



Effective Cyber Security Bolsters Business Growth

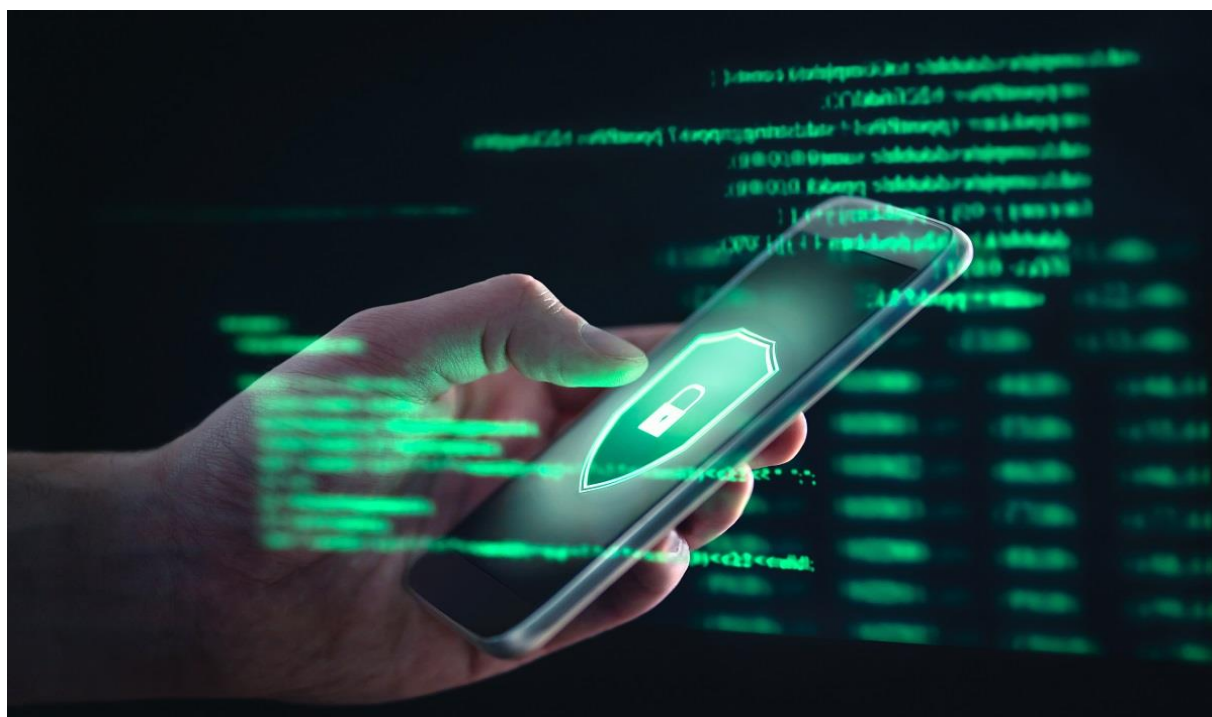
Looking back a few years, cyber security would be viewed as a necessary overhead to protect data. Fast forward a few years and the cyber security industry has grown exponentially and going stronger with time. The critical question here is, can cyber security accelerate your business? If so, how?

To get to the answers of the above, first and foremost we must get some clarity on the basics.

What is Cyber Security?

Cyber security elastic binds the technologies, processes and practices that have been put in place to provide protection from cyber-attacks that are designed to inflict damage to a network system or access data without authorisation.

Why elastic? Because the cyber security measures keep updating themselves to be armed against novel structures of cyber attack mechanisms. Ideally, the solution is a dense concoction of a firewall, anti-virus, anti-spam, wireless security and online content filtration. But you never know when an additional layer of protection becomes an absolute necessity. This is because the threats, classified as ad wares, spy wares, ransom ware etc keep evolving and gaining on their invasion-potential as is evident with the nature of attacks and the extent of damage caused.



Recent Security Breaches of the Year Gone By

In early December 2020, a cyber security company came under attacks from what they believed were state-sponsored sources. They revealed that they were attacked by a “nation with top-tier offensive capabilities” and that their protection tools were compromised.

In early 2020, an international hotel chain in the US came under threat as personal information of 5.2 million guests were accessed. In this attack, accounts of major public figures including then-US presidential candidate Joe Biden, Barack Obama, Elon Musk, Bill Gates, Jeff Bezos, Apple and Uber were simultaneously hacked by attackers to spread a cryptocurrency scam. The breach originated in a franchise hotel that operated under the reputed international brand.

British low-cost airline group revealed that they were targeted by extremely sophisticated cyber attack forces and about nine million passenger data were compromised.

Indian healthcare sector experienced the biggest ever ransom ware attack on one of their premier laboratories in 2020.

One of the top software companies had their networks paralysed for weeks when they came under a ransom ware attack.

The instances above section establish the need to strengthen the security protocols against threats from external agencies who hawk on minutest of weaknesses.

Effective Cyber Security

While cyber security companies gear up to combat cyber crime, vulnerabilities keep popping up. It must be understood that risk elimination is never hundred percent and that cyber security teams pull forces to minimise the risks. It is of great importance for the enterprises to employ the provider who fully comprehends the working of the company through its entire life cycle.



