Country view: Canada

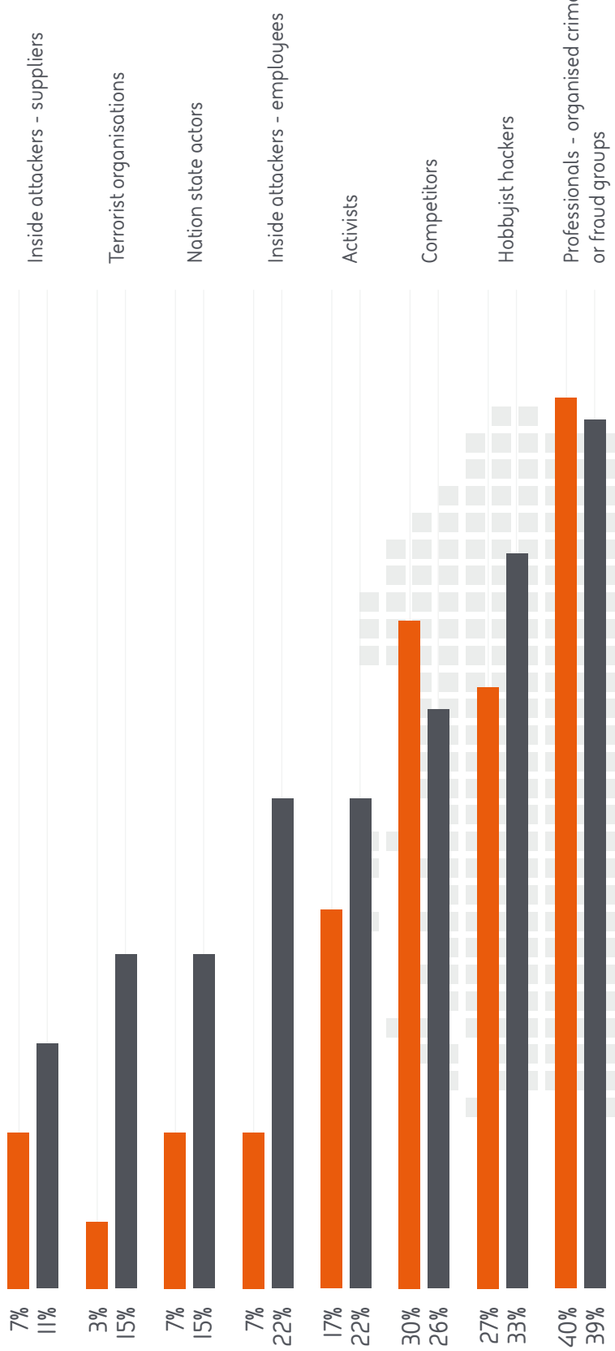
Along with Australians, and their neighbors in the USA, Canadian ITDMs and C-suite respondents rank as the most confident that their organizations are equipped to repel cyber attacks. ITDMs in Canada are also very likely to argue that their counterparts are responsible for an attack succeeding: 54% of IT Decision Makers said they thought responsibility for a security breach lies with senior management, compared to 20% of Canadian C-suite respondents who felt it was up to the IT team.

It's interesting to compare Canadian responses to those from South of the border, too. Despite this proximity, it's clear that business and technology assumptions and experiences are different enough to generate strong differences of opinion.

Canadian respondents agreed that organised crime or fraud groups posed the most likely threat, the second most likely being hobbyist hackers. This second threat stood in direct contrast to US ITDMs, who worried about cyber attacks from terror groups as their second most likely threat.

This, of course, should be tempered with a more sober assessment of the reasons for a successful cyber attack. Four out of five (80%) Canadian C-suite respondents cite human error by employees as the primary reason for a successful cyber attack. IT Decision Makers named a wider variety of reasons, with only 40% citing employee error. Interestingly, exactly half of C-suite respondents pointed towards a lack of investment in IT security as the reason for a potential breach, with a preference for blaming outdated software (43%) as the reason.

