IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 5, May 2022

An Examination on Rising Threats of Cyber Security

Anu Sharma, Assistant Professor,
College of Computing Sciences and Information Technology, Teerthanker Mahaveer University,
Moradabad, Uttar Pradesh, India
Email Id- er.anusharma18@gmail.com

ABSTRACT: ***The discipline of securing our computer systems, data, and networks against weaknesses or outside attacks is known as cyber security. The risk of cyberattacks is rising along with the number of internet users. It is crucial that we take the appropriate precautions to defend ourselves against these assaults and prevent unintended harm. The main objective of this study is to concentrate on emerging cyber security trends as new technologies like mobile computing, cloud computing, e-commerce, and social networking become more widely adopted. Although they are crucial, firewalls, antivirus software, and other technical solutions to secure user data and computer networks fall short. The development of information technology as well as Internet activities depends on cyber security. Our attention is typically focused on "Cyber Security" whenever people hear about "Cyber Crimes". As a result, when we talk about "National Cyber Security", people first think about how prepared our infrastructure is to handle "Cyber Crimes". It is essential to teach our folks how to use the cyber infrastructure that our nation is rapidly developing. The results conclude that the goal of cyber security, often referred to as information technology security, is to prevent unauthorized access to, alteration of, or destruction of computers, software, systems, and connections.***

KEYWORDS: ***Business, Cyber Security, Cyber Crime, Information Technology, Internet.***

1. INTRODUCTION

The internet is one of the most rapidly developing sectors of technological infrastructure. Disruption technologies such as cloud computing, social computing, and next-generation mobile computing are radically transforming how businesses use informational technology to share information and do business online in today's business climate. Because more than 80% of all commercial transactions are now conducted online, this area necessitated a high level of security to ensure transparent and efficient transactions [1]. Cyber Security encompasses not just the security of Information Technology (IT) systems within the organization, but also the larger digital networks on which they rely, such as cyberspace as well as critical infrastructures. Cyber security is critical to the advancement of both information technology and Internet services. Improving cyber security as well as safeguarding important information infrastructures are critical to the security and economic well-being of any country [2]. Cyber systems have grown more important in many aspects of human life, including business, banking, health care, energy, entertainment, communications, and national defense [3].

According to recent study findings, public concern over privacy and personal information has risen since 2006. Web users are concerned that they are disclosing too much personal details and wish to be forgotten when there are no genuine reasons to do so. Exploring the metaphors we use in the cyber security area might help us think and talk better in four ways. First, we could acquire a better grasp of the usefulness and limitations of the concepts we've mapped into the cyber security domain from other domains. Second, experimenting with less frequent or novel metaphors may

ISSN PRINT 2319 1775 Online 2320 7876
Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 5, May 2022

pique the interest of scholars and policymakers. Third, highly effective metaphors might be expanded into entirely new frameworks as well as sets of concepts for solving cyber security issues. Fourth, a metaphor works as a heuristic device, allowing non-specialists to get a better grasp of abstract notions from the subject of cyber security by applying them to realms with which they are more connected or familiar [4]. Public's attention and judgments while setting up, maintaining, and using computers and internet are critical to cyber security. Physical protection (including hardware and software) of personal information and technology resources against unwanted access achieved through technical methods is covered by cyber-security. Challenges cannot be handled with the same degree of knowledge that generated them, according to Albert Einstein. The challenge of End-User Errors cannot be solved by just adding more technology; it must be tackled via a collaborative effort and collaboration between the Information Technology community of interest as well as the broader business community, as well as senior management's vital support.

Digitalization is an ongoing, ever-expanding process that has been going on for a long time. The digitization process ideally helps to eliminate a large portion of manual labor as well as considerably boost efficiency [5]. Technology has become increasingly important in our culture, economy, and essential infrastructure. In a 2018 cybersecurity assessment, Siemens claimed that "the digital world is stimulating change in everything," as billions of devices are connected through the Internet of Things (IOT). This has enormous promise for the globe, but it also carries a significant degree of danger. While we celebrate the benefits of digitization by integrating a larger portion of essential infrastructure, the economy, and society into cyberspace, it also provides a fertile ground for cybercriminals to exploit the same benefits. According to the authors, as our reliance on information technology grows, criminals will have more motivation to commit crimes, which might result in catastrophic consequences. Vital infrastructure, cybercrime, cultural relevance, risks, and problems are all important topics.

Cybercrime became one of the globes fastest rising threats. Internet dangers evolve at a far quicker rate than threats to military capabilities or international terrorism. While the latter takes months or even years to evolve, cyber dangers are continually evolving. Focusing on the catastrophic amounts of cybercrime that have occurred throughout the world is an indication of the current world's status of cybersecurity. This isn't to imply that cybersecurity isn't a concern. There is no such thing as 100% secure cybersecurity, according to Communications Electronics Security Group (CESG). At some time, every organization will be attacked in some way [6]–[9].

Being vulnerable to assaults indicates that there is a serious issue that must be addressed. If it is not handled, it will breed distrust and result in a slew of issues. If the requirement for security isn't baked in all the time then we're not going to be making headway in the degree of assurance that people all need in the future, said Joel Jacobs, the Chief Information Officer and Chief Security Officer Corporations. This remark undoubtedly portrays a bleak picture if cybersecurity is unable to provide the much-needed data protection. As a result, there is more ambiguity. While uncertainty will always exist in cyberspace, we may endeavor to find strategies to lessen the levels of uncertainty by exploring and adopting accessible tools. According to CESG's report on ways of reducing the effect of common cybersecurity attacks, the majority of attacks can be avoided and the resulting impact reduced significantly by properly implementing as well as utilizing

ISSN PRINT 2319 1775 Online 2320 7876
Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 5, May 2022

components of governance, aspects of risk management, instilling factors of consciousness, and being proactively prepared to address possible emerging threat factors [10], [11].

The purpose of this study is to emphasize the need of having a sound cybersecurity strategy by defining cybersecurity in key infrastructure components. Explanation about cybercrime and its magnitude. The report also looks at cybersecurity problems in terms of governance, risk management, culture, and awareness, as well as upcoming cybersecurity threats. The purpose of emphasizing these aspects is to demonstrate the true extent of cybersecurity. It will also stress the need of implementing comprehensive cybersecurity, which necessitates a thorough awareness of the problems and dangers so that any breaches or attacks may be avoided and the damage reduced to the greatest extent feasible. While we are making computing advances into the quantum domain, it is not a stretch to believe that we will be able to use these technologies to foresee potential inbound attacks before they happen. Furthermore, while technology is not the only factor in play, it is critical to shift cultural perceptions and skepticism in order to solve challenges with the human factor. In the end, this will represent the necessity for more in-depth study in the hopes of uncovering solutions to problems and proactively controlling growing risks.

2. DISCUSSION

Digitalization is an ongoing, ever-expanding process that has been going on for a long time. The digitization process ideally helps to eliminate a large portion of manual labor as well as considerably boost efficiency. Technology has become increasingly important in our culture, economy, and essential infrastructure. In a 2018 cybersecurity assessment, Siemens claimed that "the digital world is stimulating change in everything," as billions of devices are connected through the Internet of Things (IOT). This has enormous promise for the globe, but it also carries a significant degree of danger. While we celebrate the benefits of digitization by integrating a larger portion of essential infrastructure, the economy, and society into cyberspace, it also provides a fertile ground for cybercriminals to exploit the same benefits. According to the authors, as our reliance on information technology grows, criminals will have more motivation to commit crimes, which might result in catastrophic consequences. Vital infrastructure, cybercrime, cultural relevance, risks, and problems are all important topics.

2.1. Challenges of Cyber-security:

The cybersecurity firm's challenges are as varied as the profession itself. As technological advances arise as well as modify firms' cybersecurity procedures, the cybersecurity environment is always evolving. Businesses across all industries must encourage their IT departments to improve their cybersecurity infrastructure as well as provide relevant cybersecurity training to all important choice in the company, whether Internet of Things (IoT) grows in size as well as scale or the emergence of 5G networks. Some of the challenges for cyber-security are as given below:

- Adapting to a remote workforce:

It's no mystery that the number of individuals working remotely has increased dramatically. As the epidemic continues to wreak havoc on communities throughout the world, many businesses are opting for hybrid work methods, whether they reopen their offices or hire a remote staff. The

ISSN PRINT 2319 1775 Online 2320 7876
Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 5, May 2022

quantity and scope of cybersecurity concerns for remote employees grows as a result of a distributed work environment. Remote workers who utilize their home networks are far more likely to be victims of security breaches. In-person employees are safeguarded in traditional office environments, but it's more difficult to assure safety for remote employees. When it comes to defending remote employees and the business itself in a remote environment, our remote working checklist is a smart place to begin.

