Country view:
United States of America

US respondents to our survey were confident in the ability of their business to fend off a cyber attack. As with C-suite respondents in the UK, US business leaders indicated that 7% of their organization's IT budget was spent on cyber security and defense, lower than the worldwide figure of around 10%.

The results show a significant difference in how the two types of respondent (ITDM and C-suite) viewed the threat landscape. While both groups viewed organized crime as the most likely source of attack, nearly a third (32%) of ITDMs saw terrorist organizations as a likely source of attack – compared to just 7% of C-suite respondents, who were more likely to suspect professional crime groups.

IT Decision Makers in the USA responded far more actively to the question of where and why they would invest extra resources in cyber security, with over half (56%) wanting to minimize their security risk, something that was a reason for only 22% of C-suite respondents. American C-suite respondents were most concerned with keeping up to date with current and new threats and minimizing risk. Reassuring customers came low on the list at 6% (compared to 27% of ITDMs), in line with the need to respond to a successful attack on the business.

When it came to cloud computing, the two groups formed something of a consensus around cloud security concerns. Almost a third (27%) of both groups saw cloud services as posing a significant security risk, although 31% of ITDMs also saw the services as supporting more agile business practices. Both groups (27% of C-suite respondents, 32% of ITDMs) also viewed Cloud services as a necessary part of doing business, but also something they'd like to impose limits upon.

Nearly a third (32%) of ITDMs saw terrorist organizations as a likely source of attack