

April 10, 2026

VIA RESS & EMAIL

Ontario Energy Board
P.O. Box 2319
2300 Yonge Street, 27th Floor
Toronto, ON M4P 1E4
Attention: Mr. Ritchie Murray, Acting Registrar

Dear Mr. Murray:

Re: EB-2025-0252: Alectra Utilities Corporation (“Alectra Utilities”) 2027-2031 Custom Rate Application for Electricity Distribution Rates and Charges – Request for Confidential Treatment of PwC Canadian Power Sector Cybersecurity – Budget and Headcount Benchmarking Report (JT-3.24)

On March 27, 2026, Alectra Utilities filed undertaking responses in respect of its custom rate application for electricity distribution rates and charges for the 2027-2031 period (the Application) with the Ontario Energy Board (OEB).

As indicated in Alectra Utilities’ response to JT-3.24, Alectra was unable to produce the PwC Cybersecurity Budget & Headcount Benchmarking Report because the consultant had informed the utility that the information within the report was protected under contractual arrangements signed by the participants in the study. It was stated that Alectra Utilities was actively working with the consultant to resolve the issue, and that an update would be filed at a later date. After deliberation with the consultant, a redacted version of the report is being provided. Alectra Utilities requests that certain information contained in the report receive confidential treatment under Parts 5 and 6 of the *Practice Direction on Confidential Filings* (the “Practice Direction”) and/or be permanently redacted from the public record as the information is not relevant under Part 11 of the Practice Direction.

Information that PwC has advised Alectra Utilities is confidential due to PwC’s contractual agreements with other participants:

- **Reference:** JT-3.24, Attach. 1 (Cybersecurity Budget & Headcount Benchmarking Report), pages 2, 4, 8-9.
- **Rationale:** The information consists of total participant numbers and group size indicators. PwC has advised that Alectra Utilities that PwC does not have participants’ consent to publicly disclose this information. This information has been marked confidential, due to PwC’s contractual obligations to other survey participants (Practice Direction, Appendix A, Part (a)(ii)).

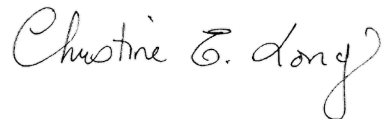
Non-relevant confidentiality disclaimers redacted at PwC's request:

- **Reference:** JT-3.24, Attach. 1 (Cybersecurity Budget & Headcount Benchmarking Report), all pages.
- **Rationale:** The redacted information consists of confidentiality disclaimers added to all pages of the report. The disclaimers are no longer relevant to the document as a redacted version of the document is being produced on the public record, and the inclusion of the disclaimer may be more confusing than helpful to those reading the document. Furthermore, PwC has advised Alectra Utilities that Alectra Utilities does not have PwC's consent to publicly disclose the disclaimers contained within their work product. In any event, the redacted disclaimers would not provide any assistance to parties or the OEB in resolving the issues in this proceeding.

Alectra Utilities has marked redactions in blue outline for non-relevant information, which it seeks to permanently redact from the public record in accordance with Part 11 of the Practice Direction, and in red outline for information for which Alectra Utilities seeks confidential treatment (in accordance with Parts 5 and 6 of the Practice Direction).

Please let us know if you have any questions or concerns.

Sincerely,

A handwritten signature in cursive script that reads "Christine E. Long".

Christine E. Long
Senior Vice-President Regulatory Affairs and Privacy Officer

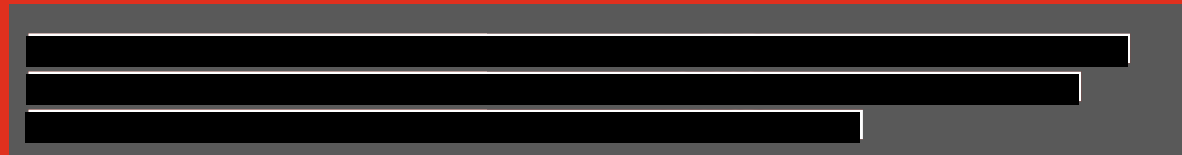
cc: All Parties
Natalie Yeates, Alectra Utilities
Charles Keizer, Torys LLP
Daliana Coban, Torys LLP
Jonathan Myers, Torys L

