Date: 23.4.2018	**Publication:** The Telegraph
Page no: 11	**Edition:** Kolkata

DIGITAL DEFENCE

Mitigating cyber risks by taking adequate caution and cover is the need of the hour, says **Sasikumar Adidamu**

We live in an era of hyper-connectivity. The various devices and applications used in our homes or at workplaces have now become so integrated that it's hard to keep them separate. In a matter of seconds, a user with Internet connection can download, transmit and transact information that can be shared across devices.

However, there is a flip side to this too. Not too long ago the biggest risk was protecting the cash in the wallet or having your pocket picked. Today we live in a perpetual fear that our banking details and data stored online could be stolen, hacked, damaged or erased. The biggest nightmare that an individual can wake up to is to see an unauthorised debit in his bank account and realise that he is a victim of an online fraud. Armed with cyber weapons, it's easy for digital criminals to rob unsuspecting online consumers via spoof SMS, phishing links, fake IDs, forged online identities — their ways are new and many.

Moreover, with the sudden spread of virulent cyber attacks such as WannaCry and Petya, India has emerged as the third most vulnerable country in terms of risks of cyber threats, such as malware, spam and ransomware, according to a report by global security firm Symantec. It is estimated that the WannaCry attack affected around 48,000 systems throughout the country, serving as a major wake-up call for all of us on the increasing danger posed by cyber crimes.

According to a recent report by the Internet and Mobile Association of India, the number of Internet users in India stood at 481 million in December 2017 and is expected to reach 500 million by June 2018.

One result of the increased use of technology is that it has opened up organisations and individual users to advanced cyber risks that they are often poorly prepared to defend against. And now, with the sharing of devices, information and networks, these risks have compounded. A majority of banking transactions today are conducted online. A lot of personal information is also available online and on social media which can be used by hackers.

The result is that cyber criminals are working overtime to develop, hack and deliver new persistent attacks to target vulnerable systems. Therefore, if organisations and individuals want to protect their networks and data from the onslaught of attacks, it is essential that they begin to have proper security strategies in place.

So, as employers and individuals navigate the rapidly evolving cyber risk landscape, here are some basic guidelines to keep in mind.

Deploy security tools

When connecting to or storing sensitive data in personal devices or applications or on your network, it is important that you have security tools in place to detect and deter malware and cyber criminals. For home networks, this often means using a firewall and encryption.

Maintain an active and strong antivirus in the computer system to detect any irregularity. A firewall ensures that malicious traffic from compromised devices, applications or websites that try to enter your network are detected and stopped.

Connecting to public Wi-Fi is another common consumer practice that poses substantial risk to a device and network security.

Browse carefully

Cyber criminals often try to scam their way into networks through phishing attacks or malicious emails posing as legitimate communications. Restrain from clicking on any link from unknown sources or advertisement or from an unknown pop-up window and downloading any item from an unknown website.

Avoid registering your email IDs with unknown sources. Emails from unauthenticated sources should not be attended and clicked on. Always look out for https:// to authenticate if the website is genuine or not.

Strong passwords

Use a strong password, preferably with alpha-numeric combination and special characters on every platform. Reusing passwords across multiple accounts makes you susceptible to account takeover. This is because if your password becomes compromised on one site, it is compromised on others that use the same password. Do not disclose the password to any other person.

Cyber insurance cover

Despite the best preventive measures, hackers today have become sophisticated. So, having a cyber insurance cover is a must. A comprehensive cyber insurance plan provides protection against various risks such as identity theft, malware attack, IT theft loss, cyber extortion, cyber stalking. It will cover financial loss resulting from being an innocent victim of email spoofing and phishing.

Losses and expenses related to defence, prosecution costs related to identity theft and restoration cost to retrieving or reinstalling data or computer program damaged by the entry of a malware are also covered. It provides cover for expenses incurred on counselling services treatment, claim for damages against third party for privacy and data breach and transportation for attending court summons.

As we move into the new digital economy where data and connectivity are highly valuable resources, ensuring cyber security by conscientiously following security guidelines is imperative. Additionally, a comprehensive insurance plan will help mitigate the growing risk of cyber compromise.It ensures that you are financially well protected against any cyber attack and can browse, surf and transact on the internet without any undue stress.

The writer is chief technical officer, Bajaj Allianz General Insurance