- Emerging 5G applications:

When 5G was first introduced this year, several businesses were eager to take use of its capabilities, whether it was mobile phone carriers selling it to their clients or manufacturing trying to boost operational efficiency. 5G will improve the speed as well as responsiveness of wireless communications, and the new technology has a promising future. New technologies, on the other hand, bring new dangers to bear, and cybersecurity experts must be on the lookout for threats to these evolving networks.

- Cryptocurrency and Block chain attacks:

The world of block chain and cryptocurrency is exploding, gaining more attention than ever before. Because crypto transactions are digital, it's only natural that security precautions be taken to avoid identity theft, security breaches, and other possible hazards. Any information that an investor, a crypto exchange, or a corporation dealing with block chain or cryptocurrency wants to be hacked is the last thing they want. As a result, businesses must consider significantly investment in their IT infrastructure and safeguarding themselves in the case of a cyberattack.

- Internet of Things (IoT) Attacks:

For those unfamiliar with the Internet of Things (IoT), it is the connecting of physical items via the use of numerous sensors that interact with one another. As more data is sent between devices, holes may appear, allowing hackers and other cyber criminals to exploit data. While linked gadgets are recognized for their convenience and intelligence, it is evident that they give thieves greater opportunity to exploit networks. As the world grows more linked, businesses must remain ahead of the curve by creating a robust cybersecurity infrastructure and a specialized IT staff. Fortunately, legislation dubbed the Internet of Things Cybersecurity Act of 2020 is in place. The legislation establishes security requirements for IoT devices and covers other IT concerns, ensuring that IoT devices and their usage are protected to some extent. While one deed may not be sufficient, it is unquestionably a step in the right direction.

3. CONCLUSION

This study has covered the significance of privacy for people as a fundamental human right. Human rights abuses include things like the wrongful collection and storage of personal data, problems involving inaccurate private information, misuse, or unauthorized dissemination of such data. This research also covers the current threats, problems, obstacles, and measures facing the IT sector in our society. The need for an efficient intrusion detection model with high accuracy

ISSN PRINT 2319 1775 Online 2320 7876
Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 5, May 2022

and real-time performance is more than ever given the surge in cyberattacks. Indian citizens must decide which security measures are most appropriate for protecting their data, systems, and the networks they use. The IT industry has been catching up with cybercriminals for years. Findings from this study are crucial for understanding cybersecurity risks and difficulties. More research is required in areas like cybersecurity governance and critical infrastructure, cybersecurity framework implementation and proper risk management, culture and awareness: the role of human perception, as well as emerging trends that are considered emerging risks. While this study offers helpful information on challenges and emerging threats.

REFERENCES:

[1] A. Kigerl, "Cyber crime nation typologies: K-means clustering of countries based on cyber crime rates," *Int. J. Cyber Criminol.*, 2016, doi: 10.5281/zenodo.163399.

[2] M. Lagazio, N. Sherif, and M. Cushman, "A multi-level approach to understanding the impact of cyber crime on the financial sector," *Comput. Secur.*, 2014, doi: 10.1016/j.cose.2014.05.006.

[3] H. Saini, Y. S. Rao, and T. C. Panda, "Cyber-Crimes and their Impacts : A Review," *Int. J. Eng. Res. Appl.*, 2012.

[4] R. Broadhurst, P. Grabosky, M. Alazab, and S. Chon, "Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime," *Int. J. Cyber Criminol.*, 2014.

[5] K. Dashora and P. P. Patel, "Cyber Crime in the Society: Problems and Preventions," *J. Altern. Perspect. Soc. Sci.*, 2011.

[6] P. Aggarwal, "Review on cyber crime and security," *Int. J. Res. Eng. Appl. Sci.*, 2014.

[7] S. Yu, "Fear of cyber crime among college students in the United States: An exploratory study," *Int. J. Cyber Criminol.*, 2014.

[8] S. Haugen, "E-government, cyber-crime and cyber-terrorism: a population at risk," *Electron. Gov.*, 2005, doi: 10.1504/eg.2005.008331.

[9] K. Kittichaisaree, "Cyber Crimes," in *Law, Governance and Technology Series*, 2017.

[10] M. Olusola, O. Samson, A. Semiu, and A. Yinka, "Cyber Crimes and Cyber Laws in Nigeria," *Int. J. Eng. Sci.*, 2013.

[11] R. Leukfeldt, S. Veenstra, and W. Stol, "High volume cyber crime and the organization of the Police: The results of two empirical studies in the Netherlands," *Int. J. Cyber Criminol.*, 2013.