iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** XI **Month of publication:** November 2022

DOI: https://doi.org/10.22214/ijraset.2022.47443

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue XI Nov 2022- Available at www.ijraset.com

Security of Information Systems and Infrastructure Against Emerging Cyber Threats

Mr. Pogula Karun Raj[1], Mr. Prathapagiri Harish Kumar[2], Bommineni Rishitha[3], Anumandla Siri Chandana[4], Mr Kotha Nikhil Reddy[5]
[1, 2, 3, 4, 5]*Students, Department of Computer Science and Engineering, Kakatiya Institute Of Technology and Science, Warangal, Telangana, India.*

Abstract: ***The information technology revolution that has been occurring over the last three decades has subtly altered how commercial and government activities are conducted worldwide. We have seen the incredible development of the commercial Internet over the past twenty years, which laid the seed for a worldwide, linked digital network that has enabled everything from online banking and commerce to telemedicine and social networks accessible and commonplace. Without taking into account cyber newline security, modern nations all over the world have moved the control of crucial activities in industry, utilities, banking, transportation, and newline communication to networked computers. As a result, there was tremendous output with little expenditures. The move to networked systems is still on the rise. Today, information technology and the newline information infrastructure are absolutely necessary for both our economic and our security. Cyberspace, industrial control systems, and newline information technology are required for the security and efficient operation of India's critical infrastructure, which includes the nation's energy, banking and finance, transportation, communication, and newline base for the defence industry. These systems are susceptible to disruption or exploitation. Organized cyberattacks on our infrastructure may be launched from a newline distance thanks to the cyber newline space. This study was conducted to examine the current situation of developing cyberthreats and ensuing cyberattacks, as well as the efforts taken by different organisations to reduce risk and safeguard their newline information systems and information infrastructure.***
Keywords: Information, Security, E-mail, Cyber attack, Communication and cyber space.

I. INTRODUCTION

The scale and scope of the virtual realm known as Cyberspace have significantly expanded during the past twenty years. The use of the Internet is increasing significantly over the world, and the numerous platforms that rely on it are bringing people who live in different places closer together. A highly linked world as a result of the remarkable rise of commercial Internet has enabled the development of services like telemedicine, social media, online banking, and commerce, among others. These services are not only widely available, but also reasonably priced. Without taking into account the danger associated with the transition to the digital age, modern nations all over the world have moved the control of crucial activities in industry, utilities, finance, transportation, and communication to networked computers[1]. On the one hand, the enormous expansion of information access and increasing digital connection have given people and organisations more power, but on the other, they have presented new difficulties for the public sector and its constituents.

Cyberspace, a virtual environment, is completely distinct from physical space in that it lacks limits and has evolved into a new realm. Today's internet has developed into an unseen thread that holds civilization together, and all societies work through this new cyberspace. Due to the benefits realised, governments are placing a high priority on the development of cyberspace technology. The rapid expansion of networks has significantly accelerated societal progress. The open networks have greatly improved the world's health, wealth, and prosperity by facilitating the easy flow of information and sharing, providing a platform for startups and innovations with lower costs. People and groups may communicate, socialise, and organise themselves in and through cyberspace thanks to the pervasiveness of networks throughout the world. People living all around the world are incorporating cyberspace more and more into their daily lives. Through cyberspace, business organisations located all over the world exchange goods and services[2]. Using the internet for business has sped up transaction times. The internet has developed into a significant sector of the global economy in addition to aiding trade in a number of other areas. Incubators for new businesses are increasingly setting up shop in cyberspace, which also serves as a positive catalyst for the spread of free speech and the creation of new social networking sites that support our economy and uphold our values.

Millions of people's lives have been improved thanks to the exponential growth of digitalization and the widespread accessibility of fast Internet, which has also increased government accessibility to the public for better governance, increased business profits, and enabled efficient competition in the global economy. Such a potent skill also has serious weaknesses that are built in. When leveraged by malevolent actors to conduct cyberattacks using the built-in invisible weaknesses in the cyberspace, this powerful capacity that may enable e-banking, telemedicine, e-auction, e-commerce, and e-governance in seconds has the potential to destroy lives. In order to sustain any nation's well-being, vital communications and electricity distribution networks, as well as the infrastructure of financial institutions, must be tough, strong, and extremely resilient against cyberattacks through cyberspace[3]. The headlines are grabbed daily by stories about malware infections, financial fraud, cybercrime, cyberattacks, etc. by a range of rogue actors. Due to their attacks occurring in a realm without physical boundaries, known as cyberspace, these malicious actors are not constrained by a need to be close to their intended targets. This is a significant problem that calls for coordinated efforts from business, government, academia, users, and cyber security experts [4]. The motivations behind cyberattacks vary; some aim to cause harm and loss for political or military objectives, others are after "trade secrets" and confidential company information, and still others are after financial data that can be used for fraud, identity theft, and other illegal activities like using cyberspace to spread or demonstrate their (terrorists' or other groups') ideology to the world (hacktivism). Through social engineering assaults, these hackers take advantage of holes in computer and network hardware, software, and applications, as well as, most critically, human weaknesses, to bring down even the most protected systems [5]. Due to poor design or the use of outdated software that have not been upgraded or phased out, these vulnerabilities exist in computers and networks. Despite recent advancements in network and information security, stories about dangerous viruses, data breaches, cyber attacks by organised crime, or misplaced laptops with thousands of sensitive client details are still widespread.

II. LITERATURE REVIEW

Due to the topic's recentness, scholars from around the world have written white papers and research papers on it. In addition, a number of businesses that deal in security products for the protection of information systems regularly conduct surveys to determine the trends in cyber attacks and publish reports on their findings. Various organisations, institutes, and associations that are interested in the topic hold seminars, conferences, and workshops throughout the world. The takeaways from these events—actionable intelligence—are then collated and disseminated for further debate. The foundational research for carrying out this study is the examination of these papers, reports, and conclusions/actionable intelligence [6]. Studying the papers pertaining to the safety of the information systems of various organisations gave the needed fuel for more study work. The Indian government has made some progress in the previous ten years on strengthening the information infrastructure by enacting the National Cyber Security Policy and the Information Act, which define cybercrimes and the associated penalties. Because the cyber sector is fundamentally dynamic and always changing, many government policies and initiatives have been examined to see how effective they are in the current situation. Solving the problem of cyber assaults is difficult due to the worldwide character and lack of borders of the cyber domain [7]. Currently, there aren't many bilateral or multilateral agreements or conventions aimed at assigning blame and putting an end to cyberattacks coming from a certain nation. This problem has also been thoroughly investigated, and the research will recommend a course of action. It has been investigated how the Tallinn Manual addresses assaults that are state-sponsored. This document lays out the requirements for what constitutes Cyber War in the eyes of a government on the other. Malware continues to pose a threat to computer networks all across the world, from home users to businesses [8]. The Threat Landscape Report 2014 by Chief Technology Officer, Fortinet 81clearly demonstrates this point. Malware leaves no stone unturned in its quest to enrich its masters. Many people learned the hard way about the importance of adequate data backups thanks to Cryptolocker [9]. According to the research, mobile malware has grown dramatically over the past year, with virtually all of it aiming to compromise the widely used Android platform. The exponential increase of new mobile devices has allowed malware authors to spread their products into a new market, as seen by the uncontrolled growth observed. Today, a significant portion of all Internet traffic is still spam. Spammers transmit literally billions of messages in the hopes that one or two of them may get past anti-spam measures and be clicked on by a user. The number of botnets has decreased, but old botnets and bot software that was formerly believed to be inactive or dormant has begun to resurface [10]. According to the Georgia Tech Information Security Center's (GTISC) Emerging Cyber Threats Report 2014, nation-state hackers compromise businesses, governmental organisations, and non-governmental organisations to build espionage networks and steal data. Cybercriminals continue to find new ways to profit from their victims. Business is hampered by trade-offs between security and usability when organisations shift data to the cloud [11]. Business data is frequently stored in the cloud with no further protection beyond what the cloud storage provider offers.

Although private-key encryption is an option, businesses lose much of the value of the cloud when they encrypt their data on the cloud. Security, usability, and efficiency trade-offs still exist with searchable encryption. According to the IBM X-Force Threat Intelligence Quarterly 4Q 2014, there will be 30 billion connected "things" by 2020, up from 9.9 billion in 2013. These interconnected "things" are primarily controlled by intelligent systems that are constantly gathering and sending data. As more "things" are produced and sold to customers, this connectedness is altering the way we live and raising new issues with Internet security, marketing, and personal privacy. Internet-connected devices that are not securely constructed have been investigated and used by malicious actors looking to control data, identities, and passwords, making them simpler targets than PCs, laptops, or tablets. More than ever, organisations and the employees using this emerging technology need to think carefully about the hazards before connecting to the business safety zone. The 2015 Insider Threat Spotlight Report's main conclusions are as follows: The largest insider danger to organisations comes from privileged users, such managers with access to confidential information (59 percent). Regular workers (48%) and contractors and consultants (48%) are next (46 percent). Insider threats have reportedly increased in frequency during the past 12 months, according to 62 percent of security experts [12]. Only 34%, however, believe that increased funding will help solve the issue. Less than half of organisations have effective safeguards against insider assaults. According to 62% of respondents, insider assaults are far harder to identify and stop than external attacks. According to 38% of survey participants, the cost of cleanup for each insider assault may be up to $500,000. The harm of a successful insider strike is impossible to predict, according to 64% of respondents [13]. The following are the findings of Sophos' 2015 Security Threat Trends report. - The quantity of exploitable vulnerabilities is decreased via exploit mitigations; Attacks on the Internet of Things transition from proof-of-concept to common dangers; Despite not everyone being delighted about it, encryption becomes the norm; more serious problems in widely-used software that the security sector had failed to uncover during the previous 15 years; Increased transparency and culpability are mandated by the regulatory environment, notably in Europe; Attackers concentrate more on mobile payment systems, although for a time, they continue to prioritise traditional payment fraud; The global skills gap is widening, and incident response and education are two significant areas of concentration; For mobile (and other) platforms, attack services and exploit kits appear; the security gap between ICS/SCADA and real-world security only widens; It's possible that intriguing root kit and bot capabilities may reveal new attack methods. The Information Systems Audit and Control Association (ISACA), a non-profit organisation of IT governance experts, created the COBIT framework for IT management in the middle of the 1990s. It offers a number of generally recognised procedures to help in maximising the advantages of using information technology (IT) and creating effective IT governance [14]. It outlines security measures that are advised by the IT auditing community and is frequently regarded as the fundamental security measures that any IT organisation must employ. Internal and external audits usually utilise it as their foundation. The picture illustrates the five principles that are documented in the most recent edition of COBIT (version 5). the control goals that are driven by the seven enablers listed in 1. The high-level control goals are examined in the COBIT framework in terms of their effectiveness, efficiency, confidentiality, integrity, availability, compliance, and dependability [15]. The framework offers a general organisational structure for information technology control and contains control goals that may be used to choose efficient security control goals that are motivated by business requirements. The Information Systems Audit and Control Association (ISACA), which supports and promotes COBIT, invests a lot of resources in this endeavour. It is the framework that is most frequently utilised to achieve Sarbanes-Oxley compliance [16]. This approach has been shown to be the most efficient and helpful for enhancing an enterprise's overall cyber hygiene and cyber security posture. To safeguard information infrastructure, it is simple to execute the measures relating to information security embodied in the framework. The latest version of ISACA's recommendations for the enterprise governance and management of IT is provided via COBIT 5.

