INTERNATIONAL JOURNAL FOR INNOVATIVE RESEARCH IN MULTIDISCIPLINARY FIELD
ISSN(O): 2455-0620 [Impact Factor: 7.581]
Monthly, Peer-Reviewed, Refereed, Indexed Journal with IC Value : 86.87
Volume - 9, Issue - 5, May - 2023 Publication Date: 31/05/2023

DOIs:10.2015/IJIRMF/202305025 --:-- Research Paper / Article / Review

Cyber Security and its cognitive ramifications on E-Governance

Kritika
Government of India, Delhi, India
Email – kritikaa2297@yahoo.com

Abstract: *With the advent of 6G technologies and augmentation of cyber crimes around the world, there persists an obligation for the uncompromising cyber security and laws to safeguard the confidential information from the mischiefs who threaten to knock down the nations with their alarming acts. E-governance is one such area which needs the utmost surveillance. The rate of augmentation of crimes has increased manifolds and the persistence of adept personnel to safeguard the organization is the need of the hour as e-governance is the protuberance of the endeavour of the governments to bind themselves together with their citizens and strengthen their bonds. Security compliances, policies, regulatory frameworks, laws must well be in place for the effective implementation and working of the government machinery to match up with the technological advancement. The conceptualization of the psychology behind such attacks needs to be understood very well. The paper focuses on the e-governance and the psychology of the cyber criminals to enact such acts of violence.*

Keywords: *E-Governance, Security Policies, Crimes, Psychology, Cyber Criminals, Ransom*

1. INTRODUCTION :

Cyber security is a resolve of mechanization and subpoena of delineated to safeguard the systems, web work, programs and informational on personal, confidential or public basis from theft, vandalize and unwarranted grant[1]. The basic fundamentalism of the resolve is to protect the CIA triad i.e. Confidentiality, Integrity and Availability of the data[2].

Confidentiality refers to legit personnel being permitted to outpour and reform information. Confidentiality can be breached either directly or unintentionally. The direct dereliction can be in the form of clinching barred ingression to software systems, prosecution and sensitive credentials of organization’s assets with the intent of misappropriating or dabbling the information. The unintentional intent curates, fault on the part of beings, negligence or improper protective resources.

Integrity often resembles to the information or data is not dabbled and is native in form and therefore, calls for its trustworthiness. It can come to terms via attacking directly using various threat trajectory or neglect or paltry security practices.

Availability of the information often tends to in hand accessibility of the information on demand of authorized personnel which can often get obstructed by denial of service attack, power failure, uncalled for calamities, or malign web application breaching.

E-governance is the protuberance of the endeavor of the governments and varied organizations linked with the government to ameliorate their alliance with the inhabitant through translucency and candor to ensure wider democratic norms.

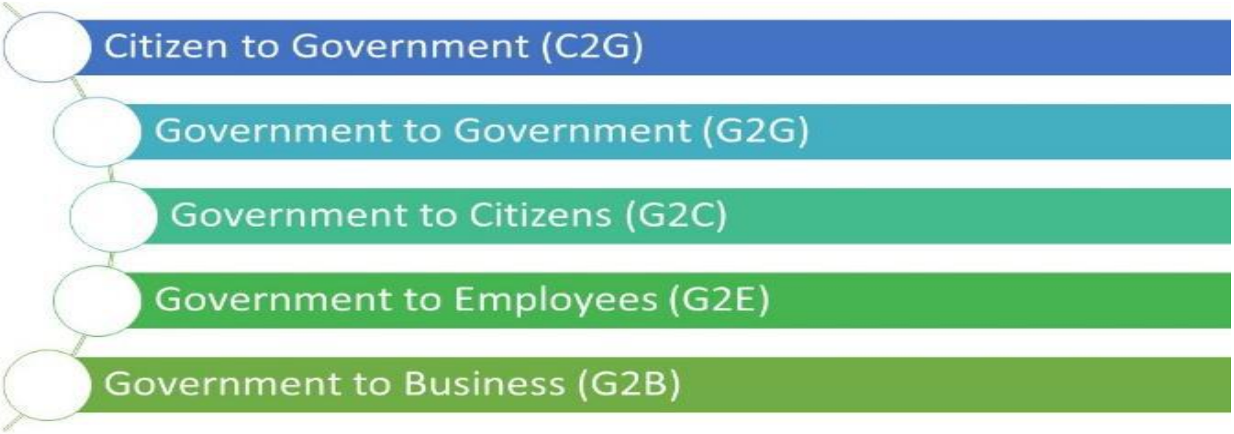
Citizen to Government (C2G)
Government to Government (G2G)
Government to Citizens (G2C)
Government to Employees (G2E)
Government to Business (G2B)

Figure 1: Components of E-Governance

There are various components accompanying e-governance as forecasted in figure 1 which is nothing but an automated interconnection between the entities.

