****

**CYBER SECURITY**

In today's world, cyber security is very important due to some security threats and cyber-attacks. For data protection, many companies develop software. This software protects data. Cybersecurity is important because it not only keeps information safe but also helps keep our system safe from virus attacks. After the U.S.A. and China, India has the highest number of internet users, this shows the growth and importance of cyber security in India.

The COVID-19 pandemic changed our world and the way businesses operate dramatically. It has also brought about a diametrical change in the way education is delivered and accessed. Education workers, students, and teachers around the world drastically altered the way they taught, learnt and worked. While this led to a massive increase in access to education for many and a wider student pool, it also created a ripe and wider attack surface for cybercriminals.

**IMPACT**

Cybersecurity attacks on educational institutions are not just an operational or financial issue. They compromise student data and harm the overall integrity and reputation of institutions that have been built painstakingly over the years. Systems are brought down to their knees, information is lost, and anxiety and stress levels of staff and students skyrocket. Universities spend millions trying to recover from cyberattacks, and the recovery itself could take months as they try to first find the compromise before attempting to fix it. Cybersecurity consultancies are often brought in to advise universities on how to defend against these cyberattacks, but with the constant evolution of these attacks, there has been no respite for universities and schools.

**WHAT IS CYBER SECURITY?**

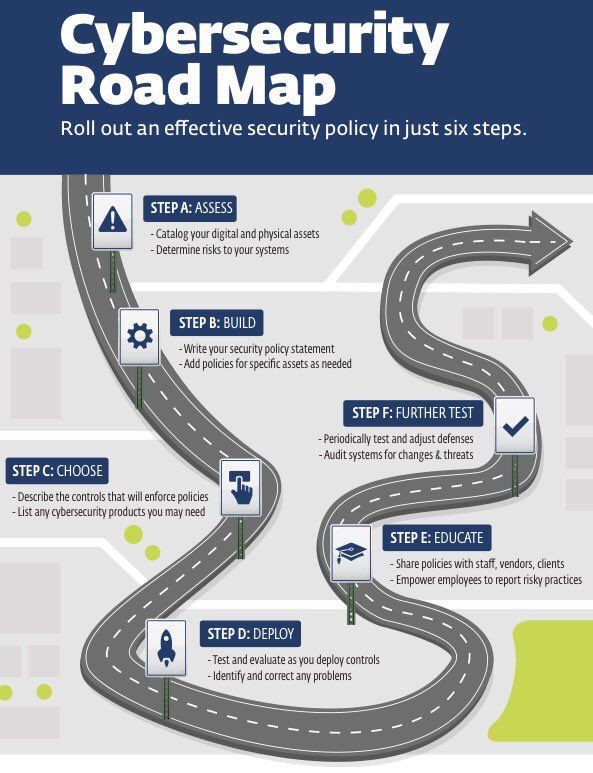
Cybersecurity is an application that protects technologies, processes, and controls from cyberattacks on systems, networks, programs, devices, and data. It aims to reduce the risk of cyber-attacks and protect against unauthorized exploitation of systems, networks and technologies.

**WHO NEEDS CYBER SECURITY?**

This is the wrong question, everyone connected to the internet needs cyber security. This is because most cyber attacks are automated and are aimed at exploiting common vulnerabilities rather than specific websites or organizations.

**SOLUTION**

While there's no denying that the threat of cyber-attacks is imminent and almost every business and institution is likely to get attacked at some point in their existence, here are a few steps people can take to ensure greater protection from cyber threats and more resilience in case of an incident.

* **Cybersecurity training:** All people should be given relevant cyber awareness training. They need to be helped in understanding that they play an important role in organisational cybersecurity and often they, can be the ones preventing a phishing attempt or a ransomware attack from having any significant impact on the organisation.
* **Make sure all systems are updated regularly.** Operating systems, browsers, and applications should always be up-to-date as each update fixes vulnerabilities and protects against new threats. This is a simple good practice that can make a world of difference when it comes to cyber safety of educational institutions entries etc.
* **Be Prepared.**

While creating awareness and instilling the importance of good security habits is imperative, unfortunately, this may not be enough. Your internet activity could still come under attack and it's important to be prepared for that eventuality. Make sure you have a good incident response plan or ransomware



response chain list that your team can refer to in case of an incident. When a crisis hits, it becomes difficult to think straight so visual workflows and pre-vetted response plans can help to cut the chaos and take the right steps.

**STRENGTHENING INDIA'S CYBERINFRASTRUCTURE**

To Protect The Overall Cyberinfrastructure Of India, organizations have online workshops and vulnerability assessments to inform citizens and secure cyber infrastructure. For example, India's Ministry of Electronics and Information Technology developed an information security, awareness website. The website provides over 1,000 workshops tailored to inform government, academic, and general internet users about software security, popular attacks, and computer terminology**.**

1. **Protect cyber hygiene:**

As noted in the India-U.S. Information Security Summit, 2004, governments can encourage cyber hygiene and cyber ethics among their citizens from an early age which allows each state to maintain a uniform and secure cyber structure. Further, bilateral cooperation to protect citizens should not rest solely with U.S. and Indian federal governments. Efforts should be made for subnational governments to share best practices and ideas, too.

**2. U.S-India cyber recovery plan:** The United States President's budget for 2020India’sIndia announced that it would allow mobile carriers to carry out 5G trials. While 5G will offer huge benefits, it has more potential entry points for attackers due to the less centralized nature of its architecture. Therefore, India and the United States should create a U.S-India toolbox on 5G similar to the EU Toolbox on 5G. The toolbox sets out measures to strengthen security requirements for 5G networks, applies relevant restrictions for suppliers considered high-risk, and ensures the diversification of vendors. There is a convergence of threats, so collaboration in securing this emerging infrastructure should have direct benefits for both nations.

There is no such thing as the cult of the defensive, just as there is no such thing cult of the offensive. Offensive and defensive actions are more a function of the nature and scope of the objectives pursued by a belligerent or set of belligerents. The more ambitious a state's objectives, the more offensive the action. Offence and defence must be in some balance.

**SOLUTION**

The responsibility for the protection of cyber information in universities falls on the shoulders of the senior management and board members. However, it's the staff and students who use the institutional systems and networks every day. This creates a bit of a divide when it comes to ensuring complete cyber resilience. In the time of pandemic with the rise in cybercrimes, with the growing rate of internet users, there is a demand for a user-friendly law that protects the internet users and makes the users reliable to use the internet. After going through all the types of cybercrimes and judicial pronouncements one can easily make out that there is poor implementation and deliberate ignorance of the provision for the infringement of the rights of the internet users. If the rights of the user are violated in cyberspace there is no fixed provision that can be applied directly, but a mix of various provisions and laws to bring it under one umbrella. There is a vital need for amendment of the consumer protection act and the information technology Act to bring the infringement of the rights of the internet user under the ambit of cybercrimes.

# **IHA PRAGYAN**

[www.ihapragyan.in](http://www.ihapragyan.in)