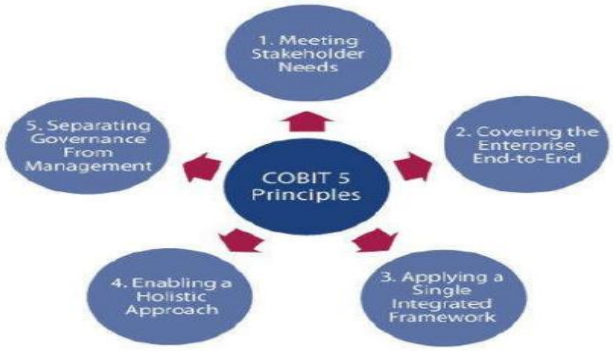


Figure.1. COBIT 5 Principles

It expands upon more than 15 years of actual COBIT usage and implementation by several businesses and users from the business, IT, risk, security, and assurance areas. Cover all areas that contribute to efficient governance and management of corporate IT, such as organisational structures, policies, and culture, in addition to procedures, including the complete range of end-to-end business and IT functional tasks. Gain greater control over the growing number of user-initiated and user-controlled IT solutions and create company value by utilising enterprise IT in new and effective ways. Deal with a far more ubiquitous IT environment; it is becoming a crucial component of the business. Even when IT is aligned with the business, having it separate is frequently no longer acceptable. It must be a crucial component of all corporate initiatives, organisational structures, risk management, policies, competencies, and procedures, among others. The chief information officer's (CIO) position and the IT function are both changing. More and more employees in the business activities are involved in IT operations and decisions and have or will have IT capabilities [17]. It will be necessary to better connect business and IT. The analysis of reports, surveys, incidents, etc.; inputs from magazine articles; and press releases of various attacked companies, among other sources of literature, show that the cyber space is highly vulnerable and that launching an attack on the cyberspace is extremely simple due to inherent vulnerabilities in the information systems and information infrastructure. Because of this and the challenge of attribution, hackers have little chance of being discovered [18]. The threat of a cyber attack is extremely harmful in terms of productivity loss if processes are slowed down, financial loss in terms of lost business and opportunity costs as well as the cost of recovery from the attack, loss of intellectual property & business secrets, loss of sensitive information to an adversary that may affect operations, loss of financial and personal information resulting in significant financial & privacy losses by individuals, etc. The list goes on forever and amply demonstrates how nearly everyone has fallen victim to a cyberattack, whether they are people, corporations, or governments.

III. EMERGING CYBER THREATS

The widespread use of information and communication technology (ICT) by corporate and government organisations alike gives cyber attackers the ability to perform any kind of cyberattacks in cyberspace. Governments, businesses, and individual users are frequently the focus of increasingly dangerous attacks as the Internet becomes more and more essential to economic and societal life. Cyber espionage has been given new life by the triumph of the Internet and the development of cybercrime, making the threat of digital intellectual property (IP) theft real. Trade secrets have been taken from businesses of various shapes and sizes, including Google, Microsoft, Sony, Boeing, Lockheed Martin, and DuPont, proving that criminals are interested in trade secrets wherever they can find them. The reasons for these assaults vary depending on the sort of attacker, who might be a state or non-state actor, a rival corporation, a person or gang, etc. for various reasons. Extremely Rich Cyberspace: For efficiency and effectiveness, the commercial and government sectors are moving their data to cyberspace. In an age where digitization is taking over the globe, even people save their data online. Banks and financial institutions have moved online to provide their clients ad-hoc services. Cyberspace is becoming richer and wealthier with time as more and more data is being digitised and transmitted there. APT1 has showed the capacity and desire to steal from at least hundreds of gigabytes of data from several organisations at the same time. Attacking is Very Simple: Launching an attack does not need the attacker to invest a lot of money. A high-end smart phone or laptop may be used to initiate the assault. Today, anybody may attack a state using the technology that is readily available and the knowledge they have gained from open source. It is quite difficult to attribute: The server and proxy server web can be used by the attacker to conceal himself. Due to a lack of International Laws & Coordination on the Prosecution of Cyber Criminals, establishing the culpability for the attack, even if it is somehow known, is a significant issue. For instance, North Korea recently attacked Sony Pictures Entertainment over "The Interview," a film that depicts the killing of North Korean leader Kim Jong Un. Sanctions were imposed on North Korea by the US government. North Korea has vehemently criticised the United States for imposing sanctions in retaliation for the Pyongyang regime's alleged cyberattack on Sony Pictures while refusing to claim responsibility for the attack.

IV. THREAT ACTORS

Those that want to obtain unauthorised access to computer networks and systems are referred to as threat sources, threat actors, and threat agents. Nation-states, organised crime, and hacktivists are the three main players who consistently appear in both public and commercial sector publications that seek to categorise such threats. It is essential to identify the threat actors engaging in various sorts of cyber-attacks harming the information infrastructures after analysing the rising cyber threats and cyber assaults of various kinds on IT users. Depending on the perpetrator, many reasons may have led to the attack. One of the major traits that set threat actors apart is motivation. For instance, the Hactivists are people who breach into networks primarily for the purpose of upsetting them and making a political statement.