Citizen to Government (C2G) is the multifaceted solutions provided by the government to its citizens about the particulars and amenities provided by it like filing of tax, forms, particulars related to various policies of the machinery among others.

Government to Government (G2G) is the transferal of the e-data or information in its electronic format between varied departments or instruments of the government with the predominant focus on the how the data is ingressed and reciprocated. It allows for an efficient implementation of various policies and acts at federal levels in a democratic setup.

Government to Citizens (G2C) is alike to C2G which is essential component in order to maintain translucency and ensure corruption free nation with increased accountability and responsibility of the government towards its natives.

Government to Employees (G2E) has the objective of limiting the pigeonhole in the functioning and decision making in the procedure carried out by the various instruments of government with augmented coherence, potency and contentment.

Government to Business (G2B) prime functionality is to minimize the hardship of the business entities with the inception of ease of doing business with national as well as international agencies while reducing the steps of approval and providing a multifaceted platform for the same. It indulges both profit and non-profit companies.

E-Governance accumulates for variety of ascendency such as undecorated testimonial like records for land and illegalization of benami assets, application like grievance redressal gets fastened, unostentatious accession of various goods and services at a reasonable rate, colossal accumulation of restricted resources to a large population, bilateral participation of citizens in the policies of the government and simplification of transactions with faster rate of recruitment process.

There are many provocations to the applicability of e-governance in various domains as mentioned. Inadequate and inefficient *infrastructure* to run trials and safeguard the data with strict security is a problem still persistent in many of the developing countries.

A requirement of humungous *fiscal capital and human capital* has masticated the resources of the nation.

Lack of accessibility to the data still persistent especially in remote areas of the country and latency problem in urban sectors due to huge demand and least supply of the required resource.

There persists a *paucity of skilled manpower* despite the augmenting rate of growth, development and employability and the paucity is grow on increasing if the skill development gets neglected at the current rate.

In a democratic institution, there will always be a possibility of a *new political party* coming into force which will alter and dampen the existing protocols leading to weakening of the procedures and security measures taken with and a persistent high gap continues to exist in the trained and training skillset.

The challenges can be overcome by laying down a stringent rules and procedures to be followed by every single ministry, department and private organisations. Though, there exists the prevalence of IT Act 2000, an amendment to the decade old act is the need of the hour with the PPP modelling to be adopted.

With timely training of personnel from lower to officer level and proper maintenance of records with multifaceted security entrance. This will also ensure that higher level officers spread awareness among peers and organize workshops at district levels for public awareness so that they can protected against ransom frauds.

2. LITERATURE REVIEW :

Zhao et al. in his research administered an investigation on e-government systems in United States and found that more than 90% of the websites use SSL encoding for safeguarding the confidentiality of its users which lacked potential mechanisms to prevent futuristic cyber threats or attacks[3].

Drew S. et al. critically examined the shortfalls and obstructions in the implementation of transactions made by the natives of the Saudi to e-government machinery[4].

Haran et al. examined the internal IT industry players that are inculpated in the e-governance domain and an itinerary of the potential threats that may happen to be launched by them. Prompt requirement of the actions to deal with the hazards in a coherent manner[5] were taken to task by internal stakeholders. The shortcomings of the Murugan et al. were highlighted and critically scrutinized[6].

Rajendra et al. investigated the cause and minimal partaking of the natives of the Kerala, state in India in e-governance applicability and came to the conclusion that rationality behind the minimal partaking[7] is security lapses in e-governance, behaviour towards development in terms of sustainability, embracing and level of perception regarding new intakes into their lives.

The tools and methodology ascertained for the examination of the rationality is based on the small set of data curated by Manoj et al[8]. The shortcomings of which is mentioned in above reference.

Gabriel et al. examined the credence and level of trustworthiness of the natives in the systems and information of Government of Ghana and came to the conclusion that there are few fundamental elements to which no proper solution[9] has been sorted i.e. bad network facilities, several services are excluded, no proper corroboration of confidential information from national database among others.

Beaman et al. through their work portrayed the contemporary developments in the ransomware attacks via investigation, recognition and preclusion[12]. They found out that most of the tools in the contemporary era used for an attack of ransomware incorporates the use of honeypots, analysis of network traffic, and machine learning techniques.
Alkhalil et al. in his depicted the major threats to an individual via phishing attack which is more prevalent in the contemporary era due to advance tools and technologies available for creating and getting the victims' personal details for sending[13]. The biggest cause of these attacks is the use of social media, befriending strangers, sharing of confidential files via emails without any security measures among others.

Rafael Wittek through his article proposed the theory of rationale choice making with broadly classifying into three dimensionality, viz, rationality, preference and individuality[15].

Kapil et al. highlighted the issue and provocation of privacy threat in India that often gets compromised with colossal workload and often opening doors to the attackers[22].

Sahu in her work forecasts the provocations in the "Digital India Mission" by highlighting various agencies operational for security purposes, their limitations and need for proactive force[10].

Panneerselvam in his work present the inquisitive examination of the cyber security framework and provocation in India and focused on educating the citizens of the country and avoid victimization in the hands of nefarious people[20].
Patel et al in their work has posed the factors influencing the victimization of people through social influence while highlighting the need to have more stringent tools and methodologies for upgradation and safeguarding of securities[21].

3. STAGES OF E-GOVERNANCE :

There are four general stages which needs to be accumulated by any governmental institution while dealing with the applicability of the e-governance in their natives.

Stage I: Framework of Information Technology

Positioning of fundamental framework relevant to the Information Technology is an imperative step towards achieving bigger goals which encompasses requirement of computer systems with potentialities, coordinated networking among them, provision of bandwidth by prioritizing the institutional setup and a platform to communicate such as intramural network.

The consolidated entrance to synergetic labour gizmos and information will augment the productivity by shared skill base.

Stage II: Digitalization

Computerization of all the particulars and proceedings of directorate and manoeuvre of e-office to maintain lucidity among various organs of the institution.

Stage III: Citizen centric readiness

Availability of particulars through delineation of a portal or platform which is easily accessible to all natives and non-natives of a nation which lucid information and making it bilateral, charismatic and uncomplicated.

Stage IV: Knowledge Base

Accessibility of the content generated by various government institutions and agencies is the bonanza for its natives which determines the triumph or collapse of the machinery of these government instruments flowing through a dedicated link of network service providers.

Thus, all the stages of the formation of e-governance needs to the tackled with utmost care and vigilance, as neglect on any single part of it can lead to damaging consequences.

4. TAXONOMY OF CYBER CRIMINOLOGY :

The cyber crimes most ubiquitous in the backdrop of e-governance are as listed.

Hacking is associated with gaining entrance to the computer systems and networking with mal-intention via unaccredited ingress of an organization or an institution[10]. The modern day hackers are more intellect in computer programming, networking and hardware detailing. The rationale has modified from an incentive relevant to ideology to monetary incentive and now to societal incentive[11].
The categorization of hackers involved in unethical hacking are usually the black hat hackers who exploit various vulnerabilities present inside the security framework of an institution to wreak havoc.

Ransomware is a sub category of cyber attacks with an objective to fend off pursuit assigned to an oganisation[12] for its daily routine work in exchange of hefty monetary benefits and prohibiting the ingress of system until the ransom is paid.

With the advent of cryptocurrencies and bitcoin newfangled technologies, are the new methodology of procuring ransom from individuals or organisations with the advantage of masking the real identity and networking details by manoeuvring VPN.