JT-3.24

Attachment 1
PwC Cybersecurity Budget & Headcount
Benchmarking Report

Canadian Power Sector Cybersecurity Budget & Headcount Benchmarking Report for Alectra Utilities Corporation

October 2023



Background



As a lead-in to a broader cybersecurity benchmarking study (launching in November 2023), a group of power companies asked if PwC could gather and report on two time-sensitive questions:

- 1/ Cybersecurity budget trends
- 2/ Cybersecurity team headcounts

The results of this early survey are contained on the following pages.

Dates of this study: October 2-23, 2023

Number of participants: ■

Provinces covered: 7

Total customers served by study participants: 6.5M

The study includes statistics from ■ power companies representing 7 provinces across Canada

Reporting by full sample, and by respondent company size



In this report, we present the statistics in two ways:

1/ All Respondents (the full sample size).

The average sized power company in the study is 2900 employees. The median (mid-point) of the sample is 2,500 employees.

&

2/ Respondents separated into two categories based upon number of employees



**Larger-scale power company
>2,500 and <10,000 employees**



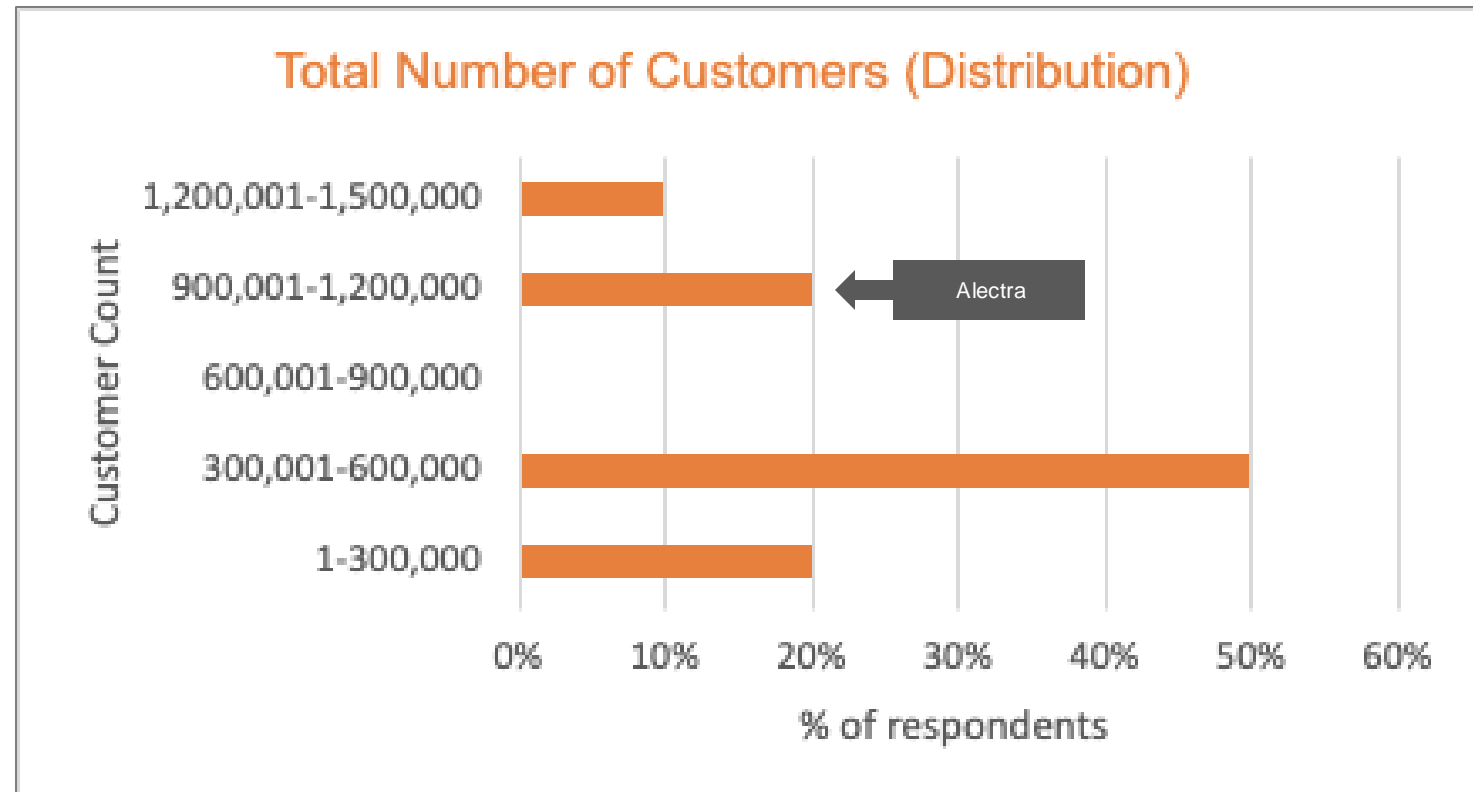
**Smaller-scale power company
< 2500 employees**



