Cyber incidents are on the rise, yet some organizations still do not have plans in place to mitigate those threats.

- 98% of US executives say their organization experienced one or more cyber incidents in the past year.
- 84% of ROW executives say their organization experienced one or more cyber incidents in the past year.

When asked if their organizations have strategic and operational plans in place to defend against cyber threats:
- 14% of US executives said NO.
- 6% of ROW executives said NO.

The biggest fail of all these cyber incidents or breaches are:
- 29% of US executives said phishing.
- 24% of ROW executives said phishing.

The challenges to cybersecurity management:
- US executives: 31% of US executives think cyber is top of mind for their boards.
- ROW executives: 16% of ROW executives think cyber is top of mind for their boards.

Cyber threats:
- 13% of US executives said supply chain deficiencies of malicious actors.
- 16% of ROW executives said supply chain deficiencies of malicious actors.

But how do executives detect or mitigate employee indicators?
- 15% of US executives said they leverage automated tools to help detect or mitigate employee indicators.
- 41% of ROW executives said they leverage automated tools to help detect or mitigate employee indicators.

Balancing business needs with customer trust has room for improvement in the US:
- 42% of US executives said they would drop an increase in customer trust.
- 22% of ROW executives said they would drop an increase in customer trust.

Additional key findings:
- Zero trust adoption continues to gain momentum:
  - US: 6% of US executives said NO.
  - ROW: 44% of ROW executives said NO.

Reach out to learn more or visit: