As the COVID-19 outbreak started two years ago, it gave rise to a new wave of opportunities to cybercriminals, who were now motivated by easier threat landscape resulting from remote workplace transition. Not only were cyber attacks increased in number, their speed and severity also amplified.

For businesses to create a reliable defense against such cyberattacks in the wake of unanticipated global pandemic, it has been a challenging time to avoid data breaches. More than ever before, there was now a need for businesses to practice extreme vigilance, implement robust security frameworks, and offer ongoing security trainings. There were multiple potential attack vectors at risk, and most of them were related to at-home networks. Subsequently, Internet of Things (IoT) devices were also at the center of these targeted cyberattacks.

## Remote Work and IoT Security during COVID 19

There has been enough time now since the onset of pandemic for organizations to work out initial security issues arising from transitioning to remote work setup. However, for many organizations, there was one problem that continued to have repercussions for a long time.

With a shortage of company-owned devices and laptops, many employees were forced to use their personal devices for accessing corporate networks to complete their official tasks. At the same time, these employees casually engaged in routine online behavior like online shopping, using social media, and streaming entertainment channels. With most of these devices lacking desktop security and endpoint protection, they were far more vulnerable to cyberattacks and malware than official devices.

From the perspective of IoT, this oversight is particularly damaging as hackers could achieve their target without even directly accessing the devices and bypassing any weak [security technology](http://www.cardzgroup.com/ScratchCard.html). Malware is easily spread via tablets, routers, and gaming systems that are interconnected to home network, as well as IoT devices like smart cameras and doorbells. Attackers could take advantage of this situation and gained easy access to systems that were not intended to be accessed by public.

Whereas this alone can impact a network significantly, it is only the first step a cyber criminal would take in attempting to exploit an organization. They were well aware that by exploiting one vulnerable device that no one expects to be exploited, they could easily gain access to an entire corporate network and all of its digital resources.

## COVID 19 and IoT Security

## Even as organizations adopted to the new normal of remote working, or even if now employees are back to the same office work routine, there are still threats out there. Though adoption of IoT technology has helped businesses in many ways, cyber attackers are very well versed with its vulnerabilities. Some of common attacks on IoT devices resulting from the pandemic included:

## COVID 19 related phishing scams: Hackers used the pandemic time as an opportunity to send malicious phishing emails, luring receivers to open them and follow certain steps to know more about the disease. They used well-drafted emails such as those including reports from news outlets and health organizations. As a result of rise in cyber attacks resulting from phishing scams, the World Health Organization (WHO) released a [statement](https://www.who.int/about/communications/cyber-security) and issued advisory warning to people to be wary of any such phishing scams.

## Attacks on Medical Devices: There were also incidents where cybercriminals were sending emails to medical device suppliers and ordering multiple COVID-related medical devices from them. The emails had a malicious MS word attachment which when opened, would import all files from the user’s computer.

## Rise in IoT adoption in a Post Covid World

## As generally perceived, IoT devices are more vulnerable to cyber attacks. However, the adoption of this technology is still continuing to gradually rise. Besides medical and healthcare industries investing in IoT, contactless and touchless devices have also attracted the attention of businesses in different industries such as retail and hospitality. Some examples include touchless Point of Sale (PoS) devices, contactless building access, and body temperature cameras.

## Moving Ahead with IoT

## As COVID 19 pandemic is still prevalent all over the world, though at much lower numbers, but even after it eventually reaches an expiry date, cybersecurity experts would still need to carry out due diligence and avoid serious losses at the hands of cyber attackers. In such circumstances, we need to take extra precautions – which include not only the IT and security personnel but all the employees of the organization. It is important that organizations create user awareness and training to educate employees about good and mandatory cyber practices.

## Furthermore, it is also time for businesses to revise their investments in security technology. There should be access control systems and secure email gateways to provide the required level of protection for the ever-evolving threat landscape. Organizations also need to consider proximity controls like Intrusion Prevention Systems (IPS), to add additional defense layers for IoT devices that otherwise cannot be secured.

## As IoT technology adoption has increased, IT teams also need to focus on integrated security frameworks for IoT devices, such as secure SD-WAN for remote employees. As long as companies remain agile and adapt accordingly, they can sustain the fight against unanticipated circumstances and be ready to face threats posed by opportunists in the future.