Number of Customers (across Distribution Companies)



Of the [redacted] respondents to the survey, [redacted] companies directly serve Canadian customers (ratepayers). The remaining [redacted] participants are generation, transmission or other non-customer-facing power companies.



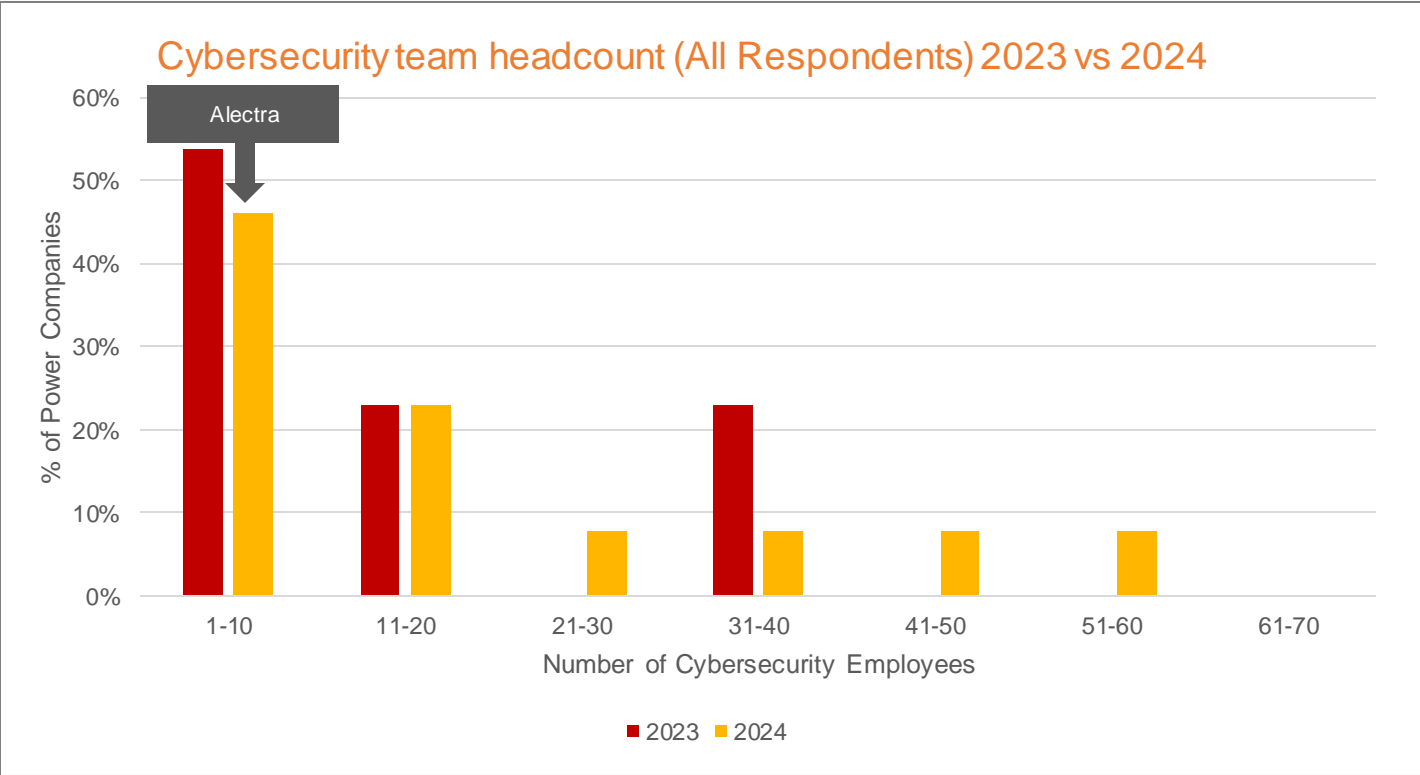
Cybersecurity Team Headcount – All Respondents



