International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi :https://doi.org/10.32628/IJSRSET

Cyber Security

Pratiksha Pralhad Mate, Palve Payal Shahadeo, Patel Hemant
Department of Computer Engineering, Zeal College of Engineering and Research, Pune, Maharashtra, India

Article Info
Volume 9, Issue 1
Page Number : 315-317

Publication Issue :
January-February-2022

Article History
Accepted : 05 Feb 2022
Published: 28 Feb 2022

ABSTRACT

In the current world that is run by technology and network connections, it is crucial to know what cyber security is and to be able to use it effectively. Systems, important files, data, and other important virtual things are at risk if there is no security to protect it. Whether it is an IT firm not, every company has to be protected equally. With the development of the fresh technology in cyber security, the attackers similarly do not collapse behind. They are consuming better and enhanced hacking techniques and aim the weak points of many businesses out there. Cyber security is essential because military, government, financial, medical and corporate organizations accumulate, practise, and stock unprecedented quantities of data on PCs and other devices. An important quota of that data can be sensitive information, whether that be financial data, intellectual property, personal information, or other various kinds of data for which illegal access or acquaintance could ensure negative concerns.

I. INTRODUCTION

An effective cybersecurity method has numerous layers of defence spread across the networks, computers, programs, or informations that one aims to keep non-toxic. In a society, the processes, the people and tools must all accompaniment one alternative to generate a real defence on or after cyber-attacks. A unified threat management system can mechanise additions across select Cisco Security goods and speed up key security processes functions: discovery, examination, and remediation.

Definition

It could be defined as the procedure to ease the security fears in order to protect repute damage, commercial loss or financial loss of all group. The term Cybersecurity obviously required that it's a gentle of security that we proposal to the organisation that frequent users can contact using the internet or over a network. There are numerous tackles and techniques that are castoff to deploy it.

GOALS

definitive objective of cybersecurity is to defend the data from actuality stolen or co-operated. To attain this we aspect at 3 important goals of cybersecurity. 1. Defensive the Privacy of Information 2. Conserving the Integrity of Information 3. Controlling the Obtainability of information only to approved users These objectives practise the confidentiality, integrity, availability (CIA) triad, the base of entirely safety agendas. This CIA triad model is a safety model that is intended to guide strategies for data security inside

the places of a society or corporation. This model is similarly mentioned to in place of the AIC (Availability, Integrity, and Confidentiality) triad to side-step the mistake with the Central Intelligence Agency. The rudiments of the triad are reflected the three greatest vital mechanisms of safety. The CIA standards are one that greatest of the societies and businesses practice once they have connected a new request, makes a record or when assuring access to approximately information. On behalf of data to be totally safe, all of these safe keeping areas must originate into result. These are safe keeping strategies that all effort together, and hence it can be incorrect to supervise one policy. CIA triad is the greatest collective standard to measure, choice and appliance the proper safety

II. LITERATURE SURVEY

Kelechi G. Eze (keze@student.pvamu.edu) is a doctoral student at Prairie View A&M University, Texas. He is a student member of IEEE. His research interests include cyber security, data security and privacy, blockchain technology, wireless sensor networks, and machine learning. Matthew N.O. Sadiku (sadiku@iee.org) is a professor at Prairie View A&M University, Texas. He is the author of several books and papers. He is an IEEE fellow. His research interests include computational electromagnetics and computer networks. Sarhan M. Musa (smmusa@pvamu.edu) is a professor in the Department of Engineering Technology at Prairie View A&M University, Texas. He has been the director of Prairie View Networking Academy, Texas, since 2004. He is an LTD Sprint and Boeing Welliver Fellow.

III. APPLICATION

Potential Applications Some of the significant applications of cyber security include :

- government organization
- Military
- finance sector
- hospitals
- college
- school
- institutes

IV. DIS-ADVANTAGES

- Difficult to implement it
- high cost of hardware and software
- Makes the system slower than before.
- Need to keep updating the new software in order to keep security up to date.

V. ADVANTAGES

1. Develop a Security-Focused Culture

When you offer training to your employees on a topic, this is communication to them that it's important. At this level of importance is a natural transition to have safety be one of your culture's foundations. Regular training instils better habits.

2. Empower Employees

When employees feel confident about their interactions with data that must follow security protocols, the less likely they are to cause an incident. Human error is after all the leading cause of breaches and attacks

3. Protect Assets

A security breach is not only devastating to a company's reputation, but it's also a big hit to finances. According to the IBM Pokémon 2017 Cost of Data Breach report, the average cost is $3.62M.

4. Prevent Downtime Should a breach or incident occur, it takes considerable time to investigate and repair That's precious time that your staff has to devote to getting back up and running..

- Develop a Security-Focused Culture
- Empower Employees
- Expand Awareness to Reduce Threats
- Collect Risk Data by Driving Awareness

- Increase Adoption
- it gives privacy to user
- Protection against data from theft
- Protect our system against viruses worm or unwanted programs.

VI. CONCLUSION

Conclude that, All organizations need to understand their threat environment and the risks they face, address their cybersecurity problems, and hire the most appropriate people to do that work.

Even large organizations with top talent and significant resources devoted to cybersecurity have suffered major cybersecurity compromises, and organizations that do not have such levels of talent or resources face even greater challenges. More highly skilled workers in cybersecurity roles would help the nation respond more robustly to the cybersecurity problems it faces. All organizations need to understand their threat environment and the risks they face, address their cybersecurity problems, and hire the most appropriate people to do that work.

VII. FUTURE SCOPE

Several researches and discussions are going on across the world among technologists, researchers, academicians, vendors, operators, and governments about the innovations, implementation, viability, and security concerns of cyber security.

Moreover, governments and regulators can use this technology as an opportunity for the good governance and can create healthier environments, which will definitely encourage continuing investment in cyber security,

VIII. REFERENCES

[1]. https://cltc.berkeley.edu/scenario-back-matter/
[2]. https://cltc.berkeley.edu/scenario-back-matter/
[3]. https://www.getgds.com/resources/blog/cybersecurity/6-cybersecurity-threats-to-watch-out-for-in-2021
[4]. https://www.google.com/search?q=what+are+the+conclusion+of+cyber+security%3F&biw=1536&bi