RESEARCH HUB – International Multidisciplinary Research Journal (RHIMRJ)
Research Paper

A Study of Cyber Security Challenges and Importance

Devendra G. Pandey

Assistant Professor, M.Sc.(I.T.),Veer Narmad South Gujarat University, Surat, Gujarat, India

Abstract: ***In fact cyber security plays an important feature in the field of technology. Security of facts has certainly become one of the biggest challenges within the contemporary times. Whenever we think of cyber security the primary aspect that comes to our mind is 'cyber crime' which is increasing immensely every day. Various governments and agencies are taking various measures to protect you from these cyber crimes. With the exception of various measures, cyber security remains an all-too-big situation for many. This paper mainly focuses on the challenges faced through cyber security on ultra modern technology. It also focuses on contemporary about cyber security techniques, ethics and trends that are changing the face of cyber security.***

Keywords: cyber security, challenges, importance.

Introduction

These days man is able to give and receive any kind of facts, be it an e-mail or an audio or video, honestly through the use of a button, but did he ever wonder how much his identity of facts? Safely transmitting or sending alternate character with complete data leakage?? The answer lies in cyber security. Nowadays internet is the fastest growing infrastructure in every day life. In the technological environment these days many current techniques are changing the face of character types. But due to these emerging technology we are unable to protect our personal data in a fully effective way and as a result cyber crimes are evolving every day nowadays. Nowadays more than 60 percent of normal commercial transactions are done online, hence the sector needs high security for transparent and exceptional transactions. That's why cyber security has ended up being a trendy hassle.

The scope of cyber security is not limited to achieving records only in the IT industry but also in various fields like cyber sector etc. Even the ultra-modern generation like cloud computing, cellular computing, e-change, net banking, etc., desire extreme levels of security. Given that technologies hold some important data related to an individual, it has become necessary to issue their security. Increasing cyber security and defensive vital statistics infrastructure is critical to the security and financial well-being of every country. Making the Internet more comfortable (and protective Internet users) has become essential to the development of recent offerings in addition to government insurance. The fight against cybercrime requires a holistic and more secure technology. Given that technical measures by themselves cannot protect you from any crime, it is imperative that law enforcement agencies be allowed to properly investigate and prosecute cybercrime. Today many countries and governments are enforcing strict felony signs on cybersecurity so that you can avoid missing out on some important information. Each character also has to study in this cyber security and protect himself from the increasing cyber crimes.

Challenges to cyber security

With the increasing generation attackers have developed some methods to circumvent the security of the device. Now a lot of techniques or techniques through which they may be able to try to gain access to an instrument. In there are some techniques through which a hacker can take advantage of any tool if the equipment has terrible cyber security. So we definitely need to maintain our gadgets comfortably from them. Yet some countries have terrible cyber security due to poor cyber security size, which is why attackers can cause cyber security without causing harm and corrupting their facts. There are many countries whose literacy rate is terrible and if we talk about cyber security then human beings understand very little about it.

2015, RHIMRJ, All Rights Reserved *ISSN:* 2349-7637 (Online)

Now not the easiest humans but the teachers who teach cyber security are not well up to date about the contemporary developments in cyber security so it is very important to be really updated. Hackers constantly use different strategies to circumvent the security of the device. We are not aware enough and as human beings, we are not prepared, our online world is a preaching threat to the countries on the global network. regardless of the increasing number. of the consumers are still being supplied under the prior or minimum ordinance. One of them is the preaching purpose and conditions for fame and recognition of the work done in the name of our online world. Our online world is representing the security risks and undertakings of the present day. The development and application of facts and verbal exchange technology has created a new difficulty of the battlefield. As a special task for global security, cyber terrorism arises. Cyber security will have a significant impact on members of the global family within the twenty-first century.

Importance of cyber security

The importance of cyber security goes all the way up to the selection of data, data and gadgets to keep them personal and secure. Across today's world, humans store large chunks of information about computer structures and gadgets connected to the Internet of sorts. Its a lot to do with passwords or monetary data being really sensitive.

If cybersecurity were to take advantage of access to this information, they could inspire a number of issues. They may want to share sensitive data, use passwords to get around price ranges, or perhaps change information so that it blesses them in some way.

Organizations want cybersecurity to keep their records, rate diversity and highbrow stuff safe. People want it for comparable purposes, no matter the reality that intellectual property is little of an element, and there is a high risk of losing important documents, in conjunction with a cycle of relative images. In the case of public services or government organizations, cyber security allows ensuring that the network can protect what their offerings depend on. For example, if a cyber attack targets a power plant, it could lead to the Metropolis-Great Blackout. If it focuses on one financial group, it can borrow from masses of hundreds of people.

Conclusion

Cyber security are an important problem and there is a strong link between the Internet and the structures to carry out sensitive sporting activities. Many corporations, institutions, authorities are the primary risk to the surrounding area (a relatively significant improvement). Cyber security technology in all its dimensions can be vital for improvement, creativity and benefits for agencies alike. There is no one way to truly sustainability, but corporations will flow as a global capability that is transparent and robust, using the way executives and enterprise alliances participate through helping safeguards. and is rich, desired in terms of task-critical structures, strategies and technologies that may pertain to cyberspace. Since cyber security is not just a technical task, a successful international cyber security team can require a great deal of critiques and information. The bigger problem seems to be that improvements are evolving every day, and so are the revolutionary ways to exploit cybersecurity for malware and cyberterrorism strategies. Due to the combination of the interconnected complexity of growing economies and therefore the extraordinary release structures, it is essential that there is a general subculture in the region toward cyber security threats. In order to manage the security problems, the economic offering industry will move through the strong protective capability.

REFERENCES

1. G.NIKHITA REDDY, G.J.UGANDER REDDY (2013) " Study of Cloud Computing in healthcare Industry",, Volume 4, Issue 9, Page nos.68 – 71 ISSN 2229-5518.
2. BOOZ ALLEN AND HAMILTON, REPORTS, (2012) Top Ten Cyber Security Trends for Financial Services" Business wires, Berkshire, Hathaway.

2015, RHIMRJ, All Rights Reserved *ISSN:* 2349-7637 (Online)

3. LIPSON (2002) Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues, Carnegie Mellon Software Engineering Institute, Pittsburgh.
4. AKHGAR B., ARABNIA H.R (2014) Emerging Trends in ICT Security, Morgan Kaufmann, Boston, pp. 507-516.
5. NICHOLSON A., ET AL. (2012) SCADA security in the light of cyber-warfare Comput. Secur., 31 (4), pp. 418-436.

2015, RHIMRJ, All Rights Reserved

ISSN: 2349-7637 (Online)