Hacktivism, for instance, refers to the defacing of Indian government websites by Pakistani hackers. Fraudulent individuals who steal from credit card or bank accounts are known as cybercriminals. Cyberspies that conduct industrial or military espionage with the sole goal of collecting industrial secrets from defence contractors or workers are the attackers whose goal is to steal information. Terabytes of information taken from Lockheed Martin or financial data from the IMF (which keeps tabs on the economy of 187 members) are two examples. Nation-states are the main player in today's cyber threat scene. These are the nations and administrations that finance and aid in cyberattacks. according to the figure. 2. Below, there is a shift in the attacker profiles from naive people with constrained technical and financial resources to a state-sponsored organisation with unlimited technical and financial resources and very well defined targets and aims.

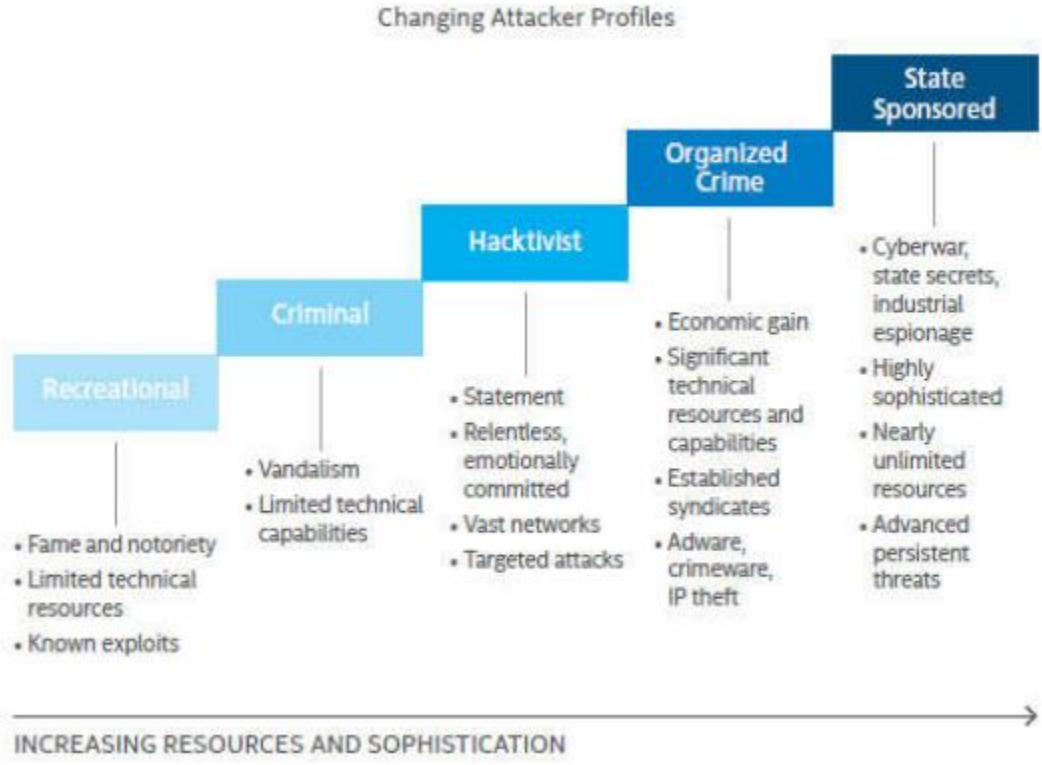


Figure.2. Source: McAfee Labs Threats Report

The introduction of IT into government and private sector organisations over the past three decades, together with the rise of tech-savvy citizens, has led to the collecting and aggregation of enormous amounts of digital data on a global scale. This has presented a challenge to security experts, as well as to government and business organisations, about how to protect this enormous amount of data from ever-increasing cybercriminals and cyberattackers who can steal, corrupt, wipe, or deny access to legitimate users through the use of cutting-edge techniques and highly sophisticated malware. As more systems are connected to the Internet, the number of cyberattacks will continue to rise. In addition to implementing technological security solutions, all users must adopt methods, processes, policies, procedures, controls, etc. to safeguard their essential data and information systems against cyber breaches and assaults. Cybersecurity knowledge and training, the need-to-know principle, operating with restricted rights, the use of up-to-date anti-virus, the usage of patch-updated computer equipment, and the use of secure passwords can all help to lessen cyberattacks by cybercriminals. The notion of personnel hygiene may be applied to cyber hygiene, where you take care of your computers on a daily basis just as you would take care of your body, to prevent cyberattacks on personal computing equipment. You must protect your computing device every day and take preventative actions to lessen cyberattacks. Cyber assaults will never completely disappear since there will always be a knowledge or technology gap between attackers and security experts. However, a nation may build an effective cyber shield to safeguard its information systems and inspire people' trust in the nation's information infrastructure through information exchange, public-private partnerships, coordination, and collaboration between business and academics. An increase in knowledge, more security specialists, technological advancements, and government acceptance of their responsibility to defend citizens online can provide the country's cyber security posture the essential boost.

V. IDENTIFIED CRITICAL INFRASTRUCTURE SECTORS

In order to prevent a crippling impact on security, national economic security, public health or safety, or any combination of these, the United States has defined 16 critical infrastructure sectors, each of which assets, systems, and networks—physical or virtual—are thought to be so essential. A catastrophic cross-sector cascade impact would result from the non-availability, incapacitation, or destruction of the critical information infrastructures (CII), which are crucial assets, systems, and networks. The graphic illustrates how different CII are interdependent on one another. 3. The image demonstrates unequivocally how the collapse of one CII can have disastrous consequences for other CIIs. For instance, a loss of electricity might have an impact on the transportation and telecom sectors as well as the availability of fuel and water to different consumers. For the sake of national security, public safety, and economic success, it is essential to safeguard such CII and ensure their continuity and resilience.

