The COVID-19 pandemic created new challenges for organizations as they had to quickly adapt to an operating model, as working from home became the “new normal”. Businesses accelerated their digital transformation, and likewise, cybersecurity also posed new threats. Considering new challenges of remote working, businesses had to analyze the operational, reputational, compliance, and legal implications. Now, even with the pandemic marking its second anniversary soon, remote working has become a norm in many businesses. As a consequence of the pandemic, technology has gained more importance in our personal as well as work lives. However, even after adapting the new work model, many organizations fail to provide a completely cyber-safe work-from-home environment.

## The Need for Increased Cyber Security

The cyber threat landscape is now more diverse than ever. Let’s see how.

* Malicious staff that is working from home with lesser supervision is easily tempted to carry out criminal activity or conduct a fraud.
* Employees who are not very vigilant are easily exposed to threats because of careless attitude and lack of reminders, which are otherwise a routine in office premises.
* Cybercriminals are aware of the increased opportunities and weak links, which makes businesses more susceptible to attacks.
* Bring Your Own Device (BYOD) policies where employees can use their personal laptops and mobile devices is putting business information more at risk. Work-from-home cannot guarantee same level of cybersecurity as an office. For instance, an employee may not regularly update anti-malware or run regular scans on their personal device, which makes their data vulnerable.
* Digital ecommerce applications such as food delivery, online banking, grocery or medicines need to protect customer data while keeping their [transactions](http://www.cardzgroup.com/ScratchCard.html) secure.

## The Evolving Nature of Cyber Threats

Hackers have now developed new ways to infiltrate and attack systems to capitalize on the remote working situation. Before the pandemic, very few cyberattacks were launched with methods or malware unknown to the people. This percentage increased during the pandemic. Some of these new methods included the use of machine learning, where malware adapts to the environment to stay undetected. Phishing attacks have also become more sophisticated and targeted by studying user search patterns.

With cyber attacks becoming more sophisticated, there is a need to develop sophisticated technology to timely detect them. User and Entity Behavior Analysis (UEBA) is one such technology that analyzes routine user behavior and uses it to detect any deviation from the normal pattern.

## How can businesses cope with the changing threat landscape?

Before COVID-19, many businesses such as banks did not allow remote working, particularly because of risks involved in protecting confidential data. The pandemic brought many challenges for them as they had to adjust to the new setup in very short time period. Organizations had to quickly increase their capability and capacity for remote working. However, cybersecurity was not a key priority in quick deployment of work-from-home capabilities.

For instance, many companies did not check that the employee personal devices were secured before they tried to gain access to corporate data. However, as the world gradually adjusted to the new work model, many organizations have now devised methods to ensure that their confidential information stays secure even as employees regularly work remotely.

Let’s have a look at how some of these measures can be implemented.

* All employees must be provided with licensed antivirus or antimalware software to use on their personal devices.
* All staff should be regularly informed about best security practices and procedures and given monthly reminders through email about how they can stay vigilant and protect themselves from phishing attempts.
* All employees should protect their home networks with strong passwords.
* Using a Virtual Private Network (VPN) when working from home can add an extra protection layer to keep corporate data secure.
* Organizations should also ensure regular security practices such as scanning their networks for vulnerabilities and patching them on time.
* They should regularly review their risk exposure to evaluate the existing security controls. All forms of new cyber attacks should be taken into consideration during the reviews.
* The IT department should make use of advanced tools like host checking, which checks for an endpoint’s security posture before it can authorize a user to access a corporate information system.
* In this time of high risks, organizations should also carry out threat simulation exercises frequently to proactively prepare for a response to a potential attack.

## Conclusion

Cybersecurity needs to be given extra attention, particularly during the pandemic. Organizations need to be more focused on proactively addressing threats, planning ways to prevent cyberattacks from being successful instead of responding to them once they have already occurred. However, as much important as preventive measures are, businesses must also be prepared to detect, respond to and recover in case of an actual attack.

Companies need to plan and reduce the likelihood of a strong impact of an attack. For this, they must devise resilient working practices and enhance their application and development of security practices.