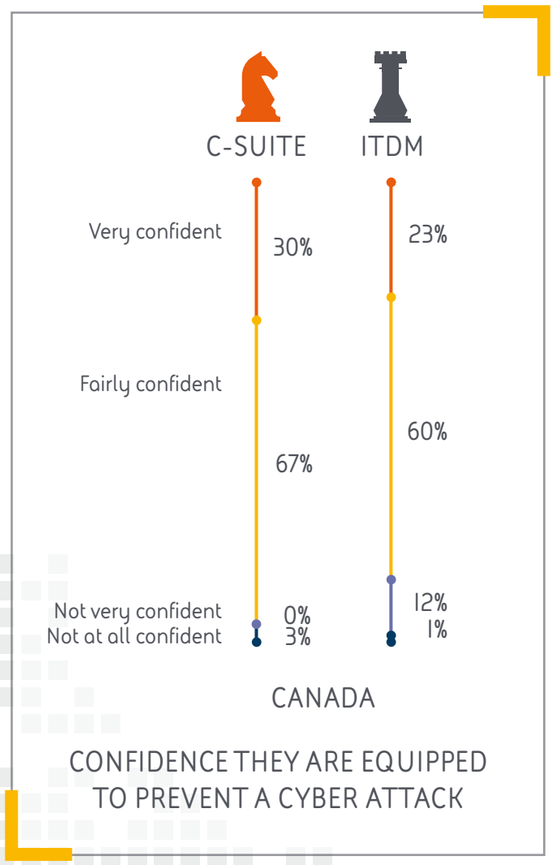
When asked for reasons as to why they would make additional investments in IT security, the answer to this problem became a little clearer. C-suite respondents talked in terms of response to new or increased cyber threats (43%) as well as plugging gaps in existing infrastructure (29%) and staying up to date with current threats (33%). In comparison, 32% of IT Decision Makers would make the investment in order to reassure customers – something only 5% of C-suite respondents put as a reason.



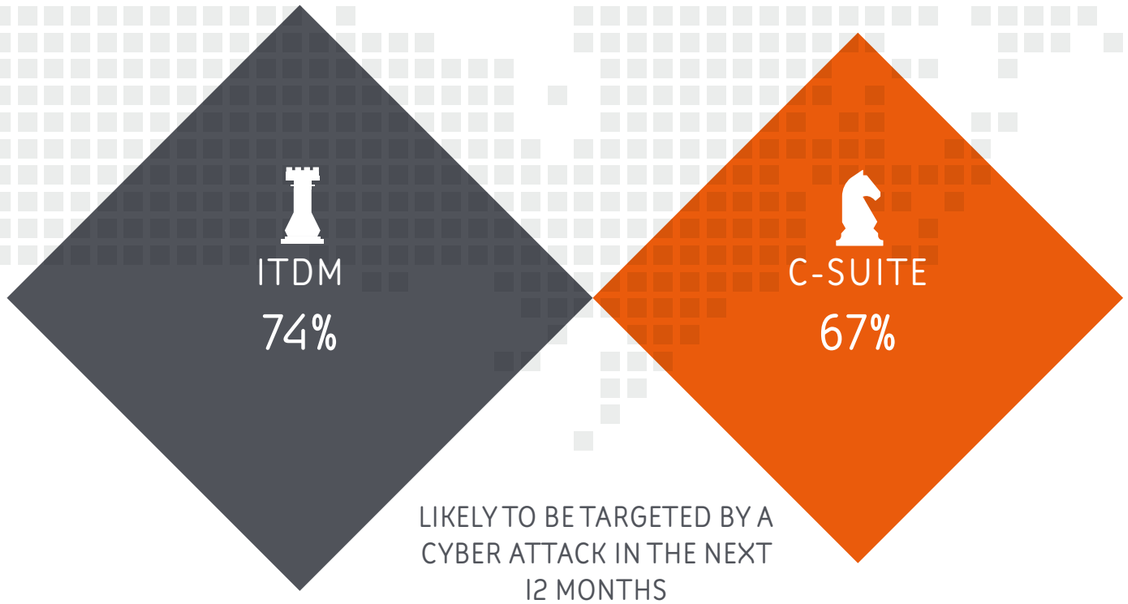
MOST LIKELY SOURCE OF THREAT - CANADA

24% of C-suite respondents want more investment to help replace legacy systems

46% of ITDMs believe more investment will minimise their cyber security risk



CONFIDENCE THEY ARE EQUIPPED TO PREVENT A CYBER ATTACK



LIKELY TO BE TARGETED BY A CYBER ATTACK IN THE NEXT 12 MONTHS