The Future of Cybersecurity

Technology runs significant portions of our daily lives.

We're often using it without thinking about it – phones, audio devices, servers, and networks. It follows that the future of cybersecurity isn't just about protecting our laptops from cybercriminals, but about protecting our data and information, wherever it is.

Current trends in cybersecurity have important implications for the future, so let's take a look at some of them and what we can expect going forwards:

Hyperconnection

In an increasingly hyperconnected world run by our smart devices and smart homes, we have to consider the vulnerabilities in the Internet of Things (IoT). While our badly secured gadgets – like smart bulbs and hubs – don't themselves store sensitive information, they are connected to devices that do.

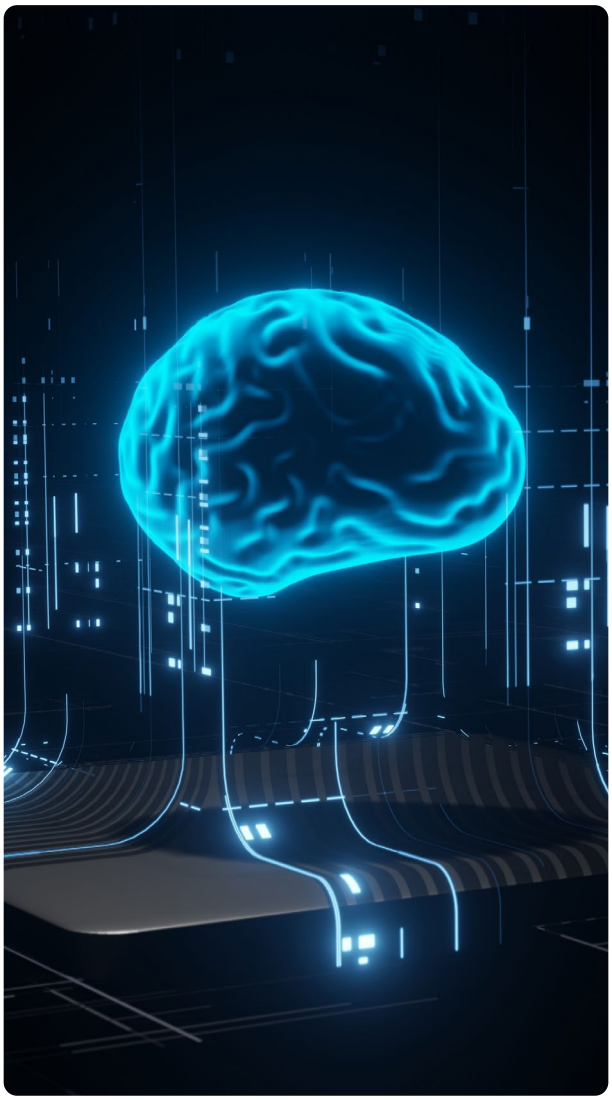
In the future, these will serve as access points for cybercriminals.

Variety of threats

Cyber threats increase in number every day, and they get more inventive, too.

So long as technology changes, so too does how cyber criminality functions. Alongside newer methods, phishing still stands strong, and many people don't have the training to know how to deal with it.

Likewise, the tools that detect and prevent these threats are improving and will continue to do so. One of those tools comes in the form of AI.



Artificial Intelligence

Unless you've been living under a rock, you'll know that Artificial Intelligence has been on the rise (significantly) for the last few years.

It has been used to identify threats, but conversely, it can be used by cybercriminals to find vulnerabilities.

While AI will continue to be used as part of a cybersecurity strategy, people won't be phased out and human minds will continue to be on either side of the security battle.

Attacks at scale

Cybercrime doesn't just happen from a single cybercriminal's bedroom nowadays, but is organised at scale, with gangs of criminals launching coordinated attacks. Data harvesting and resale can yield huge profits for cybercriminals.

We're also seeing an increase in governmental cybercrime – cyber attacks coming from within governments, used for political gain.

Policy and law

In recent years, we've witnessed some deregulation of cybersecurity laws. Since the UK left the EU, for example, it has also left European cybersecurity bodies.

In the future, we could see stricter data protection and cybersecurity laws come into play.

Passwords are being slowly phased out and swapped in for facial recognition and other biometric identifiers. But could this be a slippery slope away from privacy?

Policymakers will need to strike a balance between cybersecurity and privacy.

Cloud and remote access

The digital transformation forced by the pandemic saw a huge shift towards cloud usage. While the cloud offers an excellent means for safeguarding data, it's not entirely safe without significant protection measures.

With the sudden shift to remote working at the start of the pandemic, many businesses struggled to keep up with the cybersecurity implications. The problem lies in isolated workers being connected to the corporate network with no guarantee regarding the security of their devices.

In the future, even more vigilance with cloud security is needed, from threat-prevention cloud tools to an adoption of a 'zero trust' security policy.

Education

Cybersecurity professionals are in high demand, with roles like Cyber Security Manager and Chief Information Security Officer on the rise – but many businesses are finding that filling those cybersecurity roles is a challenge.

There's a shortage of talent, and part of the solution lies in education. Cyber education is vital, both in the form of training for workers and in higher education to promote cybersecurity careers.

We're also set to see a necessary increase in diversity in the sector, opening up the pool of candidates and pushing cybersecurity forwards.

The changing future

Technology changes day by day, and so too will cybersecurity. It's difficult to predict where this train is going, but we can certainly see some possibilities.

Ultimately, cybersecurity strategies will continue to get deeper and more complex, with multiple technologies (and people) working together to mitigate the increasing risks.

If you're interested in finding out more about the private cloud, do check out how we help small and medium-sized businesses keep their data secure with our private cloud services.

vinters