Cyber Security: The Hidden Potential

In general terms Cybersecurity refers to the sets of the measure adopted to provide protection to the integrity of software, hardware, networks, programs and data from the theft, attack, damage or unauthorized access. But with the recent developments, cybersecurity has become one of the major sector that has the major potential to grow. As today most of the organizations fear of becoming victims of the cyber attacks which is of great concern as it affects the ability to deal with clients and safeguarding their data or even the internal user's data more securely. That's one of the main reason why organizations nowadays are spending billions of dollars on their cybersecurity.

Even according to the Forbes, the global cybersecurity market is expected to grow up to $170 billion by 2020. Apart from Forbes, International Data Corporation (IDC) predicts the overall global cyber security market, to grow at a compounded annual growth rate (CAGR) of 8.3% between now and 2020, rising from $73.6 billion in 2018 to $101.6 billion by 2020.

Types of Threats

As the cyber network uses a large variety of devices and software, hence the threats to them are of various types. The major threats which are nowadays quite common are-

1. Application Threat
2. Information Threat
3. Network Threat
4. Disaster Threat

5. Operational Threat

6. End-user Threat

With a world with such a high use, dependence on technology and the rise of the Internet of Things (IoT), the type of threats has also been increasing. For multiple uses, various social networking sites have also set up a counter threats task force in which they are pouring millions to keep up with the different type of threats and neutralize them as they come up.

The need for Cyber Security

The main idea behind Cyber Security involves protecting information and data from cybercrimes. From the past few years, there has been a tremendous increase in the need for the cybersecurity due to:

1. Instances of Attacks: With the growing population of users using the cyber devices, it makes virtually every user a target of such attacks. This is making the need of protecting the victims as well as potential victims a priority.

2. The severity of attacks: The crimes are getting worse and the attacks related to the loss of money is above them all. These attacks are getting bigger sometimes affecting the whole economy at once.

3. Economic Implications: The hacking attack on the entertainment industry, Sony, has seen one of the worst cybersecurity hacks losing millions of dollars. Another such case was Talk Talk, also lost around 50 million pounds which eventually resulted in the drop of 20% in their stock value. Thus, these attacks have put major pressure on the global economy amounting a loss of $400 billion last year.

4. Vulnerability: Our systems have become more vulnerable because of the technological changes that we see everyday. The better the technology, easier it will be for the criminals to exploit it. The increasing use of cloud computing has made the data more vulnerable than ever as it allows them to use the data from a single point for their own good.

5. Future Growth: The future growth of an organization is going to depend on the amount of money the company is investing in its cybersecurity operations. The more the company invests, more consumers it will attract because everybody wants to invest in the organization where their data is safe.

Eventually, if a company has its servers and data secured from any kind of attacks more the people want to connect with your organization which leads to increase in goodwill of the company ultimately leading to profits for the firm.

Countries having the best cybersecurity measures

As per **2017-18** survey done by International Telecommunication Union (ITU), the countries with the highest score for cybersecurity are The USA, Canada, and Japan.

GCI RANKING

Ranking	Country	Index(2015)	Index(2017)	Score
1	USA	0.824	0.919	**8.72**
2	Canada	0.794	0.818	**8.06**
3	Japan	0.706	0.786	**7.46**
4	UK	0.706	0.783	**7.45**
5	South Korea	0.706	0.782	**7.44**
6	France	0.588	0.819	**7.04**
7	India	0.706	0.683	**6.95**
8	Germany	0.706	0.679	**6.93**
9	Israel	0.676	0.691	**6.84**
10	Brazil	0.706	0.593	**6.50**
11	Russia	0.500	0.788	**6.44**
12	Turkey	0.647	0.581	**6.14**
13	Italy	0.559	0.626	**5.93**
14	China	0.441	0.624	**5.33**
15	Iran	0.294	0.494	**3.94**
16	North Korea	0.000	0.000	**0**