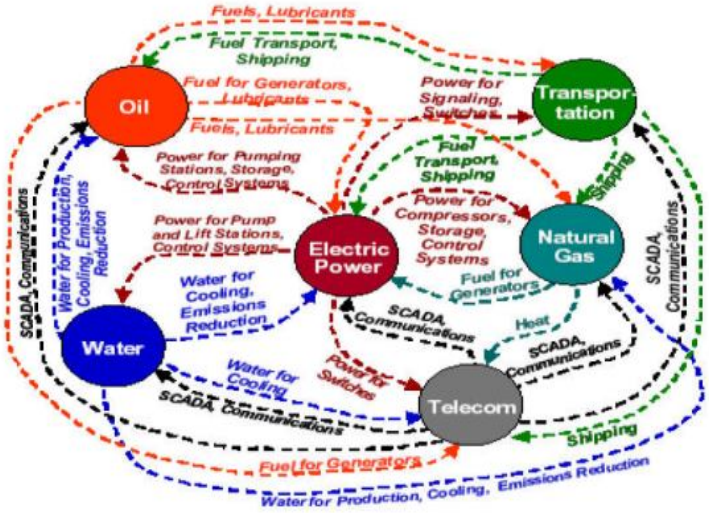


Figure.3. Complexity and Interdependence of CII

It is essential to protect the National CII and establish a system for ongoing cooperation across the critical infrastructure sectors, owners, and operators in the face of the extraordinary growth in targeted cyberattacks by sophisticated adversaries. Around the world, the vast majority of vital infrastructure is either privately owned or run for profit. The owners and operators of critical infrastructure are often in the greatest position to manage operational risks and choose the most effective mitigation measures. The aforementioned diagram makes it very evident how interdependently all CII sectors are, making CII protection a shared obligation. Therefore, it is imperative that different stakeholders from the public and commercial sectors work together to design, implement, and enhance cyber security standards, regulations, and laws in order to protect crucial assets. Governments, the commercial sector, academia, and civil society all rely on critical infrastructure to deliver crucial services and goods, therefore cooperation, coordination, and collaboration are essential to enhancing cyber security and hardening the critical infrastructure. Any nation should concentrate on this because there are increasingly more infrastructures running on Internet-facing networks in every nation, increasing the attack surface for cyberattacks that could jeopardise a nation's critical infrastructure and ability to deliver essential services to its citizens. Exploits that have the potential to harm a nation's infrastructure typically get access to high-value sectors like transportation, energy, or financial networks using basic or sophisticated tools that can access mobile and other personal devices. 155 To combat these constantly changing cyberthreats, all nations must make concerted efforts to improve cybersecurity capabilities in critical infrastructure by giving management-level officials, policymakers, and security personnel working at their critical infrastructure specialised training. All nations should have a national plan that includes achieving safe cyberspace and enhancing cybersecurity capabilities for the protection of vital infrastructure. Due to more individuals connecting at faster Internet speeds than ever before, the world is growing smaller. The expansion of the Internet of Things (IoT) has revolutionised how people interact with one another, transformed commercial operations, and modified how governments and vital infrastructure are run. Despite the inherent hazards, this hyper-connectivity must stay open and available for the growth of governments, businesses, and people alike since it is a potent development instrument that gives everyone the chance to thrive. Our capacity to balance and manage these risks for the foreseeable future is the challenge. Hyperconnectivity's accessibility and openness have made it easier for criminal entrepreneurs to start their businesses because they can now engage in illegal activity practically everywhere.

Because of this, it is challenging for law enforcement to identify the culprit and place of the crime. But in order to defend vital infrastructure from cyberterrorists, we must be aware of the possible threat actors. Internal and external threats are the two basic categories into which risks to CIIs may be divided. One or more people who have access to and/or inside information about a business, organisation, or enterprise that would enable them to take advantage of the weaknesses in that entity's security, systems, services, goods, or facilities are considered internal threats. IT sabotage, fraud, and the theft of confidential or private information are losses brought on by insider betrayals. This could be deliberate or the result of ignorance. External threats, on the other hand, are created by people, groups, terrorists, foreign government agents, and non-state actors and come from outside the organisation. These risks include crippling CII, espionage, cyber/electronic warfare, cyber terrorism, and more.

VI. RESULTS AND DISCUSSION

This analysis of the survey report offers a distinctive viewpoint into the management of information systems in various organisations, information security framework being adhered to, security technologies being adopted, information security policies in place, the number of information security professionals, the reporting chain of the cyber security manager, involvement of top executive management, the information security budget, priorities in spending, the training and education, and the number of information security professionals. The report also looked at how well-prepared organisations were for the always changing cyberattacks. It contained information on actions taken to reduce risks from cyberthreats, technology used, human resource allocation and training, senior executive management engagement and comprehension of cyberthreats, etc. The following key points have emerged after analysing all the replies to the "Cyber Security Administration" questions. Information Security Framework: Nearly 90% of organisations have an information security framework in place, which consists of a security awareness policy, regular information security audits, and monitoring and reporting of incidents. A paradigm for security that includes asset classification for IT assets is used by about 80% of organisations. Alarmingly, just 56% of organisations do not use business continuity management. The fact that just 57% of organisations have CISOs shows that many still consider information security to be a normal IT task, and top management does not see the need for a distinct CISO. Budget for information security: The majority of organisations' (59.6%) budgets for information security are combined with their IT budgets, which leads to insufficient funding for information security. Since the majority of the IT budget is spent on meeting the organization's IT requirements, there should be a separate budget set out for information security. In over 70% of the organisations, the poll finds that less than 10% of the IT budget is set aside for information security. However, the majority of respondents stated that during the past three years, the budget for information security has gradually grown. After compiling all the audits, the cyber audit database contains the audit data for every PC. Using the "Toad for MySql" programme, the assembled report may be exported from the "audit" table. "root" is the default user name and password for connecting to a SQL database on a WAMP server by default.

