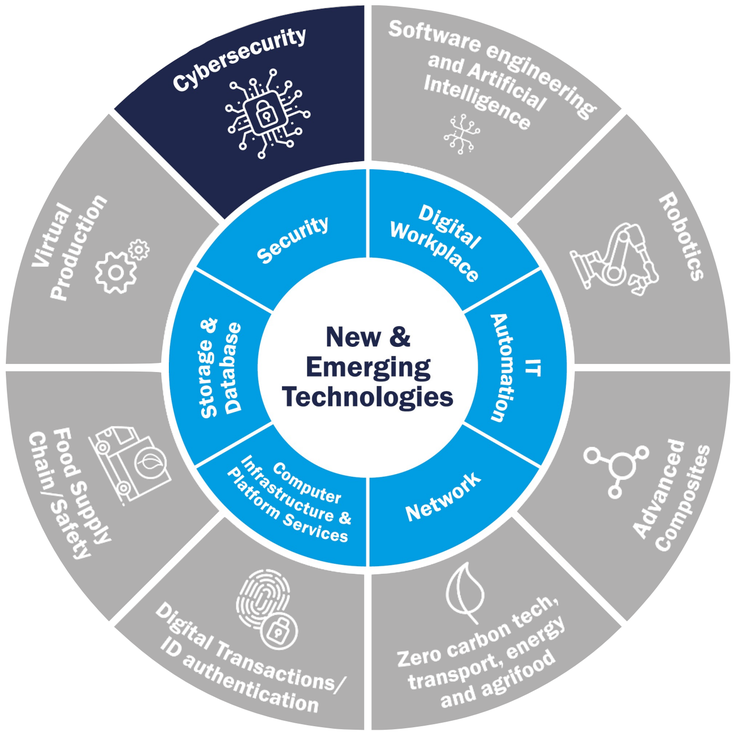


Sources	Microsoft	Date	November 2020

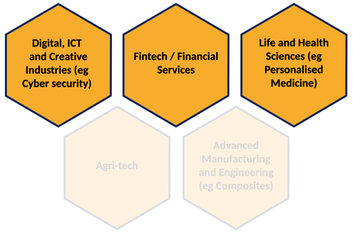
Potential scale of impact	Certainty of outcome	Impact horizon
★★★★	★★★★	H1 H2 **H3**

One in three UK workers are currently based exclusively at home. It's the same in the US and it's creating a major headache for IT security teams. One in five UK home workers has received no training on cyber-security, according to a November 2020 survey by Microsoft. The survey also found that two out of three employees who printed potentially sensitive work documents at home admitted to putting the papers in their bins without shredding them first. A separate UK study from April 2020 found that 57% of IT decision makers believe that remote workers will expose their firm to the risk of a data breach.

Companies need to ensure that

- All staff are using a dedicated and correctly configured work laptop. Personal laptops - particularly those shared by other family members who may be gaming or downloading from file sharing websites - must be regarded as insecure
- Remote computers have secure and encrypted connections through a VPN or virtual private network, not a personal one that may be infected with malware
- Staff are fully aware of - and do not act on - "phishing" emails designed to trick someone into handing over sensitive data or downloading malware
- All staff receive proper cyber-security training
- They have policies in place so that staff know who to report a threat to and that they are not afraid of repercussions - which might lead them to cover up mistakes

Cyber security expert Tim Sadler, CEO, Tessian, notes: "Time and time again we see how simple incidents of human error can compromise data security and damage reputation. The thing is that mistakes are always going to happen. So, as organisations give their staff more data to handle and make employees responsible for the safety of more sensitive information, they must find ways to better secure their people. Education on safe data practices is a good first step, but business leaders should consider how technology can provide another layer of protection and help people to make smarter security decisions, in order to stop mistakes turning into breaches."



REMOTELY THREATENED

57% of IT decision makers believe remote workers expose their firm to the risk of data breach

Home Page
www.10xhorizonscan.online