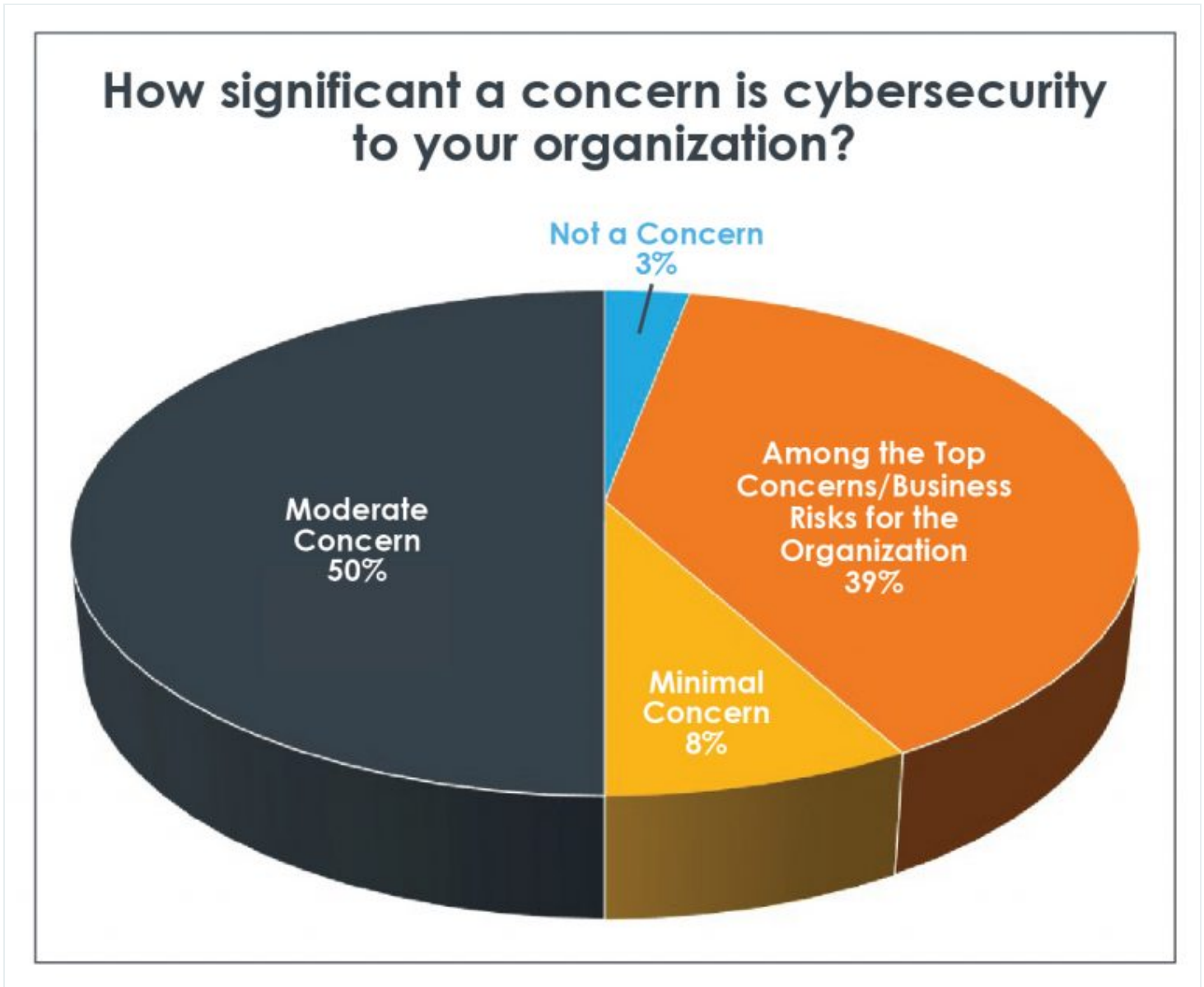


Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

firms, conducted a global survey with Nexia International to assess the current state of cyber preparedness. More than 350 companies from around the world provided ...

Jan. 31, 2018



This year, CohnReznick LLP, one of the nation's leading accounting, tax, and advisory firms, conducted a global survey with Nexia International to assess the

current state of cyber preparedness. More than 350 companies from around the

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

- Only 39% of respondents consider cybersecurity a top concern.
- 46% of respondents across the Americas do not have a formal cybersecurity program.
- 50% of respondents indicated that hacktivists, organized crime, and employees – both current and former – are the sources of greatest cyber risk.
- 20% of respondents have not conducted a cybersecurity assessment, and only 25% of respondents provide cybersecurity training to employees at least annually.
- 20% of respondents who are required to have a cybersecurity program based on governmental, industry or customer regulations do not currently have a cybersecurity program
- Limited time and budget along with a lack of qualified staff were the key reasons cited for not having an effective cybersecurity program.
- More organizations that have a cybersecurity program reported experiencing a breach than those who do not have a formal cybersecurity program.
- The majority of the respondents indicated underinvestment in advanced cybersecurity initiatives such as a robust security incident response plan to identify, detect, and handle security incidents including data breaches.

The above, taken with the rest of the survey data and responses, highlights an overall lack of intensity and awareness of the need for a comprehensive cybersecurity program. And if the rising cyber threats and increasing fines are not enough for companies to rethink their cyber programs, there are ample new regulations that may provide the needed impetus.

[Access full report](#)

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us