This year’s focus for National Cyber Security Awareness Month goes beyond the technology and looks at the role played by the workforce in protecting an organisation.

“Do your part. #BeCyberSmart”.

Surveying IT & Security decision makers across France, Germany & UK we found that employee behaviour can make or break network security. For 35%, insider threat has increased this year due to employee disengagement.

For 36%, one of the biggest future challenges will be employee security education. For 37%, said insider threat is the number one risk in the Zero Trust journey.

49% are considering Zero Trust in order to prevent workers from compromising the system.

While improving security posture is front of mind for IT and Security leaders, they know getting the workforce on board is a must before kick-starting any cyber initiatives.

For 40%, the biggest obstacle to Zero Trust is the need for a culture shift. For 28%, said employee support is fundamental to embark on a Zero Trust journey.

65% of non-adopters stated they didn’t have the right company mindset for Zero Trust.

That being said, the survey demonstrates the multiple benefits of Zero Trust make the effort worthwhile.

87% said Zero Trust can improve productivity.

97% said Zero Trust can help deal with the current global situation. For 76% it would be unwise not to consider Zero Trust given the increase in attacks.

So, how can your team #BeCyberSmart in the #NewTomorrow?

1. Watch out for scams
64% of companies have seen an increase in phishing attacks this year.

2. Run security updates on your home network
53% said remote working makes them more vulnerable due to insecure devices.

3. When in doubt, stick to the rules
48% see shadow IT as one of their top security challenges in the future.

Discover how Zero Trust can mitigate the human factor in cybersecurity.

LEARN MORE