Organizations that exploit digital trust, privacy, concern and care for their customers are going to establish a very differentiated position and it is the excellent cybersecurity talent that is required to actually have an impact on the security of the organization. But talent is a bigger challenge. It takes longer, it is more work to recruit people, it is very difficult to provide the environment and the compensation to retain people.

31% indicate either lack of training or staffing budget as their single biggest inhibitor to cybersecurity provision.

Reframing the debate around expenditure and particularly the debate around the benefits from a purely transactional; you know how much did it cost to lose this record to:

- What was the impact on our brand?
- What was the impact on our perception with our customers?

Shifting the discussion in that direction I think opens up a much greater engagement from the business in the security function.

73% Brand Reputation is the most vulnerable business goal for data security.

And in appreciation for the importance of moving security towards digital trust, towards a brand attribute, towards a fundamental aspect of the business rather than security being a back office function.

And what is separating these successful organizations from the unsuccessful organizations is increasingly governance, business alignment, the credibility with the security executives with the rest of the organization.

43% Indicate the Culture of Cybersecurity Awareness is very or critically important to their overall business.