There is a tremendous change in the world since COVID-19 hit us. Our way of life has changed extremely and everything is affected. Cybersecurity also got a major hit by this virus as it unleashed the doors for cybercriminals. Mostly, everything is shifted online due to the pandemic. Thus, hackers took this opportunity to exploit the online users.

With the increase in cyber-attacks, it has become more complex to keep systems [secure](http://www.cardzgroup.com). Furthermore, the attacks are more sophisticated than before which makes it difficult to tackle them.

**Recent Incidents**

Recently, around 800K businesses and 24 million people were affected by the [Experian Breach](https://www.infosecurity-magazine.com/news/experian-data-breach-24-million/). All these people and businesses reported that their data was stolen. Another recent attack was a ransomware attack on [Cognizant Technology Solutions](https://www.bleepingcomputer.com/news/security/it-giant-cognizant-confirms-data-breach-after-ransomware-attack/#:~:text=In%20a%20series%20of%20data,over%20%2415%20billion%20in%20revenue.). They had to pay 70 million to the attackers to get back their services.

One of the most popular online meeting applications, Zoom, also got a big blow from a cyber-attack. Online meeting applications are an essential app these days. In such times, attackers got access to private meetings. Thus, they could leak chats, conversations, and other essential information. Not only this, the attackers used this opportunity to destroy the reputation of Zoom by sharing inappropriate videos.

These are only a few of the major security perishing incidents since COVID-19.

**Changing Nature of Attacks**

The biggest problem of cyber-attacks during the pandemic is their changing nature. Almost 35% of the attacks nowadays are unseen and cannot be understood by IT professionals. Thus, no secure system is in place for these unseen attacks.

A simple example of a new nature of attack can be the phishing attack with voice mail. Furthermore, there is a misuse of the news of vaccines which makes people click a link. Ransomware attacks are also top-a-notch as hackers combine it with data leakage.

**Impact on Businesses**

The modes of communication online are a source of relief for many of us. However, the shift of businesses to online communication made them vulnerable at the hands of cybercriminals. Most of the companies were not prepared for such a mass shift online. A data breach is the most common type of insecurity that organizations deal with during COVID-19. The risk management and IT teams feel relevant pressure to keep their systems secure. Businesses always need a real-time risk analysis to cope with the complex attacks taking over the digital world.

Agile teams play an important role in such critical situations when you are always under the threat of an attack. Furthermore, it is also essential for businesses to maintain synchronization in their employees especially those who work in the agile team.

Businesses that used online platforms even before the outbreak of the global pandemic face less trouble than those who are new to the Internet. Companies that don't have access to Internet services and cannot control their applications remotely online face trouble. Thus, businesses now realize that remote access capacity is a major constraint for them when working online.

**The Cybersecurity Response**

Cybersecurity professionals actively deal with the problem of increasing attacks. It has become essential for them to respond aggressively and promptly to ensure a secure online environment. The basic step by Cybersecurity professionals was to make the company’s remote workforce aware of the scams. Then security efforts of deploying technologies and solutions were made, in which companies can adapt quickly such as cloud hosting services. Professionals also put significant emphasis on dynamic scalability. PAM services, cloud services, and remote private access are some of the solutions to cyber-attacks.

**Conclusion**

Cybersecurity was always important for us. However, now that the world is changing and facing extreme levels of cyber threats, there is a need for immediate action. With the second wave of COVID-19 and the third wave ready to approach, people should take a pro-active decision to secure their systems.