fasthosts ProActive

Future IT risks

on the horizon

The tech world is a fast-paced environment, constantly evolving with new innovations and challenges. As IT professionals, it's our responsibility to stay ahead of the curve and anticipate the risks that may lie ahead. We know that cybersecurity threats are here to stay, and while it's our job as professionals to be the company's eyes and ears when it comes to risks on the horizon, it's good to be aware of potential problems that could arise.

Let's take a look at the future risks that IT professionals should understand and what businesses should keep in mind.

What to watch out for

Cybersecurity threats, AI and automation

The recent rise of AI-powered attacks, and the beginning of quantum computing could make current encryption methods obsolete. This may then expose sensitive data and make businesses vulnerable.

Data privacy and regulatory compliance challenges

As technology moves forward, so do data privacy concerns. Evolving data protection laws, such as the GDPR and CCPA, demand stricter compliance measures from businesses.

Disruption and downtime risks

Service outages, cyberattacks, or even supply chain disruptions can halt operations, leading to financial losses and reputational damage.

Impact on businesses and industries

The effects of IT risks range from minor tech concerns to major financial problems for businesses. Costs from issues with data breaches, including forensic investigations, legal fees, and regulatory fines, can take a significant toll on companies' bottom lines. In industries where compliance is important, non-compliance with regulations may result in hefty penalties.

A breach in cybersecurity or a failure to uphold data privacy standards can also affect a company's reputation. Service interruptions resulting from cyberattacks, system failures, or supply chain disruptions impact day-to-day operations, disrupt supply chains, and can result in a lack of trust from customers.

Protecting yourself as a business

So, what can businesses do to protect themselves? The key is to stay vigilant. This means regularly assessing your IT infrastructure for vulnerabilities, implementing robust security measures, and staying informed about the latest threats and trends in the tech industry.

But it's not just about defence – it's also about resilience. In today's fast-paced digital world, it's not a matter of if a cyberattack will occur, but when. That's why businesses need to have robust backup and disaster recovery plans in place to make sure they can quickly recover from any potential breaches or incidents.

IT professionals – ProActively addressing issues

Ultimately, the future of IT risks is uncertain, but one thing is clear – businesses need to be proactive in addressing them. So, the job of IT infrastructure professionals is to stay informed, implement security measures, and foster a culture of cybersecurity awareness, whoever they're working with.

In a recent episode of our podcast series, "Spill the IT," we sat down to discuss the future of IT risks and how businesses can prepare for them.

If you have any questions, or need any advice, please get in touch. You can give us a call on 0333 111 2000 or book a meeting at a time that works for you.