Cybersecurity team headcount for full-time employees and contractors (indicated in Red), and the forecasted cybersecurity team headcount (indicated in Orange).

CURRENT: The average number of cybersecurity team FTEs is 16, with a median of 9 FTEs.

FORECASTED: The average number of forecasted cybersecurity team FTEs is 20, with a median of 15 FTEs.



The average percent team size increase in 2024 will be 28%

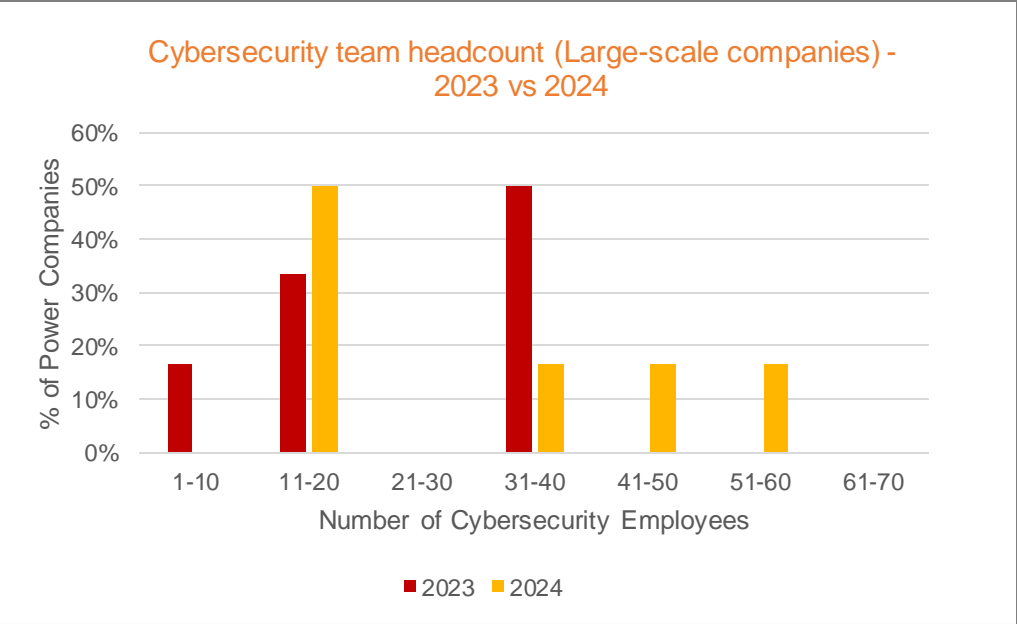
Note, this excludes external professional/managed services resources, and excludes other IT or OT resources within the organization who may perform cybersecurity tasks but are not within the core cybersecurity team.



