. Finally, absence of over reacting frame work and assurance in cyber security at the competition of national level of bench marking on the basis of adhoc. Hence, the visibility absent in cyber system procedure of a country.

The cyber security practices are spread with wide range for improving posture in cyber security but metrics of bench marking performance was absent. According to this analysis looked forward for emerging cyber security assurance by developing frame work in India.

5.2 Cyber assessment in country level

Cyber security threats are overcome by secured implementation of ICT (information and communication technologies) and ICT related services. For protecting national level organization's information encountering cyber threats by implementing advanced cyber security measures.

Wherefore, all countries had been implementing various measures and spending important sources and improved cyber security facility in organizations and implementing difficult cyber security systems. (Bahuguna, Bisht, & Pande, 2019) the followed paper mainly focuses on cyber security that prompting on Indian organizations. On board two TTX (table top eXercises) and five workshops were executed for collecting data form entering entities in mediator based and self-assessed mode in cyber security by six dimensions.

a) Initial elements, priorities and challenges.

b) Technical and legal measurements.

c) Organizational measurements.

d) Sharing information and Co-operation.

e) Awareness augmentation and capacity building

Cyber security implemented in maturity assessment of organizations in India. The followed workshops and table top exercises are further used for highest security measures of cyber security organizations. The assessment validated security and blocked form unwanted threats and attacks. The data had been gathered and analysed the scenario of cyber security within Indian organizations. Future research for adopting the above measures in all organizations in India.

5.3 Cyber security in energy sector organizations of India

Cyber threat resulted high cost, downtime, efforts and affects psychological conditions of organization's environment that destroy the firm's performance and not only firm's economy and also national economy growth. (Venkatachary, Prasad, & Samikannu, 2018) aimed for highlighting the numerous security attacks and threats on the energy constructive structure and its effects. In this discussion emphasising world security in cyber system of organizations. The author gathered numerous observations in energy sectors had moved up from bottom to second highest. The energy sector had been vulnerable. The hackers and attackers focused on collecting information and details that also created financial loss, hence the energy firm's needed to be more aware of these risks for protecting its important and valuable information as well as ICS or SCDA networks of organizations. Cautious methods are needed for mitigating the effects of threats in the structure of cyber-attack and cyber terrorism. The past historical data and authenticates documents data had been implemented as measurements for analysing and providing constant answers. Creating powerful public and private partnership had been needed for documenting the problems where, authenticated documents implemented for discovering and learning future knowledge about cyber-attacks. An adjusted computer had been resource area for attackers for entering network security system and retrieving data. Thus, it had been a significant and crucial for securing the operating system of computer. Conducting awareness program that helped for identifying social engineering threats.

5.4 Cyber security in Rajasthan's E commerce sector

The cyber-crime problems and issues were creating critical challenges in all sectors, and organizations and it integrated in the fields of national security, financial transaction trust and safety, personal information privacy and web surfing so far. Wherefore, improving the range of awareness about cyber security and offering ideas for ensuring privacy and safety measures of gadgets and devices. (Adholiya & Adholiya, 2019) Here, investigating the knowledge of regular and public e-banking sectors with cyber security measures and ideas in Udaipur, Rajasthan by focusing on various security threats and attacks in online activities by non-financial or financial with gathered information via questionnaire. The latest banking services or electronic banking service users are the defendants and their responses and comments were assessed into statistical method as regression and F-test. Hence, it used for analysing for identifying the highest level of awareness about cyber threats and issues that impacted on banking and social economical services. The statistical testing method supported for interpreting the social economic constraints played an important part for increasing the customer's knowledge about cyber security attacks and threats and providing ideas and tricks for overcoming the cyber security issues. The banking customers of Udaipur district in Rajasthan, had learned perfect amount of awareness about security issues and privacy problems by improving cyber security measures to their electronic and banking devices.

