Of global organizations confirmed they have been breached at least once over the last 12 months.

According to research conducted by Vanstone Bourne Research.

Physical and virtual assets are connected to organizational networks on an average business day. And only 60% of these assets are monitored.

Of the respondents, report using 10 or more different sources to collect data relating to threat intelligence. Only 58% of this information is actionable.

Of respondents say employees are downloading shadow IT to connected assets in the work environment.

Of organizations admit to still using manual spreadsheets.

Of organizations claim to have complete visibility of the organization-owned and managed assets currently connected to their network.

Consequences of a breach:
- Operational downtime
- Financial loss

Of organizations report their vulnerability and patch management processes are known across the organization.

In the US, 61% of organizations have been breached as a result of a cyber attack in the last 12 months.

In France, 44% of respondents indicated a lack of visibility over employee owned assets connected to the business environment.

In the UK, 49% of the cybersecurity team feels overwhelmed by cyber threat information.

ONLY 35% have a formalized process to examine vulnerability and patch management.

91% reported a lack of control and management.

For the complete report that includes findings for the UK, UK, France, Germany, Australia, New Zealand and Singapore go to https://www.armis.com/attack-surface-management.