The ongoing pandemic has affected all the aspects of our lives, from the way we live to the way we work. COVID-19 has had a significant impact on the cybersecurity space as well, as is illustrated through the statistics below:

Since February, IBM X-Force has observed a 4,300 percent increase in COVID-19-themed spam
IBM’s Research insights titled ‘COVID-19 cyberwar: How to protect your businesses'

Between 2 February and 2 May 2020, India witnessed 9,100 COVID-19-themed cyberattacks
Quote by Ann Johnson - Microsoft Corp Corporate Vice President (Cybersecurity Solutions Group)

Between March and April 2020, cyberattacks soared by 86 percent
Reuters report

The sudden increase in cybersecurity threat vectors can be attributed to the following reasons:

**Increased security risk from remote working**
The COVID-19 crisis has forced organisations to switch to remote working without adequate planning and security considerations. This is making them more vulnerable to cyberattacks than before.

**Failure/potential delays in detecting and responding to cyberattacks**
Currently, organisations are working with limited staff and have remote access to systems, which has led to delays, and in some cases, failure to detect potential attacks and take corrective actions.

**Exposed physical security**
Physical security of information assets has also been exposed due to insecure teleworking practices and distributed residence of data in uncontrolled environments.

**Influx of cyber criminals**
The ease of cyberattacks, coupled with the panic caused by the pandemic, has enticed more cyber criminals to attempt cyberattacks.

**Failure of Business Continuity Plans (BCP) to feature pandemics**
The unexpectedness of the pandemic revealed that most organisations had disregarded pandemic-related safeguards in their BCP. This led to a lack of preparedness for addressing the COVID-19 pandemic.
Unlocking the value of Cyber Insurance

How can organisations increase vigilance and resilience to combat cybersecurity threats?

Organisations can combat the elevated risks of cyberattacks and data breaches if they:

- Create cybersecurity awareness amongst their employees,
- Monitor and manage availability of business applications,
- Enhance security monitoring of business applications and systems, and
- Revisit BCPs.

Cyber Insurance: Imperative for a secure future

Although the above practices can make organisations vigilant and resilient to cyberattacks and data breaches, the sheer urgency to protect the organisation makes cyber insurance the need of the hour and a critical risk management tool.

According to IBM's Cost of a Data Breach Report-2019,

As per the global average, a typical data breach has a financial impact of **US$ 3.92 million**

In India, the average data breach costs over **INR 13.7 crores**

The high financial impact, increased probability of risk materialisation, and existing disruptions in business test an organisation's risk appetite. Cyber insurance helps to cover and mitigate the financial risk of a cyberattack and data breach.

Cyber insurance, unlike general insurance, cannot be picked off-the-shelf. Organisations must carry out an in-depth risk exposure evaluation and identify a tailor-made insurance policy per their organisation's requirements. It is pivotal that organisations select a cyber insurance policy that resonates with their threat exposure.

As the pandemic continues, risk professionals need to work with their insurance advisors to carefully review their requirements and select an insurance policy best suited for their organisations.
Selecting the right cyber insurance policy

It should ideally provide coverage against network security liability, privacy liability, security response and forensic costs, data recovery and restoration, ransom event costs, reputational harm, network business interruption and associated expense, system failure, contingent business interruption, and privacy regulatory defense. In addition, organisations may also consider the following aspects:

- Liability arising out of personal and corporate data breach due to increased probability of data breaches
- Regulatory fines and penalties arising out of data breaches
- Defense cost for litigations and in connection with proceedings brought about by regulators due to data breach
- Cost of computer forensic investigation for root-cause identification of COVID-themed cyberattacks
- Cost of civil litigations and criminal investigation for cyber frauds and attacks
- Crisis management and customer notification expenses

It is imperative that an organisation reviews its cyber risk management programme and actively considers an appropriate cyber insurance policy to address the elevated risks owing to the pandemic.

To gain an in-depth understanding on cyber insurance, click here to read our detailed report on Unlocking the Value of Cyber Insurance.