Cybersecurity Team Headcount – By Company Size

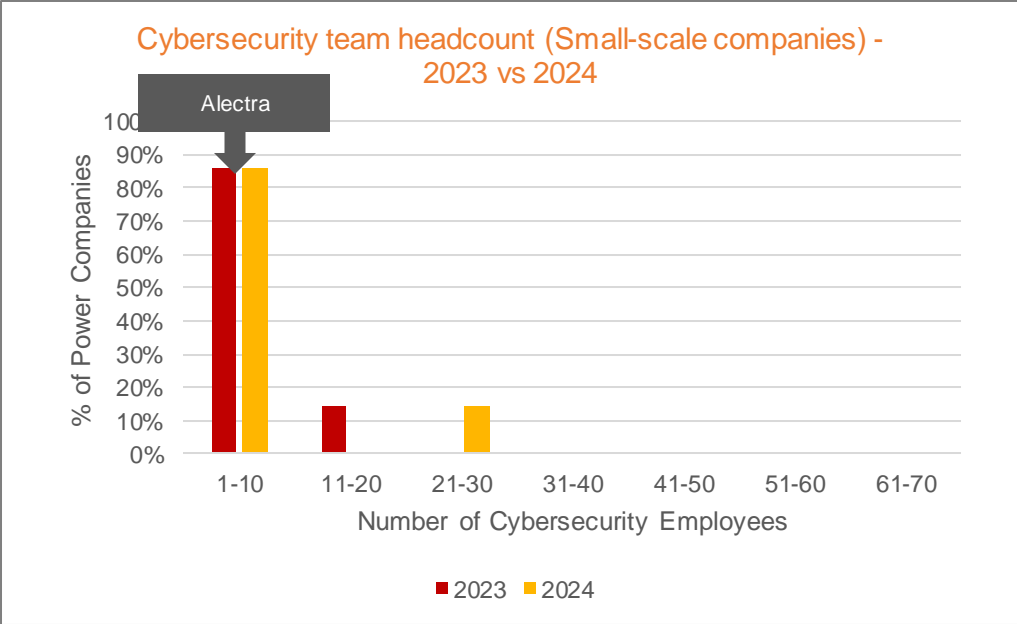


These charts provide the distribution of current cybersecurity team headcount for full-time employees and contractors (indicated in Red), and the forecasted cybersecurity team headcount (indicated in Orange).



CURRENT: The average number of cybersecurity team FTEs is 24.

FORECASTED: The average number of forecasted cybersecurity team FTEs is 32.5.



CURRENT: The average number of cybersecurity team FTEs is 8.5.

FORECASTED: The average number of forecasted cybersecurity team FTEs is 10.

Note, this excludes external professional/managed services resources, and excludes other resources within the organization who may do cybersecurity work but are not within the core cybersecurity team.