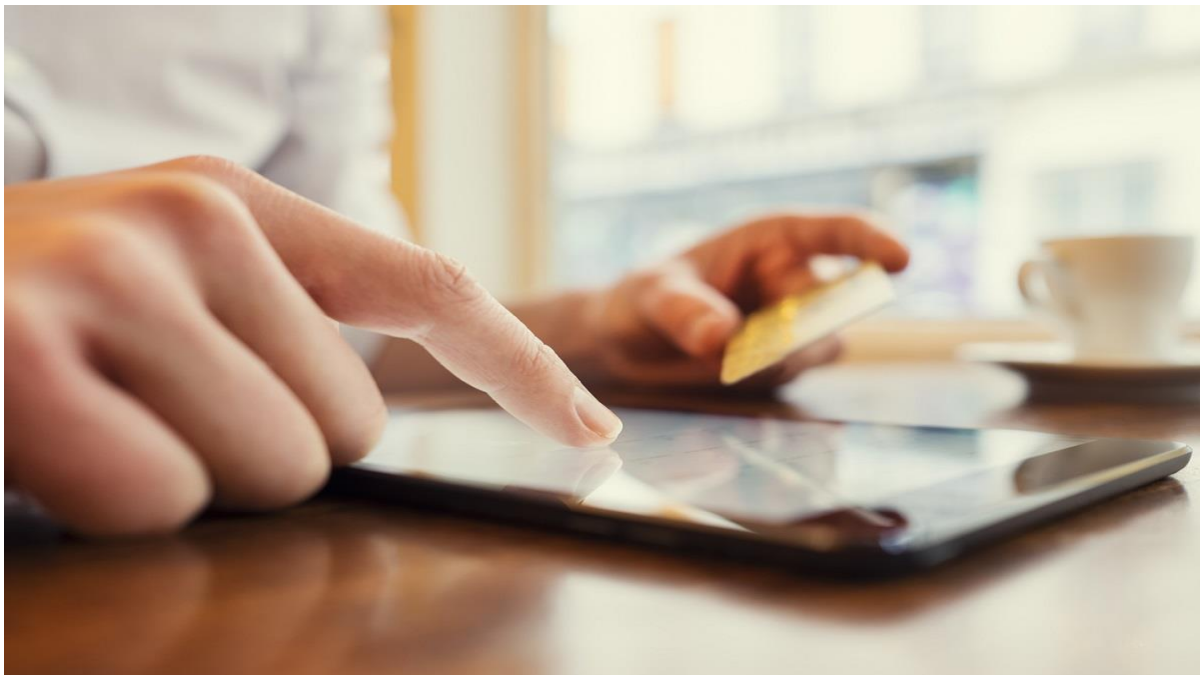
Expansion of business ventures progressively leads to vulnerabilities. Cyber miscreants take advantage of such loop holes to launch highly coordinated assaults, invading the secure channels to access sensitive information. It is advisable to sort out your standing with regard to cyber preparedness and recognise your prompt needs to move from your current state to the ideal state.

Progressively developing threat actors prowling across the web and frequently uncovered vulnerabilities, force the companies to strengthen their security and protect their assets. It is advisable to stay agile and agile while adding resources into cyber security developments; this will ensure that your business is equipped to adjust to the risk scenario.

But, How does It Help Businesses Grow?

It is remarkable that even after these shocking cyber attacks, business ventures have not held back from floating online. Cyber security industry emerges more strengthened than before post recovery from each attack. The companies now offer protection on many levels outside your data reserves.

In the world of digitization, it is more important than ever to protect your critical assets. Issuing strong identities to users and non-person entities while protecting your data at rest and in transit are critical to a strong cyber security posture. Whether it is in-house or cloud based, utilizing a public key infrastructure (PKI) with sound policies and practices will help institutions accomplish this.



Yet another way in which cyber security accelerates businesses is by 'enabling and empowering'. Cyber security is by no means limited to PC security. With people working on the go, geographically expanding the workforce essential for innovation and growth. Having a robust cyber security behind you empowers you to innovate and grow without a care about the cyber threats. You know they're taken care of.

More and more companies are migrating to clouds for support of enterprise and mobile workers. As opposed to on-premises solutions, hosted cloud environments offer

significant advantage for employee collaboration and data access from any location. This, however, leaves companies vulnerable with their data as cloud environments are overwrought with cyber security challenges. To justly exploit the cloud resources companies need to employ expert internal or external resources to correctly plan, design, architect, and implement strong cloud computing environments and supporting policies.

Keeping up with ever changing rules and regulations imposed by the Government and data privacy regulations is tough. This responsibility of streamlining the compliance landscape is left to the cyber security teams while the businesses can focus on expansion and innovation.

This is to say when security concerns are handled by trusted experts companies can channel their focus entirely to rise further levels i.e to accelerate growth.

Finally

To mitigate the risks it is wise to regularly exercise your cyber resilience. It is no longer the question when the attack will be launched but will the system be able to combat the assault? If not how soon can the company recover and restore normalcy in operations.

To conclude, security and cyber security cannot be left afterthoughts. Cyber security is a critical strategic priority to digital businesses. Also in order to fully churn out your digital potential regarding any goal it is only normal to ask for complete reliance with respect to cyber security in order to fully engage in advancement of the project.