Table 1: various cyber security attacks and prevention - globally especially in India

S.no	Author name	Region	Attacks	Potential Impacts
1	(He & Zhang, 2019)	USA	• Some organization's employees are lack in cyber security knowledge. • Hence, if threats occurred it may not cleared or solved immediately. • In between this cyber attacker theft all valuable information in systems.	• For improving the single employees' cyber security knowledge and behaviour the organizations should engage employees and training for developing cyber security awareness programs. • So it motivated the employees and staying alert and solving issues in minutes.
2	(Srinivas, Das, & Kumar , 2019)	India	• Viruses • Phishing • Trojan horses • Worms • DoS • Illegal access • Theft of valuable information.	• The CIMF (cyber security incident management framework) are implemented in this study. • The three objectives of this method are: • Security operations • Computer emergency response centre • Technology infra-structure.
3	(Kaba	South	• Minimal management	• Cyber security in

	nda, Tanner, & Kent, 2018)	Africa	support • Low budget priority • Size less vulnerable • Less technologically complex • Difficulty while using cyber tools • Priority in complaint policies and regulations.	SME (small and medium firms) are significant in developing countries. • Some factors needed to be concern are: • Internal factors • Handling institutional pressures. • Consumer and technological related concerns.
4	(Georgiadou et al., 2020) (Oyelami & Kassim, 2020)	Greece	• Threats in critical domains • Not enough high standard security in high tech domains	• Security culture frame work model • Continuity • trust and Access • assets • security governance • operations • defence • attitude • competency • behaviour • awareness
5	(Puthal, Mohanty, Nanda, & Choppali, 2017)	Australia	• DDoS • Vulnerabilities • Misconfigurations • Brute force • Phishing	• The study used SDP (software defined perimeter) replacing network centric solutions. • Brute force and phishing are eliminated by SDP and TLS combined to secure clients encryption key.
6	(Sahoo, Behera, & Mohan	Odisha and Bhubaneswar, India	• Lack of cyber security knowledge • Data theft Not aware of allocation given by government	• OSSC Odisha staff selection committee • Women and child development • Central poultry

	ty, 2018)		scholarships and funds to particular individuals.	BDA (Bhubaneswar development authority)
7	(Sun et al., 2018)	Australia	• Threats in Indian organizations data, network data, reports dataset, synthetic data, data from websites and data retrieved form unknown sources.	• There are some methods used: • Cyber security incident analysis • Security issues in modelling • Feature engineering • Data processing and collection • Model customization Evaluation.
8	(Sun et al., 2018)	Florida, US	• Intentions of attackers • Intrusion prediction • Attack projection and intention recognition	• Based on this attacks models are created some are: • Attack graphs • Markov models • Bayesian networks • Continuous models like: • Grey models
9	(Akalp & Torii, 2020)	Japan	• Malware types like: • Trojan.WinLNK.starter, • Hoax.MSIL.seguras.a, • Trojan.WinLNK.Runner.jo • Attacks in nuclear plants and banks.	• Using OSINT tools are analysed and used for cyber stacks in India. • Currently OSINT tools are used in japan.
10	(Padmavathy)	Assam, India	• Hacking • Email harassment • Identity theft • Spoofing • defamation	• This organized study collected the responsible activities of parents, policy makers and teachers. • They must look forward from being victim of cyber security threats and attacks.

6 Challenges of Cyber Security

The most common cyber security challenges are discussed below. Although these are regular attacks and threats but it not been full diminished but some of them are controlled by new software and methods. And also some of threats boomed itself to another level of theft and hacks. The followed issues created user/organizations by facing more challenges for maintaining cyber security systems.

6.1 Ransom ware with double theft

Ransom ware involved in hacking the user's data and prevented it from locating unless random amount had been paid by user. Ransom ware attacks are difficult for single user because they doesn't had enough knowledge about hackers. Moreover, hackers may not realised the user data even so they paid random amount to them. Random ware attackers used this hacking method as business for stealing amount from user(Almaiah, Al-Zahrani, Almomani, & Alhwaitat, 2021; Mylrea, 2019).

The double ransom theft are encrypted files and demands organizations for recovering process if organization doesn't pay or even they paid random amount the hackers leaked their confidential data in internet and it sold for heavy amount. Ransom ware had been more familiar in cyber security limitations in India. According to latest survey 82% of Indian organizations had been attacked by ransom ware (Rodgers, Attah-Boakye, & Adams, 2020).

6.2 Cloud adopted exceed the security

Adopting cloud had been raised in recent years. With a less man power organizations required accessing, scaling and flexible by cloud based resolutions. An average 75% of business enterprises securing data in cloud based structure had been most important concerns. Knowing about the knowledge of securing systems that initiated the joint servers in vendor's special surroundings for maintaining cyber security system with perfect cloud vendor environment.

Latest survey explained that some organizations are failed to achieve efficient cloud security system that showed 99% of attacks happened only by weak cloud storage and security system (Kafol & Bregar, 2017).

6.3 A new focus on Mobile malware

Mobile malware had been a developing malware in recent years because of digital world, the technology had been improved rapidly (Alshammari, Beach, & Rezgui, 2021). Everyone in the world had smart phones, even kids had been using mobile phones not only for education purpose but also for gaming. The initial reason for mobile malware the usage of non-secured URL or unknown WiFi source or other internet resources. The mobile security report, showed about basic and initial stages of malware and how it had been developed into the mobile devices

According to 2021 survey 97% of organizations faced mobile malware form various vendors while using their internet sources(Aldawood & Skinner, 2019). Vulnerable vendor's malware inherited Trojan, virus into server system of organizations. The application that are downloaded from malicious sources of internet and its related links had coated the mobile devices users with attacks and spam threats (Walker-Roberts, Hammoudeh, Aldabbas, Aydin, & Dehghantanha, 2020).

6.4 Still no control on phishing

Phishing had been a one of the social engineering attacks more over it used for stealing user's data and confidential information like credit card numbers and passwords, and login details. The hackers used information for theft the money and also for illegal money transferring and online shopping. Phishing attacks are popular within the hackers as they used data as their advantage unless users found theft (Geluvaraj, Satwik, & Kumar, 2019).

It had been a main threat in India according to latest report analysed 29,000 of practical security accidents among that 36% of data theft had been occurred by phishing that increased with 11% when compared to past year (Karjalainen & Kokkonen, 2020).

6.5 A growing IoT attacks

The practices of IoT (internet of things) devices had been a most popular in emerging technology because of it powerful and quick reaction timing with low cost. IoT devices are mechanical, computing and digital devices that transferred data independently through network. Some examples of IoT are laptops, desktops, smart security devices and mobile phones. Adopting IoT devices while it un-predictively increased the rate of cyber security issues (Kumar, Biswas, Bhatia, & Dora, 2020). Attacks in IoT devices must resulted for the compromising of sensitive data user. Therefore guarding IoT devices form cyber security had been a most challenging on in these days.

Table 2: Comparative analysis of cyber security methodologies and applications considered by traditional researchers.

S.no	Authors	Attack focused	Methodology	Applications	Future recommendations and suggestions
1.	(Khatoun & Zeadally, 2017)	• Malware infection • Unauthorized entry by users • System failure	• Two factor authentication system with one time passwords • Such as Imprivata	• Smart city or building sector	• Future recommendations of the study to ensure the smart cities privacy and

		• Controlling fire system • Damaging and controlling lifts • Modifying smat meters • Disabling electricity and water supplies • Stopping RES (renewablke energy system)	OneSign, STMicroelectronics, Comodo security and secure MCU. • IoT forensics such as DigiCert, IoT PKI solutions • Data backup solutions such as CommScope solutions, Socomec solutions.		control as illegal to government. • Motivates public to adopt smart cities as a secured system.
2.	(Varela-Vaca, Gasca, Ceballos, Gómez-López, & Torres, 2019)	• Compliance of cyber security polices in software organizations • New software installation without any notification • Installation of malwares while installing software in online.	• CyberSPL frame work for the configuration of software products, services and applications. • It automates cyber security management while installing software configuration.	• Software industry	• Future suggestions are automatic update of feature models with advanced technology • Diagnosis of cyber security threats before installations. Make proposed system as mandatory
3.	(Sohal, Sandhu, Sood, & Chang, 2018)	• Unauthorized device attacks in fog environment because of data fetching form online • Malicious edge devices in fog environment	• Cyber security framework utilized three technologies such as IDS (intrusion detection system), Markov model, VHD (virtual honeypot device).	• Fog environment in IT industry	• Future of this study, to integrate the proposed system with large scale of ethical hacking system and create robust and resilient technique to deal with hackers.
4.	(Matta & Cantelli-Forti, 2019)	• False alarm, less level of threat detection, high rate of false detection and alarm	• In this study, APSS (Airport physical-cyber security system) was proposed to enhance the cyber security system in airport.	• Airport industry	• The proposed system suggested this frame work in critical infrastructure with minimum of effort.

