4 of 5 respondents believe that there are broad gaps in their cyber defenses.

74% feel their cybersecurity is at risk.

Many companies have adopted a fragmented approach with 43-56% of surveyed companies believing that they have limited oversight for compliance.

Only 22% believe they have effective third-party agreements.

Only 6% believe they have sufficient internal capabilities.

INVEST TO INNOVATE AND OUTMANEUVER

To drive financial understanding and business alignment, it is important to engage with enterprise cybersecurity leaders.

The top three targets for investment are:

1. Business and technology
2. Cyber resilience
3. Cyber response

BUILD CONFIDENCE IN THE SECURITY ORGANIZATION

1. Make security a critical priority in protecting company value.
2. Focus on cybersecurity strategy development.
3. Develop a robust response to protect and recover key assets.
4. Understand the threat landscape, develop approaches and use "design for resilience" techniques.
5. Align the security program with the business strategy.
6. Create a clear-cut cybersecurity chain of command.
7. Establish a cyber incident response plan, strong cyber incident communications, tested plans, and effective escalation paths.
8. Be ready to cooperate during crisis and effective third-party agreements and focus on cybersecurity clauses and management.
9. Develop an understanding of the internal business-relevant threat monitoring, peer monitoring and other areas of cybersecurity threats.
10. Align the security program with the business, identify key drivers, decision points and barriers that could materially affect the business.