"Deficient, Disconnected & in the Dark": the first report in a two-part independent global study of 4880 IT security practitioners by the Ponemon Institute and sponsored by Websense.

There is a disconnect between data breach perception and reality. Despite the average cost of an organizational data breach estimated at $5.4 million*, respondents believe that executive teams do not seem to understand the potential revenue loss to their business.

Security professionals are in the dark as they find it difficult to keep track of the threat landscape or even know if their organizations have been attacked.

Only 41% believe they have a good understanding of current cyber threats.

37% are unsure if their organization was attacked in the past 12 months.

8% are unsure if their organization has suffered attack in the last 12 months as a result of a breach.

17% are unsure if their organization has suffered a breach in the last 12 months.

44% believe their organization would not have been attacked by an external actor.

Only 7% believe their organization lost sensitive or confidential data as a result of a recent cyber attack.

48% say that board-level executives have a sub-par understanding of security issues.

69% say that cybersecurity threats sometimes fall through the cracks of their existing security systems.

57% say that advanced cyber threats are beyond their protection.

59% say they are not adequately informed about the threat landscape.

63% of companies do not have adequate intelligence or are unsure about attempted attacks and their impact.

57% feel unprotected from advanced cyber threats.

69% say that cybersecurity threats sometimes fall through the cracks of their existing security systems.

63% of companies do not have adequate intelligence or are unsure about attempted attacks and their impact.

69% say that cybersecurity threats sometimes fall through the cracks of their existing security systems.

Only 10% believe they have a good understanding of the threat landscape.

41% believe they have a good understanding of current cyber threats.

Only 7% believe their organization lost sensitive or confidential data as a result of a recent cyber attack.

48% say that board-level executives have a sub-par understanding of security issues.

69% say that cybersecurity threats sometimes fall through the cracks of their existing security systems.

57% say that advanced cyber threats are beyond their protection.

59% say they are not adequately informed about the threat landscape.

63% of companies do not have adequate intelligence or are unsure about attempted attacks and their impact.

57% feel unprotected from advanced cyber threats.