			- This methodology will reduced false rate of alarm and increases the confidence level of threat detection.		
5.	(Yousefi-Azar, Varadharajan, Hamey, & Tupakula, 2017)	- Intrusion in network and malware attacks	- This study suggested a feature learning technique named AE (auto encoder).	- Embedded security systems	- This study recommended to practically implement the proposed system in sensor network in Internet of things.
6.	(Baig et al., 2017)	- Malicious code - data threats - confidentiality and integrity compromise - Eves dropping - DoS (Denial of Service Attacks) - Malware injection - Data locations and Regulation of boundaries.	- This study suggested, Smart Grids, UAVs (Unmanned Aerial Vehicles), BAS (Building Automation Systems) and smart vehicles with cyber security sensors enabling with IoT	- Smart city infrastructure	- This study recommended to improve security in Smart city with ICT infrastructure.

A comparative analysis had been made for the various organizations. Smart city affected with various cyber security attacks, to rectify them UAVs, smart grid, BAS are utilized form over coming these attacks efficiently.

7 Conclusion

As well known that, Cyber security had been a state of performing for the protection and retrieving data from networks, computer systems and other electronic devices from any category of cyber-attacks. The study showed about the organizations cyber security methods in India and how to overcome. (Reghunadhan) The digitization of India by Indian government, an significant and special program for achieving digital communication over the country and transforming demographic, social and economic condition and political facets.

Although, government initiated for digitalization in India, the lot of public doesn’t had enough knowledge about digitalization and its threats. Some people may notice cyber threats and reported to government cyber security officers, but some people may not know about cyber threats and loss their money and property. In India recent ransom ware threats are gathering bank login credentials and passwords and stealing money in it. Not aware of this many people lost their money and attempted suicide or May loss of lives happened. Hence, cyber security programs should be conducted for eliminating this issues.

Cyber threats increased in small and large business organizations. Developing e commerce network security site with technological techniques and worked with reputing security vendor are basic choice for small and large business for successfully protecting data form cyber-attacks. Some of network security measures are suggested to consider are authentication, confidentiality, integrity, availability, non- repudiation. ***Some Applications of cyber security like*** DNS based content filtering, Privacy frame work, voting system security, Threat detecting and preventing and Privacy engineering were also discussed. Protecting organization from cyber-crimes, i) educating the employees or staff about cyber security measures and how to resolve the threats ii) guarding valuable and sensible data carefully with full of protection iii) installing antivirus software and update regularly iv) usage of strong passwords v) keeping operating system and software up to date version vi) avoid synchronizing e mails from unknown resources and accepting public WiFi.

In future works of cyber security systems with AI, server less and security app in mobile devices that provided the full protection for data which included organizations valuable data and personal information etc. furthermore, the global networks still finding for the solution for cyber threats because of hackers are advanced in their tactics so, security system had been cautiously updated as to reducing the threats.

References

[1] Adholiya, A., & Adholiya, S. (2019). A Study on Cyber Security Practices and Tips Awareness among E-Banking Services Users of Udaipur, Rajasthan. *Int. J. Sci. Res. in Multidisciplinary Studies Vol, 5*, 8.

[2] Adlakha, R., Sharma, S., Rawat, A., & Sharma, K. (2019). *Cyber Security Goal’s, Issue’s, Categorization & Data Breaches.* Paper presented at the 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon).

[3] Akalp, G. A., & Torii, N. (2020). Analysis of Cyber-Attack Trends in India Using OSINT. *情報処理学会第 82 回全国大会, 1*, 05.

[4] Alali, M., Almogren, A., Hassan, M. M., Rassan, I. A., & Bhuiyan, M. Z. A. (2018). Improving risk assessment model of cyber security using fuzzy logic inference system. *Computers & Security, 74*, 323-339.

[5] Aldawood, H., & Skinner, G. (2019). Contemporary Cyber Security Social Engineering Solutions, Measures, Policies, Tools and Applications: A Critical Appraisal. *International Journal of Security (IJS), 10*(1), 1.

[6] Almaiah, M. A., Al-Zahrani, A., Almomani, O., & Alhwaitat, A. K. (2021). Classification of cyber security threats on mobile devices and applications *Artificial Intelligence and Blockchain for Future Cybersecurity Applications* (pp. 107-123): Springer.

[7] Alshammari, K., Beach, T., & Rezgui, Y. (2021). Cybersecurity for digital twins in the built environment: current research and future directions. *Journal of Information Technology in Construction, 26*, 159-173.

[8] Androjna, A., Brcko, T., Pavic, I., & Greidanus, H. (2020). Assessing cyber challenges of maritime navigation. *Journal of Marine Science and Engineering, 8*(10), 776.

