Data breaches make headlines monthly, if not weekly. Corporations worry about the hit to their brand and their future access to data. Just as alarming is the attitude of consumers who suspect that by sharing their data, or simply going online, they're giving up something of value to them: their privacy. C-suite executives are concerned, as in the words of Ian Soffe, CEO of OSS Group in New Zealand, "A consumer rebellion is emerging against data privacy invasions."

The cost of data incursions is too high to ignore. Research on Fortune 500 companies has shown that just 20 percent of organizations had instituted policies about data transparency and opt-out control of their data to customers. When data breaches occurred, the organizations that didn't provide transparency or control had 1.5 X larger drops in their stock prices.[7]

Combined with the right talent and governance, AI can help accelerate a shift in cybersecurity, turning what was primarily a defensive proposition into a proactive one. In attempting to make such a shift, organizations should consider three important guidelines:

- Security of business platforms will be critical to trust and their longevity, but companies need to balance this with frictionless customer and employee experiences.
- Organizations must work to secure both the human and machine elements along key workflows and data sources.
- The ecosystem of business platforms requires an open network approach to security across all parties, driving collaboration and insights at speed.

"One of the key challenges is maintaining customer trust in a world where new data-driven businesses constantly emerge. We need to ensure our customers know that we treat their data in a trustworthy way."

Marcus Claesson,
CIO, Daimler Commercial Vehicles, Germany