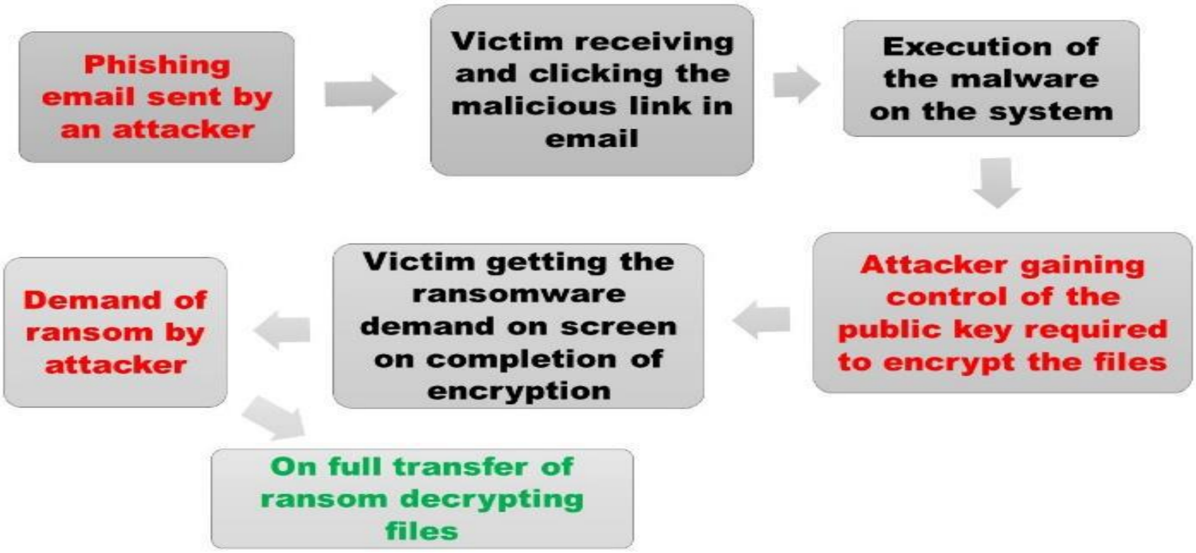
Phishing email sent by an attacker
Victim receiving and clicking the malicious link in email
Execution of the malware on the system
Attacker gaining control of the public key required to encrypt the files
Victim getting the ransomware demand on screen on completion of encryption
Demand of ransom by attacker
On full transfer of ransom decrypting files

Figure 2: Steps of ransomware attack

Phishing is defined as a deceitful venture of delineating a fake website, a facsimile of the native website into tricking personnel of disclosing their confidential, monetary and watchword details[13].
The various techniques used for phishing indulges with deceitful content sending via emails, messages or attachment of malicious links within an advertisement.