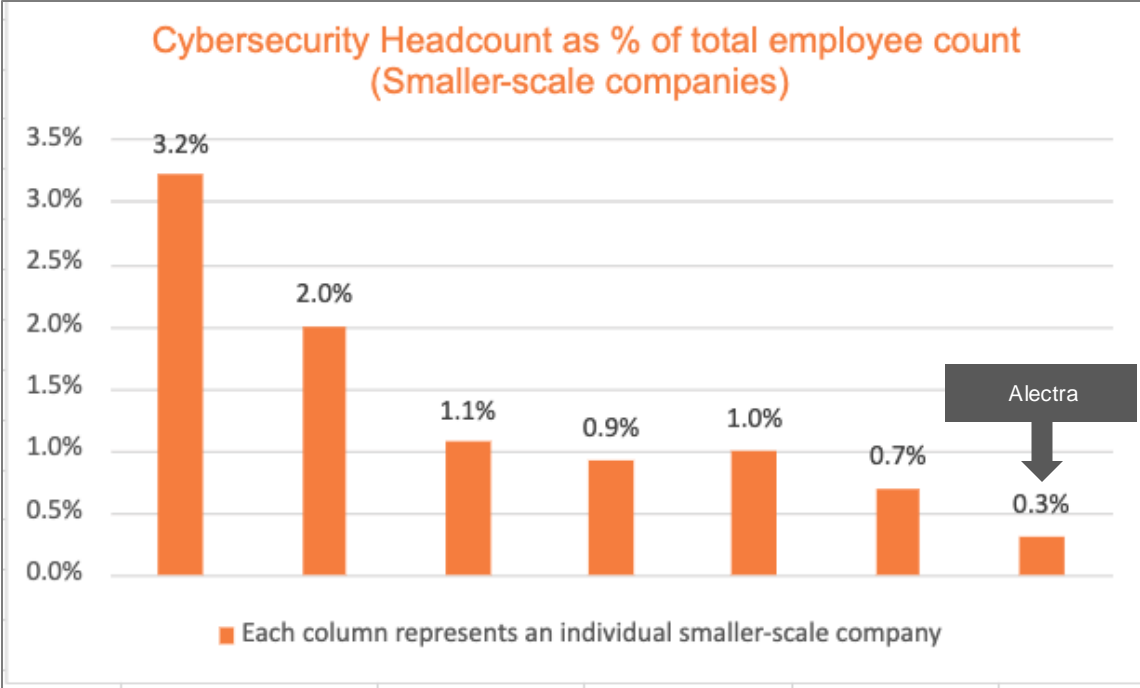
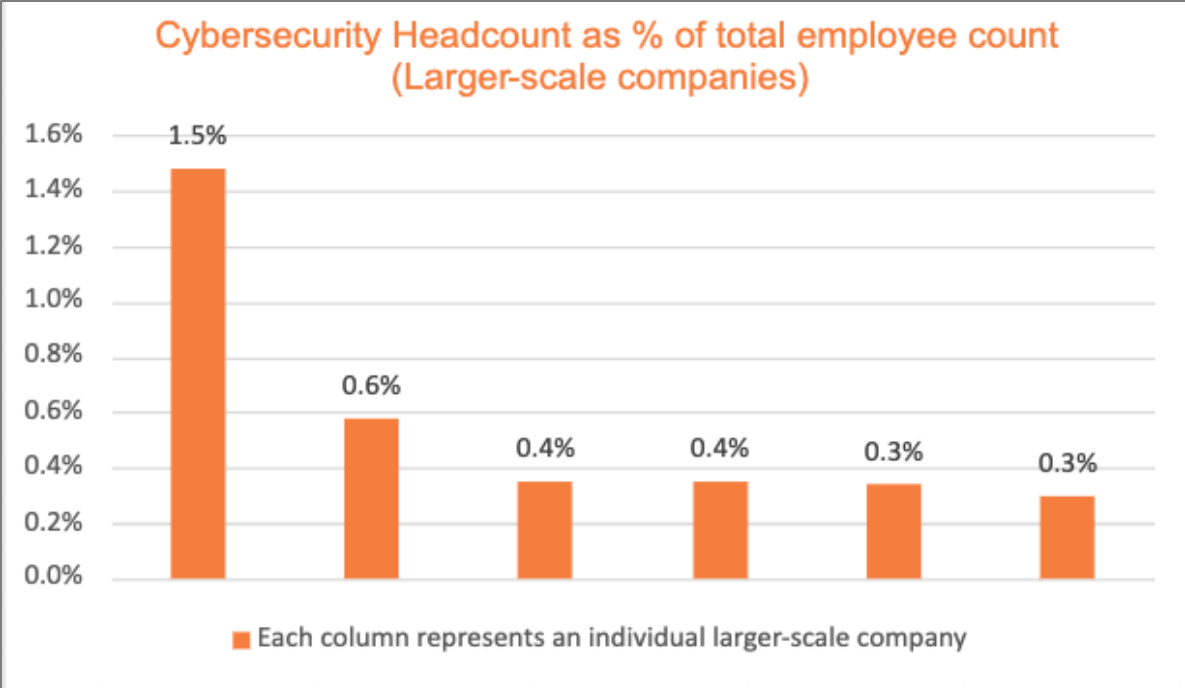


Cybersecurity Team Headcount – Relative to Total Employees



These charts provide the relative headcount of the current cybersecurity team versus the headcount of total employees.

Displayed separately for larger-scale and smaller-scale power companies.