[9] Askar, A. J. (2019). Healthcare management system and cybersecurity. *International Journal of Recent Technology and Engineering*, 237-248.

[10] Bahuguna, A., Bisht, R. K., & Pande, J. (2019). Assessing cybersecurity maturity of organizations: An empirical investigation in the Indian context. Information Security Journal: A Global Perspective, 28(6), 164-177.

[11] Bahuguna, A., Bisht, R. K., & Pande, J. (2020). Country-level cybersecurity posture assessment: study and analysis of practices. *Information Security Journal: A Global Perspective, 29*(5), 250-266.

[12] Baig, Z. A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., et al. (2017). Future challenges for smart cities: Cyber-security and digital forensics. *Digital Investigation, 22*, 3-13.

[13] Bhuyan, S. S., Kabir, U. Y., Escareno, J. M., Ector, K., Palakodeti, S., Wyant, D., et al. (2020). Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations. *Journal of medical systems*, *44*(5), 1-9.

[14] Das, R., & Morris, T. (2018). *Modeling a midstream oil terminal for cyber security risk evaluation.* Paper presented at the International Conference on Critical Infrastructure Protection.

[15] Dixit, P., & Silakari, S. (2021). Deep learning algorithms for cybersecurity applications: A technological and status review. *Computer Science Review, 39*, 100317.

[16] Geluvaraj, B., Satwik, P., & Kumar, T. A. (2019). *The future of cybersecurity: Major role of artificial intelligence, machine learning, and deep learning in cyberspace.* Paper presented at the International Conference on Computer Networks and Communication Technologies.

[17] Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2020). A cyber-security culture framework for assessing organization readiness. *Journal of Computer Information Systems*, 1-11.

[18] He, W., & Zhang, Z. (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of Organizational Computing and Electronic Commerce, 29*(4), 249-257.

[19] Hopcraft, R., & Martin, K. M. (2018). Effective maritime cybersecurity regulation–the case for a cyber code. *Journal of the Indian Ocean Region, 14*(3), 354-366.

[20] Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: a systematic mapping study. *Arabian Journal for Science and Engineering, 45*(4), 3171-3189.

[21] Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in hospitals: a systematic, organizational perspective. *Journal of medical Internet research, 20*(5), e10059.

[22] Jeyaraj, A., & Zadeh, A. (2020). Institutional isomorphism in organizational cybersecurity: A text analytics approach. *Journal of Organizational Computing and Electronic Commerce, 30*(4), 361-380.

[23] Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce, 28*(3), 269-282.

[24] Kafol, C., & Bregar, A. (2017). Cyber Security—Building a Sustainable Protection. *DAAAM International Scientific Book,* 81-90.

[25] Karjalainen, M., & Kokkonen, T. (2020). *Comprehensive Cyber Arena; The Next Generation Cyber Range.* Paper presented at the 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW).

[26] Khatoun, R., & Zeadally, S. (2017). Cybersecurity and privacy solutions in smart cities. *IEEE Communications Magazine, 55*(3), 51-59.

[27] Kour, R., Aljumaili, M., Karim, R., & Tretten, P. (2019). eMaintenance in railways: Issues and challenges in cybersecurity. *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit, 233*(10), 1012-1022.

[28] Kour, R., Karim, R., & Thaduri, A. (2020). Cybersecurity for railways–A maturity model. *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit, 234*(10), 1129-1148.

[29] Kumar, S., Biswas, B., Bhatia, M. S., & Dora, M. (2020). Antecedents for enhanced level of cyber-security in organisations. *Journal of Enterprise Information Management*.

[30] Lezzi, M., Lazoi, M., & Corallo, A. (2018). Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Computers in Industry, 103*, 97-110.

[31] Malatji, M., Von Solms, S., & Marnewick, A. (2019). Socio-technical systems cybersecurity framework. *Information & Computer Security*.

[32] Matta, W., & Cantelli-Forti, A. (2019). An Innovative Airport Physical-cyber Security System (APSS). *Information & Security, 43*(3), 285-293.

[33] Mylrea, M. (2019). Distributed autonomous energy organizations: Next-generation blockchain applications for energy infrastructure *Artificial intelligence for the Internet of everything* (pp. 217-239): Elsevier.

[34] Oyelami, J. O., & Kassim, A. M. (2020). Cyber security defence policies: A proposed guidelines for organisations cyber security practices. *International Journal of Advanced Computer Science and Applications, 11*(8).