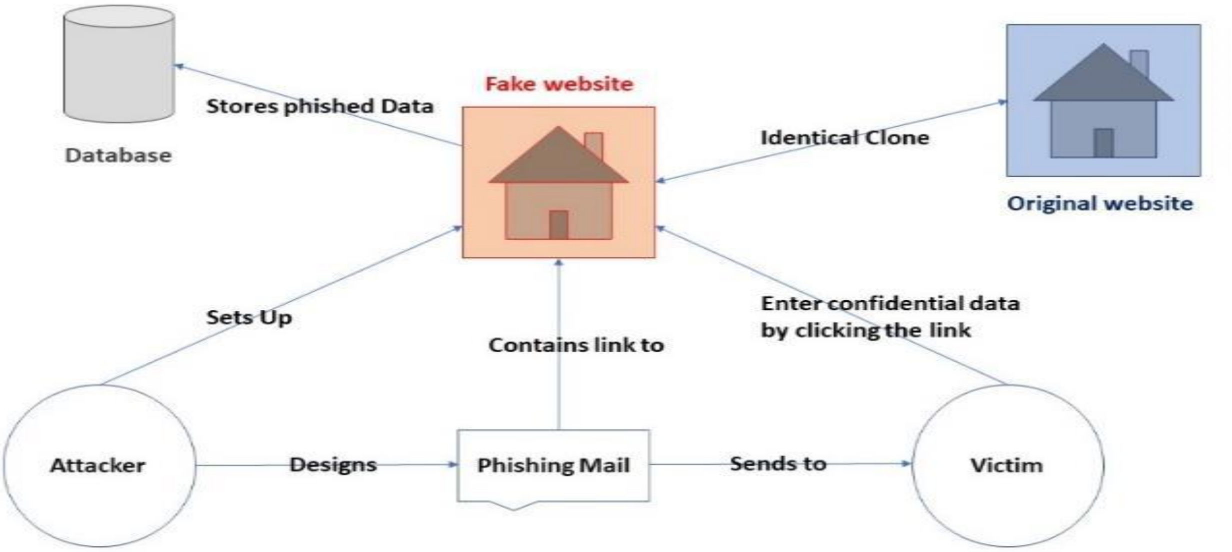

Figure 3: Steps taken for phishing attack

Data Diddling, a category of cyber attack related to the treachery of data by mutating the facts and figures of an organization or an institution in terms of fiscal expanse.
The central intention is to publish fake bills, evasion of tax, or portrayal of wrong turn over of an organization in order to attract external investors into funding more for the organization and masking the shortfalls of the institution.
It is often correlated with data breaching or data leaking of sensitive, confidential or restricted information ingress of an institute.

The way to avoid or secure the data from data diddling incorporates identifying critical information and delineating roles and responsibilities of who to access what kind of data.

Identity Theft is defined as the manoeuvring of an individual's intimate particulars for activities prevalent to criminology without the consent[14].
The worst case scenario in the world of e-governance indulging identity theft can cause a colossal damage to the security infrastructure of the organization leading to the breaching of the vitalities of the breaching of the citizens, and bolstering the fear of victimization by the criminals with the intent of revenge or political defamation or fiscal modification.

DDOS or Distributed Denial of Service Attack is an attack on the organisation's network to disrupt online operations by a malicious vector

The above highlighted criminal taxonomy are the most prevalent in the case of e-governance which ransomware gaining the highest percentage of attacks on government websites.

Thus, a need to strengthen the security infrastructure is the need of the hour along with the skilled manpower and timely training of personnel on every level from lower to officer level and spread awareness among people especially in the rural and remote areas where the spread of knowledge is still impacted by the limited availability of network infrastructure.

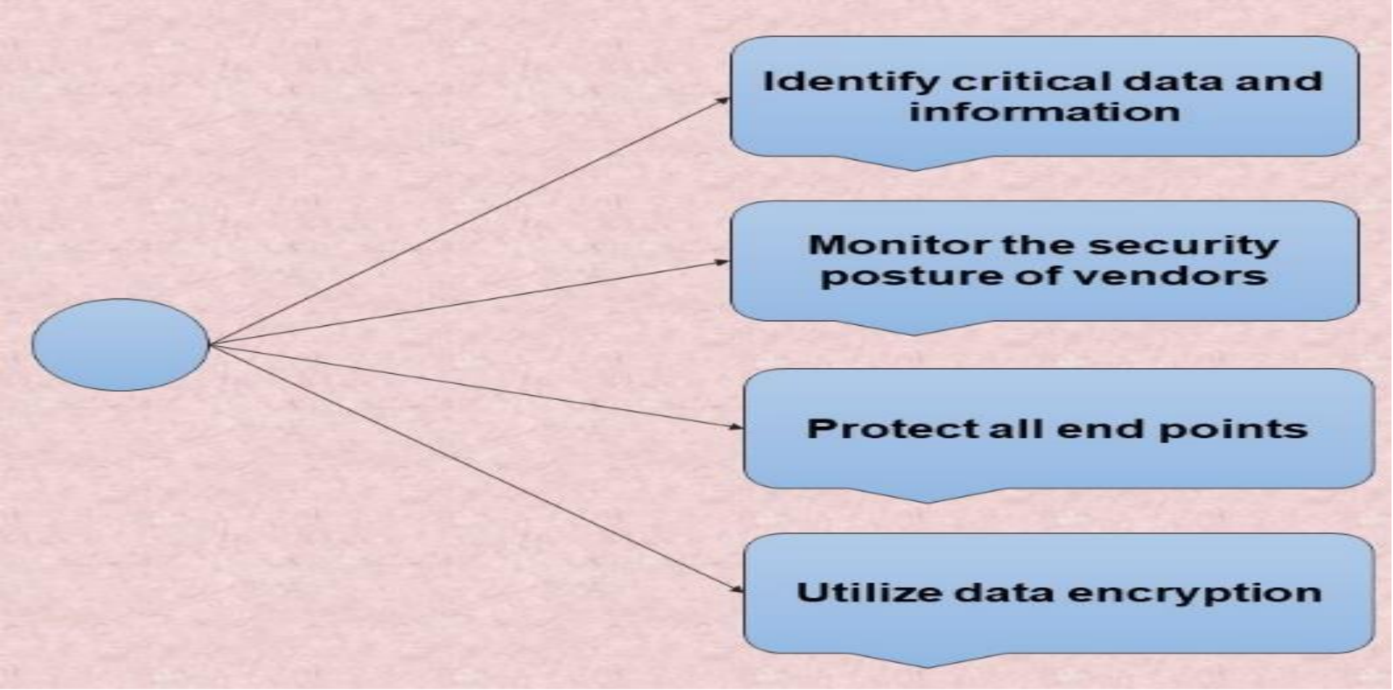
Identify critical data and information
Monitor the security posture of vendors
Protect all end points
Utilize data encryption