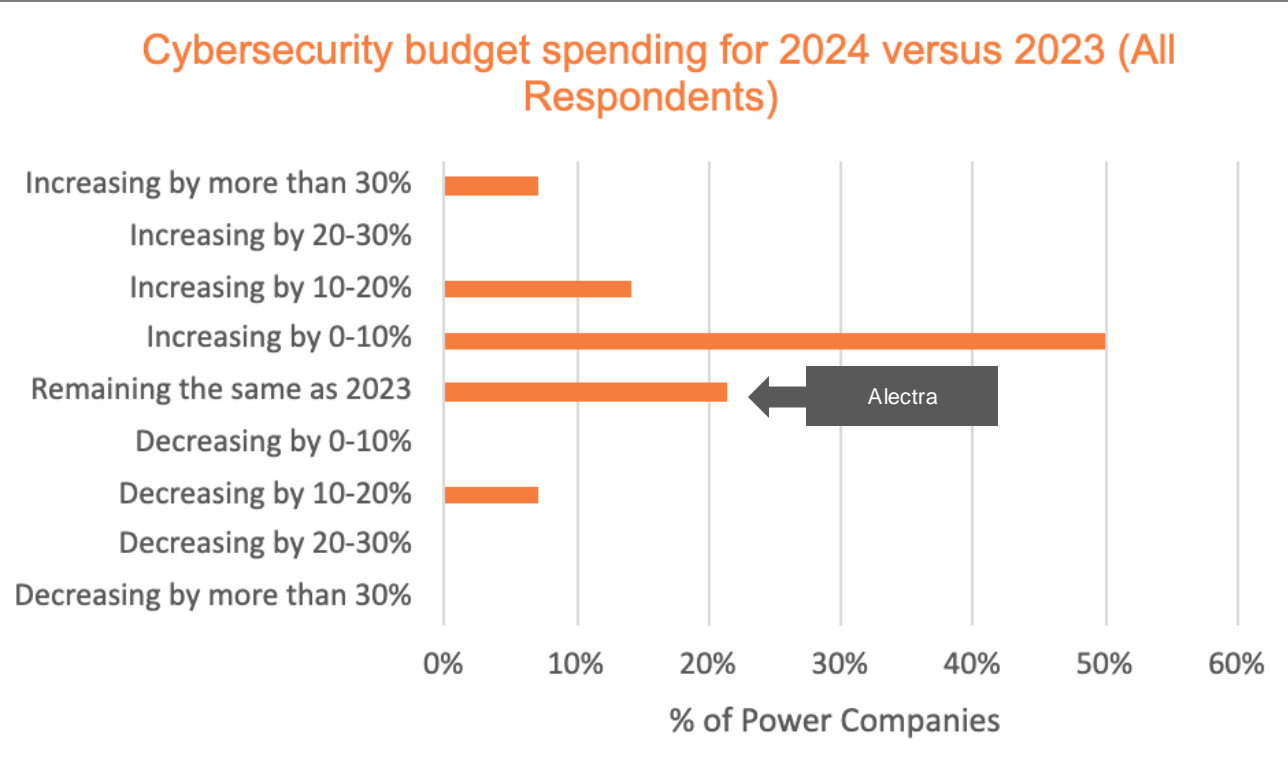
Cybersecurity Budget – All Respondents



This chart shows how cybersecurity budgets are increasing or decreasing across the sector in 2024 vs 2023.

CURRENT: The average 2023 cybersecurity budget across all respondents is \$9.7M. The median current budget is \$3M.

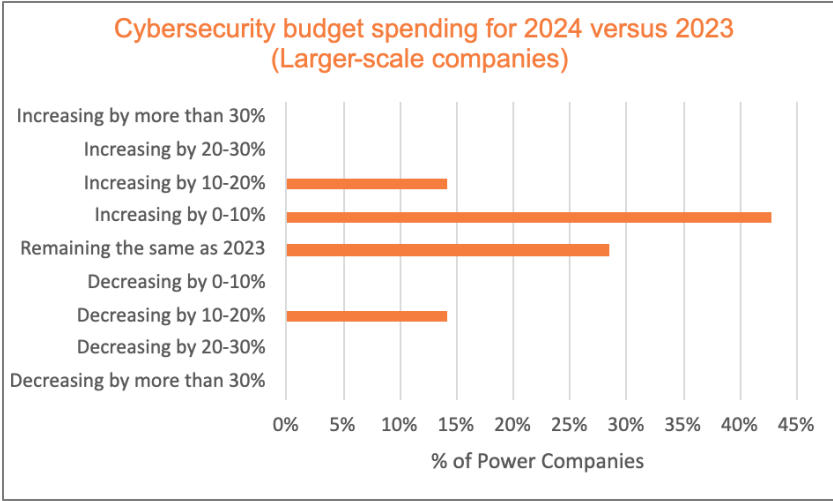
FORECASTED: For the forecasted 2024 cybersecurity budget, 71% of respondents plan to increase their cyber budget by an average of 12%. Only 1 out of [redacted] respondent plan to reduce their cybersecurity budgets next year.