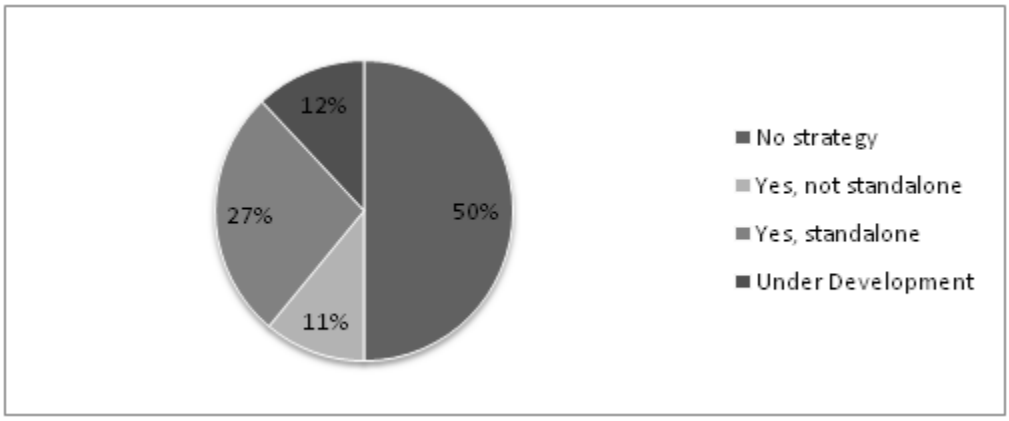
Source:(ITU,2015:1-6;ABI Research,2014,ITU,2017)

This ranking indicates what kind of amendments and studies were done by states on their legislation at cyber security levels, the technical measures were taken, preparedness of institutions and organizations, the conduct-ed standardization studies and certification programs aimed to improve their cyber security capacities, and the result of the coordination and cooperation activities carried out in national and international fields. That is, this ranking is of much importance in the sense of monitoring the national and international levels of awareness of states, as well as the seriousness and care in the studies they needed to conduct.

Opportunities

with Cyber Security Every coin has two sides. Where on one side the cybercrimes are posing a threat to the IT sector, the other side of cybercrimes can be seen as the opportunity for various IT solution companies. If these opportunities are rightly used one can see the hidden potential of the Cybersecurity market. For that one just need a good knowledge of changing technological trends and highly skilled IT professionals. And there are a lot of areas in which work needs to be done like

Cybersecurity strategy: Though governments of different countries are trying to make better policies with the help of the IT companies still many reforms needed in it. The following data gives an overall picture of the strategies that require a lot of efforts it can be clearly seen that the half of the countries don't have a cybersecurity policy.



Source: Global cybersecurity Index 2017

Apart from that, the cybersecurity industry is currently dealing in billions of rupees which is of great opportunities for many IT firms that provide solutions for various cyber threats happening on daily basis.

Scope

With newer technologies breaking through the horizon, challenges for cybersecurity are ever higher. With Blockchain, AI and increasing use of IoT, the complexity of safety for users is evolving. Earlier when the internet started, HTTP was considered as a secure but with cyber attackers cracking their way through the system, and fake websites popping up, HTTPS was invented to take control of the situation and to let the users know the authenticity of the site. Similarly, various other developments have been coming up to be able to keep up with the newer technologies.

The following table shows the Development Rate of the Countries' Software Industry for 2015. It is evident from the following data that the developed country like the USA has the major scope for growth in coming years keeping in mind its technological development and the amount of money spent on the software industry. Apart from that, it is clear that other countries do have a major scope but need to work on the technological aspect including India.

No.	Country	Index (Billion $)	Score
1	USA	160	**10**
2	UK	31	**6.77**
3	Germany	30	**6.7**
4	China	27	**6.49**
5	France	22	**6.09**
6	Japan	17	**5.58**
7	Italy	14	**5.2**
8	Canada	12	**4.2**
9	India	5	**3.17**
10	Brazil, South KoreaSouthKorea	4	**2.73**
11	Israel, Russia	1	**0.19**
12	Iran, North Korea	<1	**0.02**

Source: (Ortner, 2015)

Conclusion

The increasing dependency on the internet gave birth to new security problems, due to the current status of information and communication technology and the internet being an indispensable element in every field of our lives. In a world that changes and develops extremely fast, the countries have the need to closely follow the developments, analyze them and pursue correct strategy and policies for their national security. For this countries have engaged in creating cyber armies to ensure safety. But apart from this something needs to be done at the micro level like Consciousness raising and awareness studies even in schools. Apart from that special training should be given to employees so that they could at least cope up with the threats on a small level. Cybersecurity is one of the major sectors that have the potential for it firms and for the nations as well which if successful in taking advantage of it can become the global powers.