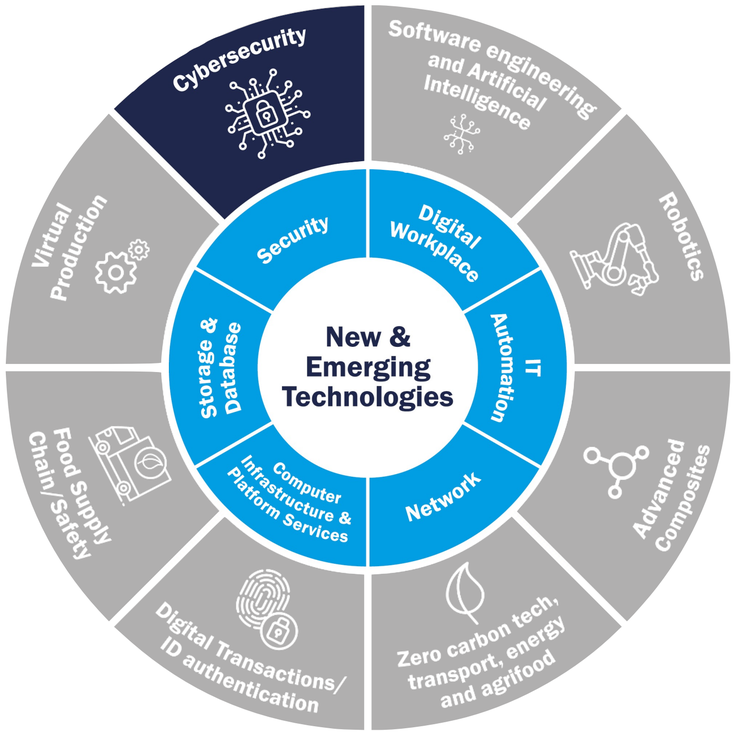


Sources	ZD Net	Date	January 2021

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

Cloud security firm Trend Micro has carried out new research which reveals that over two-fifths (41%) of cybersecurity professionals believe that AI will replace their role by 2030.

Its predictions report, Turning the Tide, forecasts that remote and cloud-based systems will be ruthlessly targeted in 2021. The research was compiled from interviews with 500 IT directors and managers, CIOs and CTOs and does not look good for their career prospects.

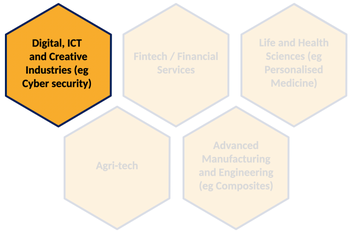
Only 9% of respondents were confident that AI would definitely not replace their job within the next decade. In fact, nearly a third (32%) said they thought the technology would eventually work to completely automate all cybersecurity, with little need for human intervention. Around a quarter (24%) of IT leaders polled also claimed that by 2030, data access will be tied to biometric or DNA data, making unauthorised access impossible.

In the shorter term, respondents also believe Nationwide 5G will have entirely transformed network and security infrastructure (21%), and security will be self-managing and automated using AI (15%).

However, attackers using AI to enhance their arsenal will be commonplace say 1 in 5 respondents. Bharat Mistry, Technical Director, Trend Micro. "We need to be realistic about the future. While AI is a useful tool in helping us to defend against threats, its value can only be harnessed in combination with human expertise."

So how can businesses mitigate the current threats? Although tech bosses believe automation will do away with many roles within a decade, they should not spend time worrying about jobs becoming obsolete for a while - and must act sooner to ensure security is strong. Trend Micro recommends that companies double down on best practice security and patch management programs and augment threat detection with round-the-clock security expertise to protect cloud workloads, emails, endpoints, networks, and servers.

It also recommends user education and training to extend corporate security best practices to the home, including advice against the use of personal devices whilst maintaining strict access controls for both corporate networks and the home office, including zero trust.



AI TO REPLACE HUMANS

Little need for human intervention to make the future cybersecure

Home Page
www.10xhorizonscan.online