Canadian Cybersecurity Budgets

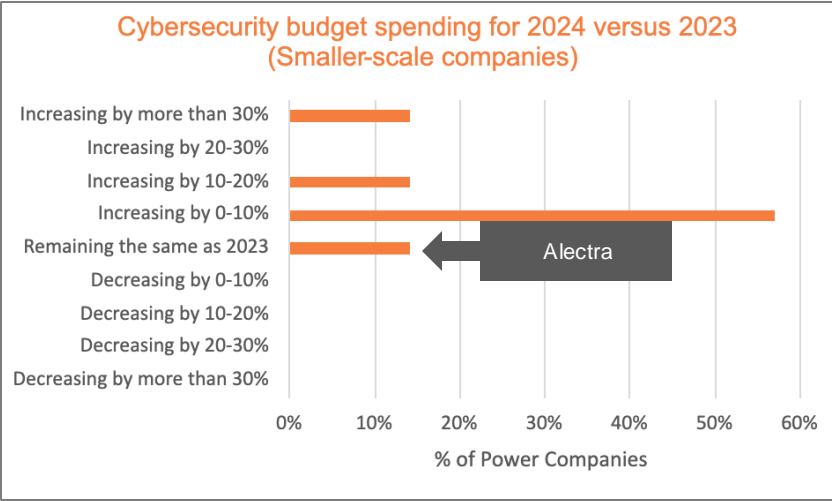


This chart shows how cybersecurity budgets are increasing or decreasing across the sector in 2024 vs 2023, displayed separately for larger-scale and smaller-scale power companies.



CURRENT: The average 2023 cybersecurity budget across larger-scale respondents is \$17M. The median current budget is \$11.6M.

FORECASTED: For the forecasted 2024 cybersecurity budget, 57% of respondents plan to increase their cyber budget by an average of 8%. 1 out of 10 respondents plan to reduce their cybersecurity budgets next year.



CURRENT: The average 2023 cybersecurity budget across smaller-scale respondents is \$2M. The median current budget is \$1.5M.

FORECASTED: For the forecasted 2024 cybersecurity budget, 85% of respondents plan to increase their cyber budget by an average of 15%. 0 out of 10 respondents plan to reduce their cybersecurity budgets next year.



Further Insights & Connections

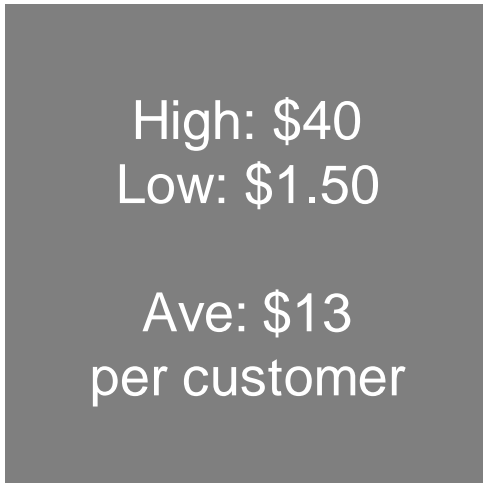


Cybersecurity spend per employee



**Alectra: \$938
per employee**

Cybersecurity spend per customer



**Alectra: \$1.50
per customer**





This document is protected under the copyright laws of Canada and other countries as an unpublished work. This document contains information that is proprietary and confidential to PwC and shall not be disclosed outside the recipient's company or duplicated, used or disclosed in whole or in part by the recipient for any purpose without prior written PwC approval.

© 2023 PricewaterhouseCoopers LLP, an Ontario limited liability partnership. All rights reserved.

PwC refers to the Canadian firm and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.