[35] Padmavathy, R. Cybercrime in India: A Trend Analysis Specific to North East.

[36] Paraskevas, A. (2020). Cybersecurity in travel and tourism: a risk-based approach. *Handbook of e-Tourism*, 1-24.

[37] Progoulakis, I., Rohmeyer, P., & Nikitakos, N. (2021). Cyber Physical Systems Security for Maritime Assets. *Journal of Marine Science and Engineering, 9*(12), 1384.

[38] Puthal, D., Mohanty, S. P., Nanda, P., & Choppali, U. (2017). Building security perimeters to protect network systems against cyber threats [future directions]. *IEEE Consumer Electronics Magazine, 6*(4), 24-27.

[39] Raghavan, K., Desai, M. S., & Rajkumar, P. (2017). Managing cybersecurity and ecommerce risks in small businesses. *Journal of management science and business intelligence, 2*(1), 9-15.

[40] Reghunadhan, R. Cyber Threat Landscape of Digital India: A Critical Perspective. *urnal of o*, 37.

[41] Rodgers, W., Attah-Boakye, R., & Adams, K. (2020). Application of Algorithmic Cognitive Decision Trust Modeling for Cyber Security Within Organisations. *IEEE Transactions on Engineering Management*.

[42] Sahoo, B., Behera, R. N., & Mohanty, S. (2018). *International Cyber Attackers Eyeing Eastern India: Odisha-A Case Study*. Paper presented at the Science and Information Conference.

[43] Sohal, A. S., Sandhu, R., Sood, S. K., & Chang, V. (2018). A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. *Computers & Security, 74*, 340-354.

[44] Son, J., Choi, J., & Yoon, H. (2019). New complementary points of cyber security schemes for critical digital assets at nuclear power plants. *IEEE Access, 7*, 78379-78390.

[45] Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems, 92*, 178-188.

[46] Sun, N., Zhang, J., Rimba, P., Gao, S., Zhang, L. Y., & Xiang, Y. (2018). Data-driven cybersecurity incident prediction: A survey. *IEEE communications surveys & tutorials, 21*(2), 1744-1772.

[47] Tam, K., & Jones, K. (2019). MaCRA: a model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs, 18*(1), 129-163.

[48] Thaduri, A., Aljumaili, M., Kour, R., & Karim, R. (2019). Cybersecurity for eMaintenance in railway infrastructure: risks and consequences. *International Journal of System Assurance Engineering and Management, 10*(2), 149-159.

[49] Toth, P. (2019). cyber security risk assessment tool *https://www.nist.gov/blogs/manufacturing-innovation-blog/how-vulnerable-are-you-cyber-attack-self-assessment-tool*

[50] Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security, 109*, 102387.

[51] Varela-Vaca, Á. J., Gasca, R. M., Ceballos, R., Gómez-López, M. T., & Torres, P. B. (2019). CyberSPL: a framework for the verification of cybersecurity policy compliance of system configurations using software product lines. *Applied Sciences, 9*(24), 5364.

[52] Venkatachary, S. K., Prasad, J., & Samikannu, R. (2018). Cybersecurity and cyber terrorism-in energy sector–a review. *Journal of Cyber Security Technology, 2*(3-4), 111-130.

[53] Walker-Roberts, S., Hammoudeh, M., Aldabbas, O., Aydin, M., & Dehghantanha, A. (2020). Threats on the horizon: Understanding security threats in the era of cyber-physical systems. *The Journal of Supercomputing, 76*(4), 2643-2664.

[54] Wang, S., & Wang, H. (2019). Knowledge management for cybersecurity in business organizations: a case study. *Journal of Computer Information Systems*.

[55] Yousefi-Azar, M., Varadharajan, V., Hamey, L., & Tupakula, U. (2017). *Autoencoder-based feature learning for cyber security applications*. Paper presented at the 2017 International joint conference on neural networks (IJCNN).

Notes on contributors

Dr. Deepshikha Bhatia is a Sr. Assistant professor from the Department of Computer science and IT working in IIS (Deemed to be University), Jaipur (Rajasthan), India. She has 14 years of teaching experience. Her major areas of research include Mobile Ad Hoc Networking, Sentiment Analysis and Cybersecurity. She has 7 publications in refereed journals. She is the reviewer of many refereed journals and member for various conferences.