International Journal of Academic Engineering Research (IJAER)
ISSN: 2643-9085
Vol. 5 Issue 1, January - 2021, Pages: 22-23

Cyber Threats as a Power of Fruitful Solution

Saidova Kamila[1] and Kendjaeva Gulrukh[2]

[1]Bukhara State University, Faculty of Foreign languages English literature department, 2nd year student.
[2]Scientific supervisor:
Phone: +998902996042
Gmail: sadovakamila06@gmail.com

Abstract*. The given article is directed into such global issue as cyber threats on world society. Therefore, with the great impact on this issue there given strategies how to be aware thus to put a fruitful resolution.*

Keywords: cybercrime, physical storage disks, telecommunications, industrial sector, software. cybersecurity.

Introduction

What concerns Strategies against cyber threats recent approaches firmly go further into combat a global issue. Nowadays Almost all companies and various services in many countries of the world have faced cyber-attacks.

The given statistics of these studies has shown the vast majority of U.S. small businesses lack a formal Internet security policy for employees and only about half have even rudimentary cybersecurity measures in place. Furthermore, only about a quarter of small business owners have had an outside party test their computer systems to ensure they are hacker proof and nearly 40 percent do not have their data backed up in more than one location.

Methods. The most popular methods of fighting cyber threats to businesses around the world are: anti-virus protection (installation of anti-virus programs and anti-virus equipment)

Private sectors suppose that the first and foremost solution to prevent cyber-attacks on companies is to have a secure and sophisticated hardware which are password protected and backed up by 2-way authentication. Also, it is better if you don't overlook the effectiveness of protecting your physical storage disks. Because if neglected, then it gives an opportunity to anyone and everyone to walk away with your firm's sensitive data

Basically there are the following strategies against risk and threats on the specific research which is still being observed. the NATO forces need an array of robust, sophisticated, and evolving capabilities across all domains to meet today's and tomorrow's security challenges,

Realizing that the Alliance remains in a technological adoption race which may not be won by those with the best technology, but by those with the most agile organizations,

Recalling that since the foundation of the Alliance NATO's technological edge has been pivotal for maintaining peace and security in the Euro-Atlantic region,

Recognizing the increasing contribution made by networked information technologies to many of the essential functions of daily life, commerce and the provision of goods and services, research, innovation and entrepreneurship, and to the free flow of information among individuals and organizations, governments, business and civil society,

Noting with satisfaction the work of relevant national and international organizations on enhancing cybersecurity, and reiterating their role in encouraging national efforts and fostering international cooperation.

Retention of arbitrary inference on the citizen's privacy.

Privacy is a fundamental human right recognized in the UN Declaration of Human Rights, the International Covenant on Civil and Political Rights and in many other international and regional treaties. Privacy underpins human dignity and other key values such as freedom of association and freedom of speech. It has become one of the most important human rights issues of the modern age. The publication of this report reflects the growing importance, diversity and complexity of this fundamental right.

Almost every foundation in the world discover a right of privacy explicitly in their Constitution. These provisions include rights of inviolability of the home and secrecy of communications.

The leading research of information technology with its capacity to collect, observe and analyze information on individuals has introduced a sense of urgency to the demand for legislation. Furthermore, new developments in medical research and care, telecommunications, advanced transportation systems and financial transfers have dramatically increased the level of information generated by each individual. Computers linked together by high speed networks with advanced processing systems can create comprehensive dossiers on any person without the need for a single central computer system. New technologies developed by the defense industry are spreading into law enforcement, civilian agencies, and private companies.

It is now common wisdom that the power, capacity and speed of information technology is accelerating rapidly. The extent of privacy invasion -- or certainly the potential to invade privacy -- increases correspondingly.

Beyond these obvious aspects of capacity and cost, there are a number of important trends that contribute to privacy invasion

Fruitful resolution in the given survey

The first and foremost solution to prevent cyber-attacks on companies is to have a secure and sophisticated hardware which are password protected and backed up by 2-way authentication. Also, it is better if you don't overlook the effectiveness of protecting your physical storage disks.

Results

Since it has been neglected, then it gives an opportunity to anyone and everyone to walk away with your firm's sensitive data. It is wise to invest in cybersecurity insurance these days- Because cybercriminals are becoming too sophisticated these days, they are coming up with ways to break into the most advanced cyber defenses. Therefore, even the most security-conscious businesses get vulnerable to cyber-attacks. This is where a cyber-insurance cover can come to your rescue. If in case, an attack occurs, most of the policies not only cover the financial loss caused from data theft but also help in co-paying the costs involved in recovering data and that includes paying to data recovery experts and for buying new hardware as well as software.

Conclusion

The most potential concern should be based on creating a digital environment, standardization, cybersecurity and data sharing in industrial sector. Therefore, the most fruitful password through cybersecurity as well as VPN are being provided in modern century. It needs to be started with the most powerful encryption password through virtual private network.

The list of used literature:

1 http://www.fcc.gov/cyberplanner

2 Constitutional Court Decision No. 15-AB of 13 April 1991.

<http://www.privacy.org/pi/countries/hungary/hungarian_id_decision_1991.html>.

3. U.S. Department of State Singapore Country Report on Human Rights Practices for 1997, January 30, 1998.

4. See Banisar and Davies, The Code War, Index on Censorship, January 1998.

5 Strategies of North Atlantic Treaty Organization at SPIMUN.
6 Office of Technology Assessment, New Technology, New Tensions, September 1987
7 PRIVACY AND HUMAN RIGHTS an International Survey of Privacy Laws and Practice
8 Cybersecurity Insiders