Figure 4: Ways to protect from data diddling

5. MENACES TO E-GOVERNANCE :

Cyber terrorism refers to admonition that is often prepense and zealous by political motifs in opposition to particulars, varied programmes and systems relevant to digitalization and data stored within such devices[20]. It is often carried on by one nation on other with the intent of spreading consternation, vandalization of global image of a nation or act an ransomware by exposing the vulnerabilities within the framework.

Dearth of expert and trained personnel is another critical stakeholder in the menace to e-governance where the machinery of various government institutions are managed by a single department or organization which overburdens an individual and there is lack of coordination among various security agencies, its functionalities and responsibilities towards the machinery. There is at present a need of 3.4 million cyber security professionals all over the world and in developing countries like India, the need accounts for more stringent numbers.

Humongous user base which is often augmenting on daily basis with increase in number of internetworking facility users showcases a task on security personnel often addendum their work[21].

Dearth of awareness among natives poses a greater risk and more prone to cyber victimization despite the holding various campaigns and drives. People are often lured by the ponzi schemes offered by the criminals often augmenting the task of incidence response teams and forensic departments.

Incompetent technical handling is the term dealing with the unskilled staff especially in the government departments who are more attracted towards dealing with things on paper and pen rather than electronic devices which often opens the door for various external as well as insider or internal threat actors such as misappropriation while handling e-office.

Technological barriers, though we are enroute advent and manoeuvre of 6G technologies, still a lot of individuals specially the ones living in remote areas or old generation people who are not well verse with the latest technological trends often becomes victims of the menace. Lack of upgradation of skill with time often poses a challenge for people to cope with advances of people like use of computer, network connectivity, sharing of files, handling of e-office, VPN knowledge base among others.

Sequestration often deals with the privacy and security issues faced by multiple organisations with unauthorized entrance gain[22] to posing as an imposter, breach of laws all poses a critical threat to the infrastructure of privacy to e-governance.

Thus, the menaces of the e-governance poses various imperils on the monitoring and functioning of the machinery and execution of e-governance instruments towards its natives on routine basis.

Few of the imperils highlighted are[23]:

Spoofing that is the act of being an imposter and breaching the security laws of the organization.

Repudiation, the act of knock backing intent of entrance into the e-governance systems on later stages after being caught in misappropriation of data.

Compromised information deals with bargaining of the confidential or sensitive information of the government machinery for want of monetary gains or political retaliation.

Denial of Service, a common predicament of lashing down the internetworking services of a particular organization by sending colossal data packets at the same time to enthrall all the resources and restrict the access.

6. PSYCHOLOGY OF CYBER CRIMINALS :

The intricacies of the brain mechanization and the quagmire of the societal norms build the behavioral aspect of the human beings, a way of interpretation of things is shaped. Criminal activities are the dysfunctional behavioural norms of a human mindset shaped by the locale in their lives. The civility bomber is the delinquent in the cyber space. One such domain of examining the relevance of the criminology of the cyber criminals is the forensic psychology, a requisition of meticulous knowledge to retort licit interrogation making an appearance in criminology, civility or other legitimate cases.

There are three studies relevant to the examination of the psychological behavior, namely, Routine activity theory, rational choice theory, and social learning theory.