Figure.4. Exporting audit report

The "audit" table under the "cyber audit" database may be chosen after connecting to the SQL database.

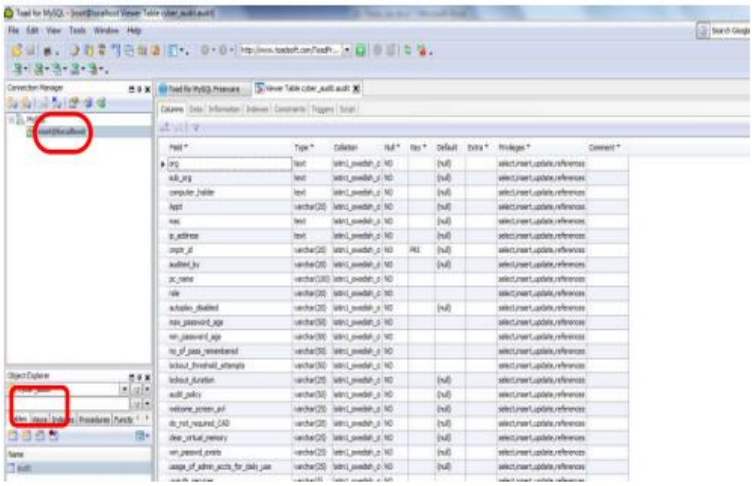


Figure.5. Viewing cyber audit database

Selecting the "Data" column will display the imported data. The exported excel file under current user profile in the folder "My Documents" contains the total report of all the audited PCs for further analysis.