Routine activity theory is an addendum to way of living theory which makes some people more prone than other to crimes. The activities are intertwined with two categorization, namely, actuating offenders and proficient guardianship. Customary it was relevant to burglary, vandalization and assault but with the advent of newer forms of technology, it is more related to cyber space leading to identity theft, ransomware, phishing among others.
The potentiality of the offenders in the contemporary era is more prone due to social media connectivity where a lot of strangers gets added to the list whose true intentions are not known leading to the misappropriation of confidential facts and fiscal deceit.

The dimension of guardianship can be elaborated in terms of social, technical, behavioural or personal. The technical guardianship refers to the act of restricting the information available and preventing attacks such as phishing and blocking with use of anti-virus facilities.

Social guardianship refers to the alliances we are associated with, the neighbouring surroundings as well as peers we engaged with on day to day basis.

Behavioural guardianship refers to the act of creating or modifying the passwords. To remember it with ease, people tend to chose passwords which are more prone to the cracked with the help of brute force attack or session hijacking like 123456.

Personal guardianship is the act of protection oneself from being the victim in the hands of notorious people who often lures people by ponzy schemes.

Social learning theory is defined as the swot analysis of a personnel at a high level making the individual reveal information about self which may be intuitive through interactivity, social get together or similar situations.
The state of affairs that lead to crime by an individual giving oneself up into is dissension in the relativity of two individuals who template or obligate the legitimacy of the societal norms. The other factor leading to is proneness of an individual to digressing model than acknowledging model and lastly paradoxical behaviour of an individual to existing norms.

Rational choice theory correlates to the behaviour that is apt for cognizance of the parameters for goals relating to proviso within the boundary restricted[15].

There are three different dimensionality of the theory i.e. rationality, preferences and individualism. Rationality deals with full awareness of an individual towards its decision making and the possible after effect likelihood. Preferences are more driven by psyche benefits rather than personal or monetary benefits with the choice of behaviour one makes and last but not the least, individualism deal with thin version of psyche i.e. methodological individualism or thick version of psyche i.e. structural individualism.

The tools for identifying the mindset behind committing crimes can be identified by using criminal profiling and geographical profiling[16-19].

The cognitive rationale categorized by three different theories viz. routine activity theory, social learning theory and rational choice theory highlights the factors or characteristics which often tends to the people falling victim to the hands of nefarious cyber criminals.

The acts like phishing, identity theft, vishing, data diddling are more prone to occur because of such mindset of the personnel as they often get swayed by the various schemes and emotional behaviours of these threat vectors.

In order to avoid being the victim in the hands of these nefarious criminals, a need to be aware of our surroundings is required at all levels be it at personal or professional levels.

7. PREPAREDNESS IN PROTECTING CRITICAL INFRASTRUCTURE

Inventory assessment

Auditing of the inventory where crucial assets are maintained is the first step in the assessment of risks. It is one of the vital steps in safeguarding the infrastructure as each and every electronic device that is astray leads to the establishment of vulnerable point in the network opening the door to the attacks. Manoeuvre of automated tools and services can outsize the impact while delivering transparent visibility into the networks.

Fortifying and executing safeguards

A trustworthy identification and management of accesses programme is essential to a zero trust strategy as it yields the requesting identity of the accessor to whichever data and application services along with the detailing of devices used for the same and manoeuvres multi factor authentication which reduces the threat of protected passwords compromise.

Descrying and recognizing threats

A reliable SOC analyst with the ground level expertise is essential to maintain critical portions of the IT infrastructure while handling and looking for the possible threat vectors while monitoring the actions of internal as well as external agents that can lead to threats. It is also important to secure end points in the network system while formulating a plan, identifying critical systems and prioritizing security with the use of tools and routine upgradation of skills of hired agents.

Recovering from threat

Restoring and recovering of data is instrumental when an attack on the critical infrastructure happens while preventing the loss of data and safeguarding the organization from financial downtime as well. Induction of automated tools and services like Rockwell Automation will increasingly help in reducing the threat to the endangered organisations.

8. CONCLUSION :

Since the inception of internet technologies and the advancement of its usage from generations, it has posed a great risk on the security operations of the nation from protecting the data to trade and commerce. The cyber security plays a crucial role in safeguarding the assets of e-governance and eliminating the trust deficit between the citizens and its governmental machinery at various federal levels.

The shortfalls of the security agencies can be overcome by building more stringent laws and formulating policies at global level and upskilling of personnel with the requirement and advancement of technologies on routine basis.

9. FUTURE SCOPE :

A need for a global security framework accepted and implemented by all nations around the world with development of new skillset and tools for detecting the threats on early basis and holding of more awareness campaigns.

REFERENCES :

1. Sarker, I.H., Kayes, A.S.M., Badsha, S., Alqahtani, H., Watters, P. And Ng, A., 2020. Cybersecurity data science: an overview
2. Lodh, A. A., & Dalave, C. V. A Study on Types of Cyber Crimes and Cyber Attacks Today.
3. Zhao, J. J., & Zhao, S. Y. (2010). Opportunities and threats: A security assessment of state e-government websites. *Government Information Quarterly*, *27*(1), 49-56.
4. Alshehri, M., & Drew, S. (2010). Challenges of e-government services adoption in Saudi Arabia from an e-ready citizen perspective. *World Academy of Science, Engineering and Technology*, *66*, 1053-1059.
5. Alshehri, M., & Drew, S. (2010). Implementation of e-government: advantages and challenges. In *International Association for Scientific Knowledge (IASK)*.
6. Nagaraju, R., Shanmugam, S. K., Rajeyyagari, S., Pentang, J. T., Bala, B. K., Subburaj, A., & Nomani, M. Z. M. (2021). Analysis of Cyber Security In E-Governance Utilizing Blockchain Performance.
7. Riswan, M. M., & Rajandran, K. V. R. A STUDY ON CYBER SECURITY IN E-GOVERNANCE WITH REFERENCE TO AREAS OF THANJAVUR DISTRICT-TAMIL NADU.
8. Manoj R, Dr. Senthil Kumar T, Maruthi M, Vivek G, “A Survey: Artificial Neural Networks in Surveillance System”, International Journal of Computer Applications,VOL.1,PP.19–22,2013
9. Botchwey, G. (2018). E-governance and cybersecurity: User perceptions of data integrity and protection in Ghana. In *5th Biennial Social Science Conference of the University of Education, Winneba, Ghana*.
10. Sahu, P. (2022). Digital India Mission: The Cyber Security Challenges. *RESEARCH HUB International Multidisciplinary Research Journal*, *9*(8), 01-10.

11. Gandhi, V. K., & Thanjavur, T. N. S. I. (2012). An overview study on cyber crimes in internet. *Journal of Information Engineering and Applications*, *2*(1), 1-5.
12. Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & security*, *111*, 102490.
13. Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, *3*, 563060.
14. Guedes, I., Martins, M., & Cardoso, C. S. (2022). Exploring the determinants of victimization and fear of online identity theft: An empirical study. *Security Journal*, 1-26.
15. Wittek, Rafael. (2013). Rational Choice Theory.
16. Garcia, Natasha. (2018). The use of criminal profiling in cybercrime investigations.
17. Tafoya, W. L. (2006). Criminal Investigation Analysis and Behavior: Characteristics of Computer Criminals. *Forensic Computer Crime Investigation*, 55.
18. Bednarz, A. (2004, November 29). Profiling cybercriminals: A promising but immature science. Network World. Retrieved
19. Buschman, J., Bogaerts, S., Foulger, S., Wilcox, D., Sosnowski, D., & Cushman, B. (2010). Sexual history disclosure polygraph examinations with cybercrime offences: A first Dutch explorative study. *International Journal of Offender Therapy and Comparative Criminology*, *54*(3), 395-411.
20. Panneerselvam, A., 2022. Framework and Challenges of Cyber Security in India: An Analytical Study. *International Journal of Information Technology & Computer Engineering (IJITC) ISSN: 2455-5290*, *2*(04), pp.27-34.
21. Patel Ranjana, 2022. Cyber Security Challenges and their solutions in India: *International Journal of Trend in Research and Development (IJTRD) ISSN: 2394-9333*, 9(1)
22. Kapil A Anil, 2017. Issues, challenges and reasons for privacy threats in e-governance: *Motherhood International Journal of Multidisciplinary Research & Development ISSN: 2456-2831*, 2(1), pp.1-9
23. Jenifer, D.I.M. and Deepamalar, M., 2017. Anti Cyber Crime Technologies for E-Governance.