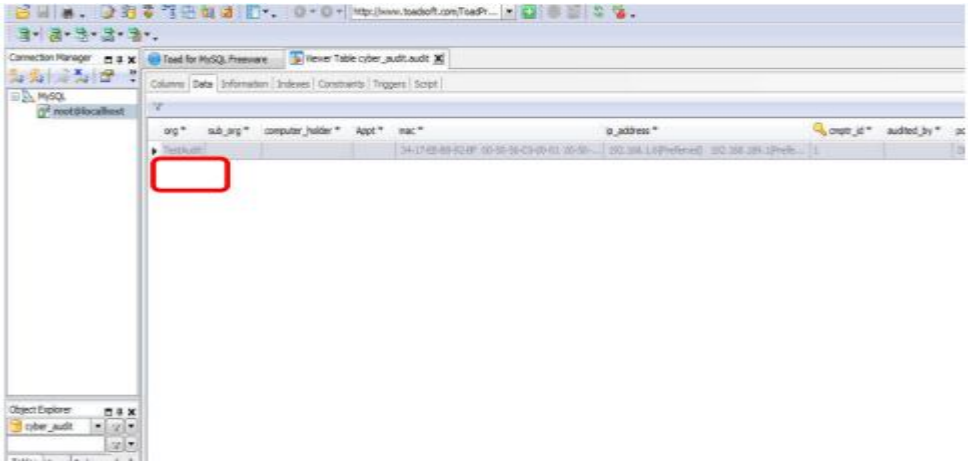


Figure.6. Viewing data column

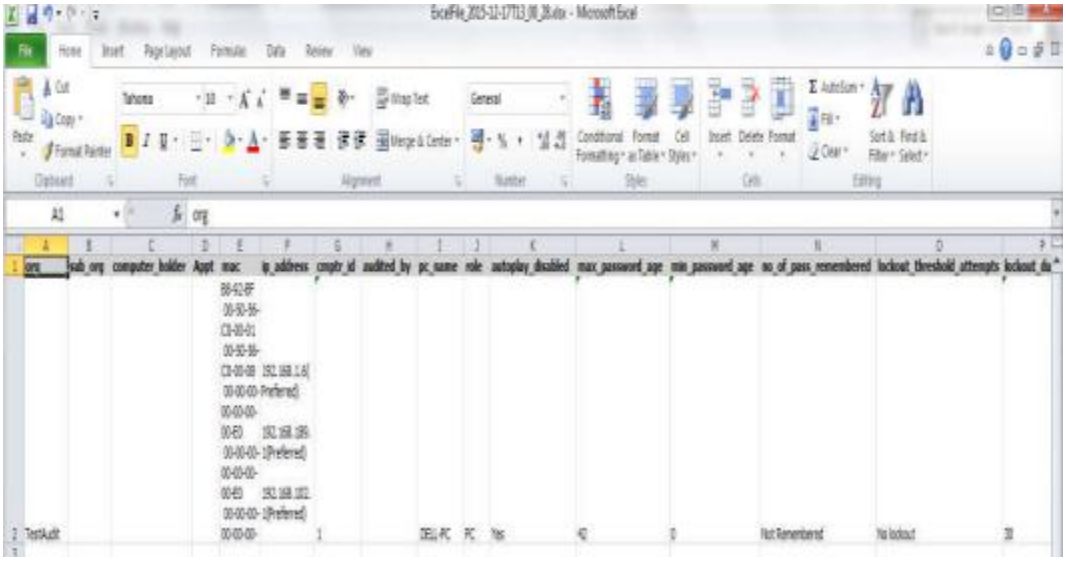


Figure.7. Viewing compiled audit report

The attack surface of the cyber domain will keep growing and expanding at a rapid rate, making it more vulnerable to cyberattacks. The enlarged attack surface will provide new difficulties for the cyber security experts in stopping new kinds of cyberattacks. Cyber security experts will face new hurdles as the Internet of Things (IoT), a major enabling technology for digital commerce, develops. As more and more non-computing devices, such as microwaves, vehicles, hospital systems, medical equipment, drones, escalators, and elevators are connected to the Internet, the network will become more insecure because of these products' inadequate security features and user interfaces. Future cyberattacks would take advantage of less secure IoT. According to industry study by Gartner, there were 3.9 billion linked items in 2018 and there will be 25 billion by the year 2020. As a result, both the quantity of linked objects and things and the frequency of cyberattacks will skyrocket. Cloud computing and big data analytics will go hand in hand with this progress, necessitating a huge increase in the number of security specialists needed to safeguard organisations' information infrastructure against new varieties of cyber attacks. With the introduction of new technologies bringing difficult concerns of cyber security, researchers in the field of cyber security have more work to perform. This work may be used as a springboard for conducting other research in the related area. The idea of "smart cities" is currently all the rage, and cyber security experts need to fight to protect people and their possessions since the more connected you are, the more susceptible you are to cyberattacks. There is a great deal of room for study in this area, and the subject is expanding quickly, giving scholars plenty of chances to do research.

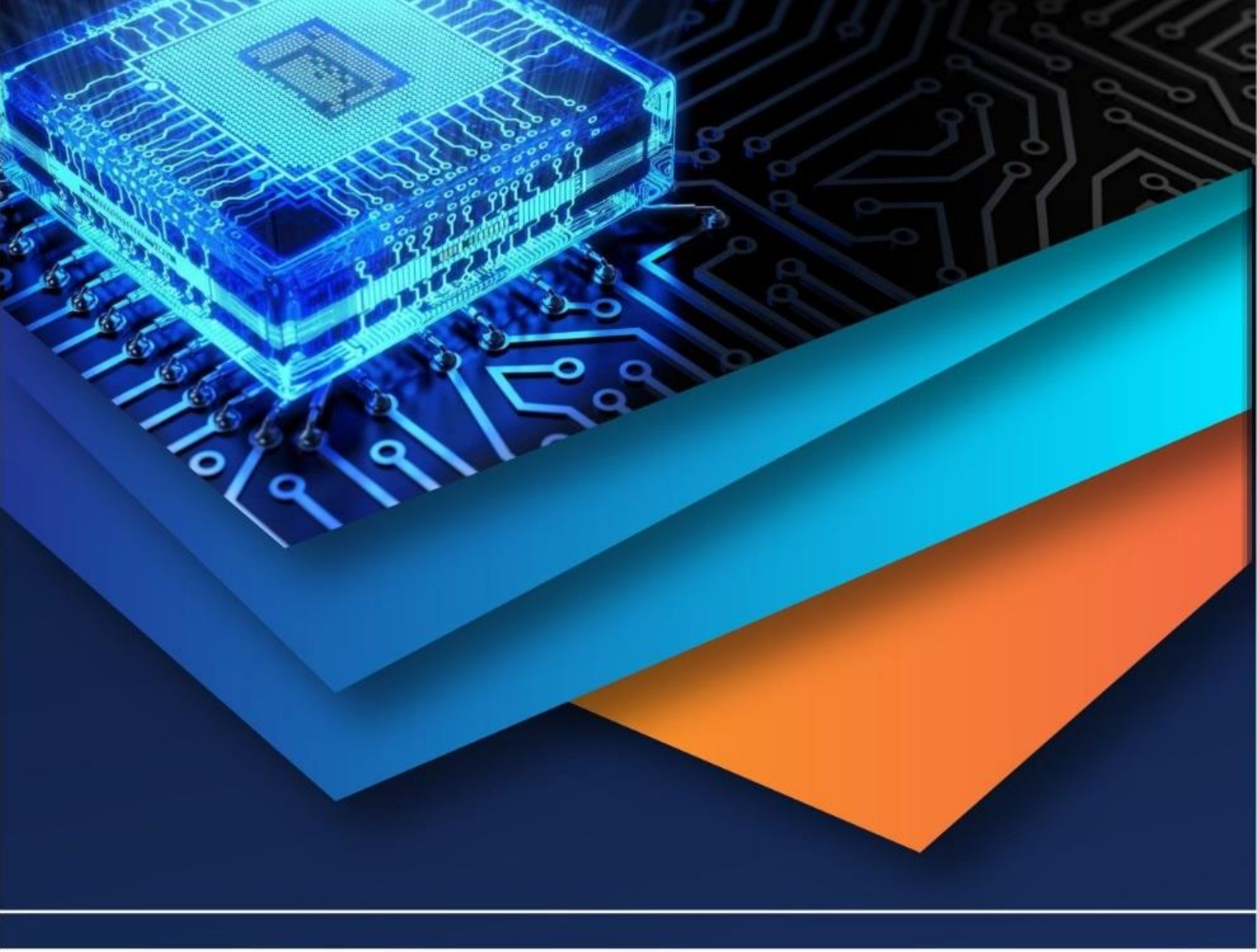
VII. CONCLUSION

It can be said with certainty that no organisation in the world is immune to cyberthreats and has experienced one form of cyber attack or another. There are only two sorts of organisations in the modern world: those that have been hacked and those that are now being hacked. Making organisations robust to emerging cyber-attacks requires information security professionals to take the appropriate measures to develop a security architecture and execute rules. Every organisation needs a plan in place for regularly evaluating its security posture and investing in and upgrading its hardware and technology to lower risk. Additionally, organisations should train information security specialists in the sphere of cyberspace and conduct ongoing employee awareness programmes. Top management needs to be aware of the substantial danger that is posed by cyber security, establish mitigation strategies, and regularly monitor. The company's strategy should include this process, and senior management must play a strategic role in enforcing the cyber-security culture. Every organization's IT resources should be used under the presumption that they are hacked. As a result, in addition to preventative controls, it should emphasise detection and reaction controls. The framework, which is based on the three pillars of people, process, and technology, might be further developed to include detailed implementation instructions for each of the stated controls. The framework might be used in all sorts of fundamental information infrastructures and customised for those that handle sensitive data. Critical information infrastructures should be kept as far away from the Internet as possible, and very tight security measures must be put in place to deter any cyberattacks, as the disruption of these services might endanger the security of the country. Additionally, the audit of computing devices within the organisation must be conducted using the baseline security evaluation software that has been recommended in order to identify any vulnerabilities and recommend countermeasures. It is possible to further customise this auditing tool for different OS systems like Linux and iOS. Implementing an information security architecture and using an audit tool will improve an organization's cyber security posture and enable it to repel various types of cyberattacks. This will take place when the organisation works to close identified security holes and adopts appropriate safeguards to fortify their infrastructure and information systems. This solution will be useful for small firms who cannot afford expensive high-end security systems due to their financial impact on enterprise businesses.

REFERENCES

[1] E. L. Quinn, "Smart metering and privacy: Existing laws and competing policies", SSRN eLibrary, 2009.
[2] Y. Mo, T. H. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, et al., "Cyber-physical security of a smart grid infrastructure", Proc. of the IEEE, vol. 100, no. 1, pp. 195-209, Jan. 2012.
[3] Y. Huang, M. Esmalifalak, H. Nguyen, R. Zheng, Z. Han, H. Li, et al., "Bad data injection in smart grid: attack and defense mechanisms", IEEE Communications Magazine, pp. 27-33, Jan. 2013.
[4] E. Bou-Harb, C. Fachkha, M. Pourzandi, M. Debbabi and C. Assi, "Communication security for smart grid distribution networks", IEEE Communications Magazine, pp. 42-49, Jan. 2013.
[5] P. Mohajerin Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros and G. Andersson, "Cyber attack in a two-area power system: Impact identification using reachability", Proc. Amer. Control Conf., pp. 962-967, Jul. 2010.
[6] Y. Liu, P. Ning and M. K. Reiter, "False data injection attacks against state estimation in electric power grids", Proc. 16th ACM Conf. Comput. Commun. Security, pp. 21-32, 2009.
[7] J. Liu, Y. Xiao, S. Li, W. Lian and C. L. Philip Chen, "Cyber security and privacy issues in smart grids", IEEE Communications Surveys & Tutorials, vol. 14, no. 4, pp. 981-997, Fourth Quarter 2012.

[8] C. Bennett and S.B. Wicker, "Decreased time delay and security enhancement recommendations for AMI smart meter networks" in Innovative Smart Grid Technologies (ISGT 2010), Gaithersburg, MD, pp. 1-6, Jan. 2010.
[9] Z. Sun, S. Huo, Y. Ma and F. Sun, "Security mechanism for smart distribution grid using ethernet passive optical network", 2nd InternationalConference on Advanced Computer Control (ICACC 2010), vol. 3, pp. 246-250, Mar. 2010.
[10] O. Kosut, L. Jia, R. J. Thomas and L. Tong, "Malicious data attacks on smart grid state estimation: attack strategies and countermeasures", Proc. 1st IEEE SmartGridComm 2010, pp. 220-225, Oct. 2010.
[11] D. Conte de Leon, J. Alves-Foss, A. Krings and P. Oman, "Modeling complex control systems to identify remotely accessible devices vulnerable to cyber attack", Proc. First Workshop on Scientific Aspects of Cyber Terrorism, 2002.
[12] D. Kundur, X. Feng, S. Liu, T. Zourntos and K. L. Butler-Purry, "Towards a framework for cyber attack impact analysis of the electric smart grid", Proc. IEEE Int. Conf. Smart Grid Commun., pp. 244-249, Oct. 2010.
[13] D. Jin, D.M. Nicol and G. Yan, "An event buffer flooding attack in DNP3 controlled SCADA systems", Proceedings of the 2011 Winter Simulation Conference, 2011.
[14] Fovino, A. Carcano, M. Masera and A. Trombetta, "Design and implementation of a secure Modbus protocol" in Critical Infrastructure Protection III, Boston, MA:Springer-Verlag, vol. 311, pp. 83-96, 2009.
[15] J. Yu, A. Mao and Z. Guo, "Vulnerability assessment of cyber security in power industry", Proc. of IEEE Power and Energy Society General Meeting (PES'06), pp. 2200-2205, 2006.
[16] E. K. MacLean, "Joseph e. davies: The wisconsin idea and the origins of the federal trade commission", The Journal of the Gilded Age and Progressive Era, vol. 6, no. 03, pp. 249-284, 2007.
[17] J. T. Kelsey, "Hacking into international humanitarian law: The principles of distinction and neutrality in the age of cyber warfare", Michigan Law Review, pp. 1427-1451, 2008.
[18] K. Intelligence, Trends in cyber security environment for 2015, 2015, [online] Available: http://www.k2intelligence.com/en/trends-in-the-cyber-security-environment-for-2015.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY