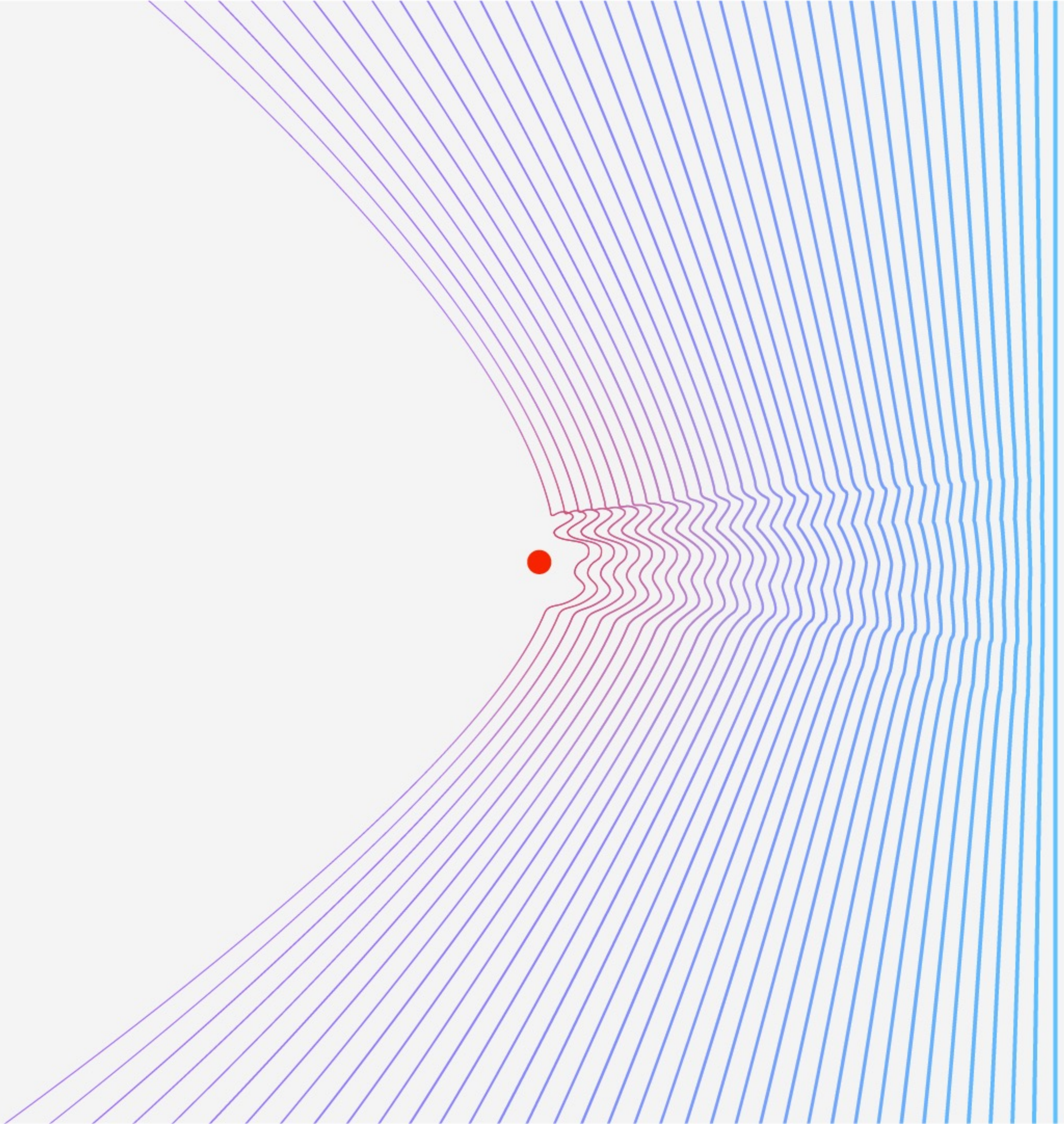
IBM **Security**

Cost of a Data Breach Report 2023

CyberAlberta Community of Interest



Canada	2023 sample
Sample size	26
Per capita in CAD	246
Total cost in CAD millions	6.94
Average records breached	25,750
Years studied	9
Currency	Canadian dollars (CAD)

Key findings

While average global cost of a data breach reached a record high in 2023, the average cost in Canada decreased 9%

CAD 6.94 million

Average cost of a data breach

CAD 11.99 million

Average cost of a breach in Financial sector, the top industry in Canada in terms of breach cost

51%

Organizations globally that planned to increase security investments as a result of a breach, with top investments in incident response (IR) planning and testing, employee training, and threat detection and response

Using Employee training, deploying IR teams and security AI and automation produced large savings

CAD 318K +

Savings for organizations using high levels of employee training

CAD 309K +

Savings for organizations threat intelligence to uncover breaches

33 days

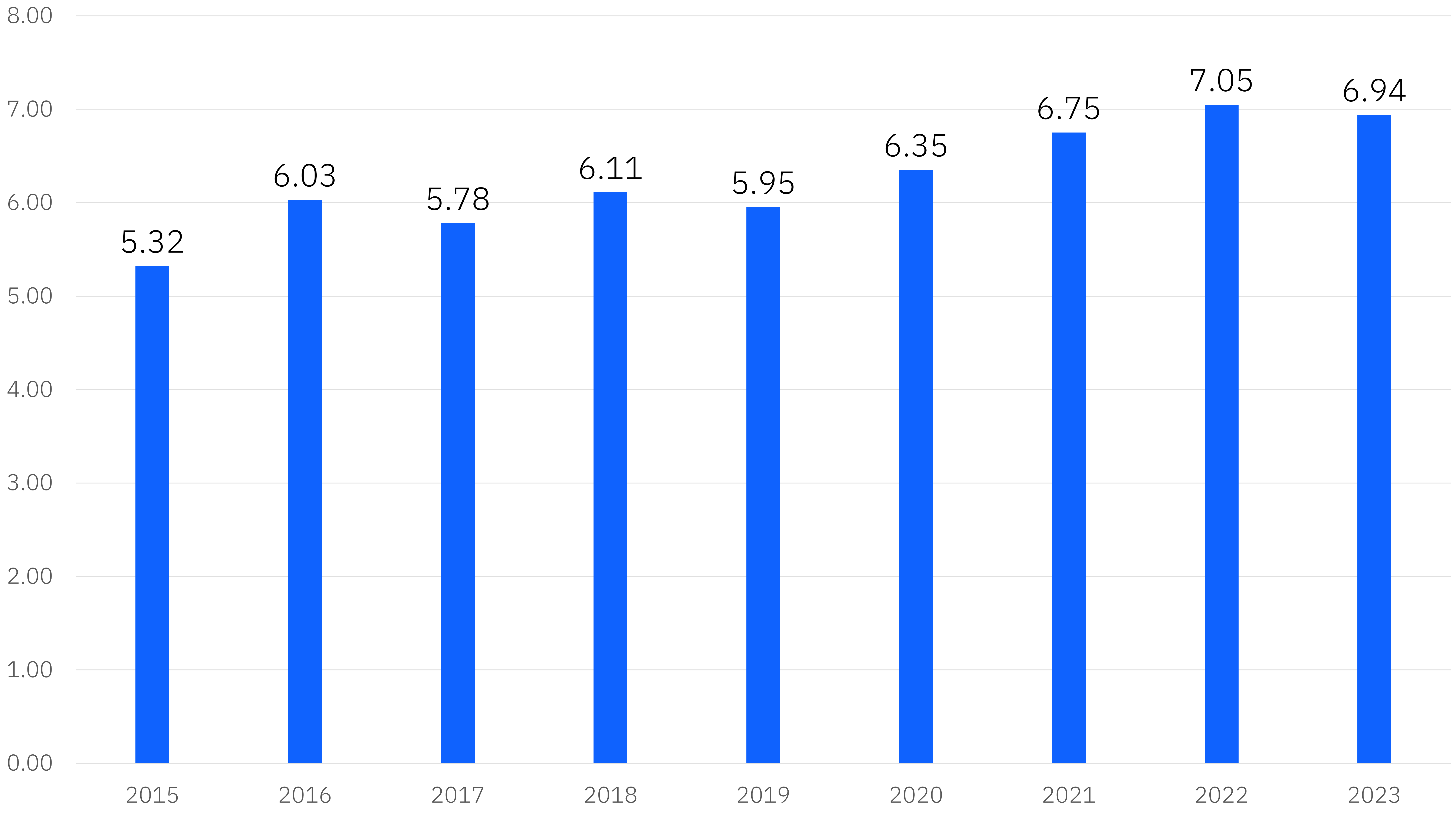
Breach response time saved for organizations with extensive use of security AI and automation

CAD 1.74 million

Savings for organizations with extensive use of security AI and automation compared to organizations with no security AI or automation deployed

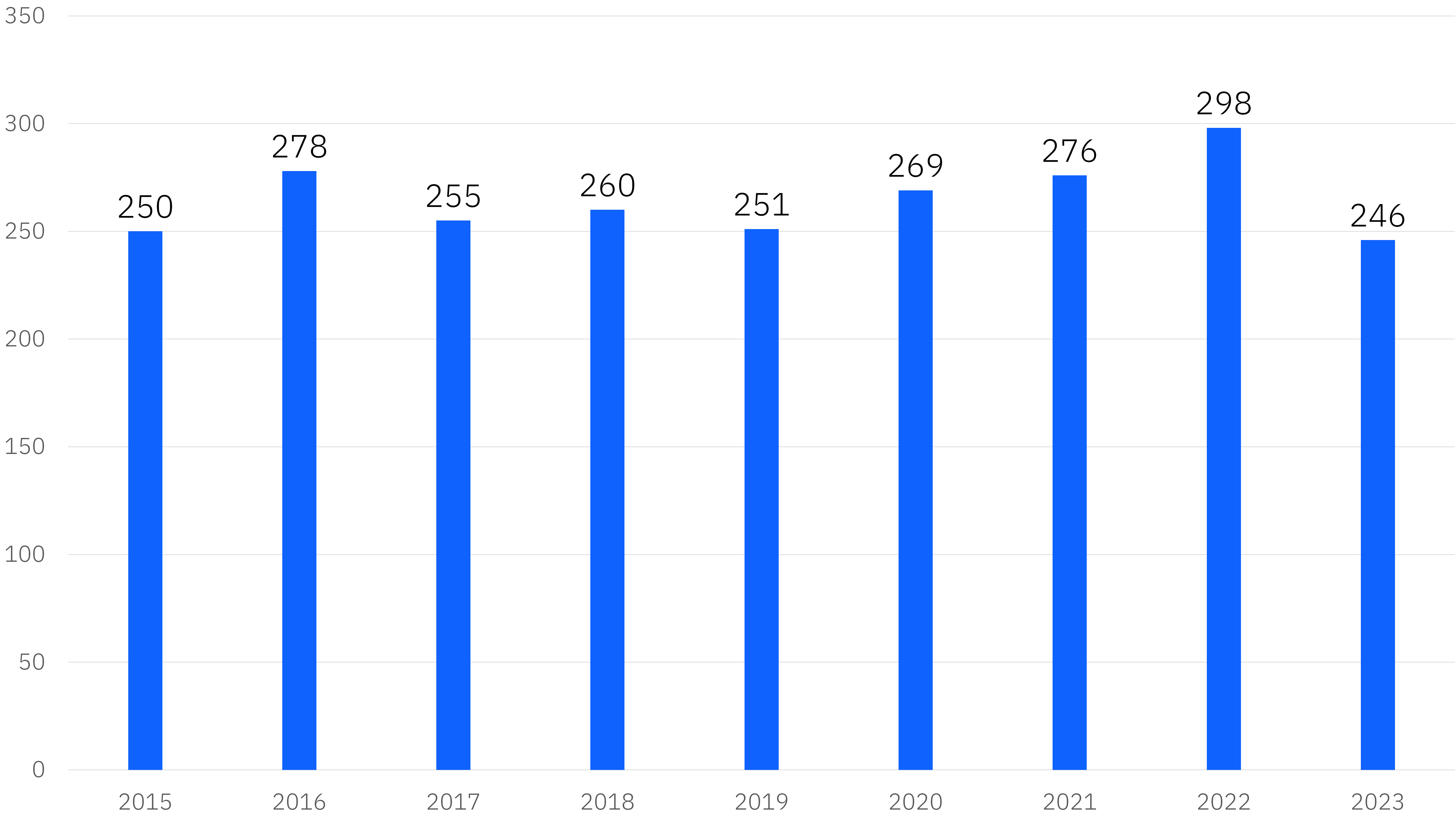
Total cost of data breach over nine years

Measured in CAD millions



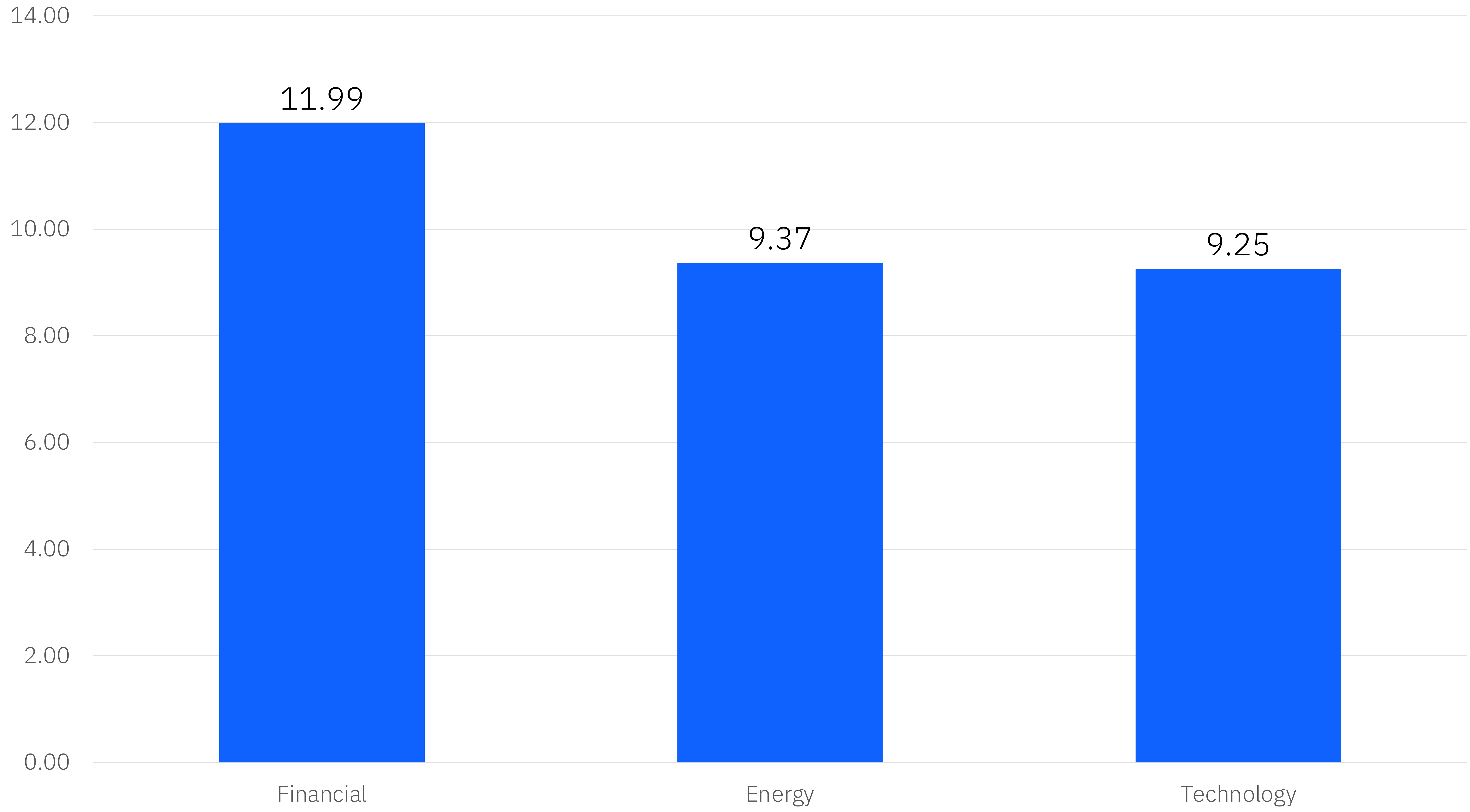
Per record cost of data breach over nine years

Measured in CAD



Top three industries in total cost of a data breach

Measured in CAD millions



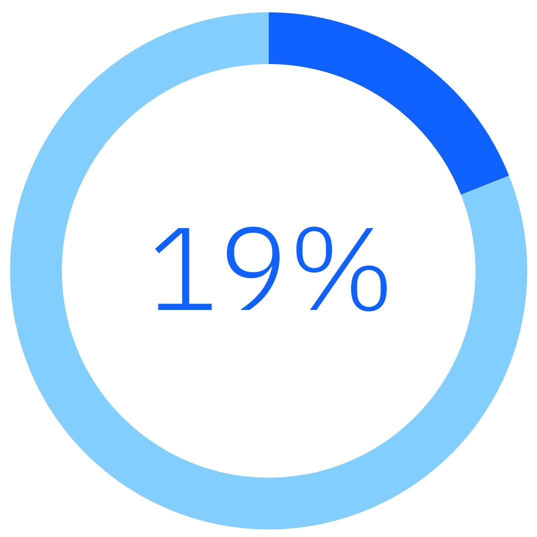
CAD 3.3M

Average cost of a data breach in Canada’s Public sector

17th highest cost
of 17 industries studied

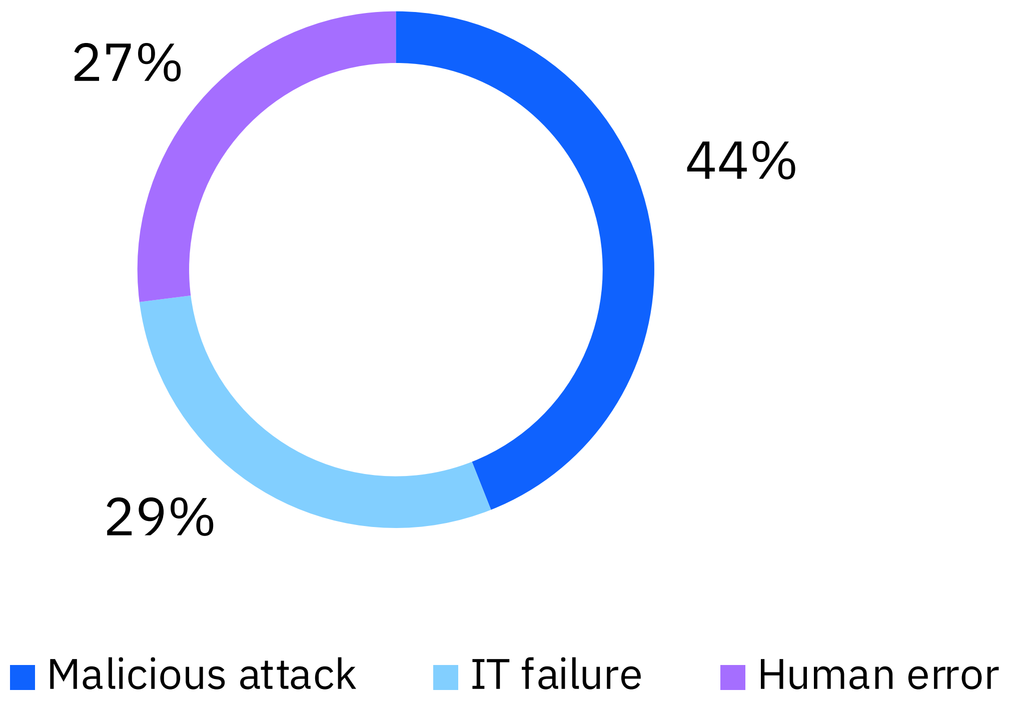
52% lower than the
CAD 6.94M Canadian average

Key statistics



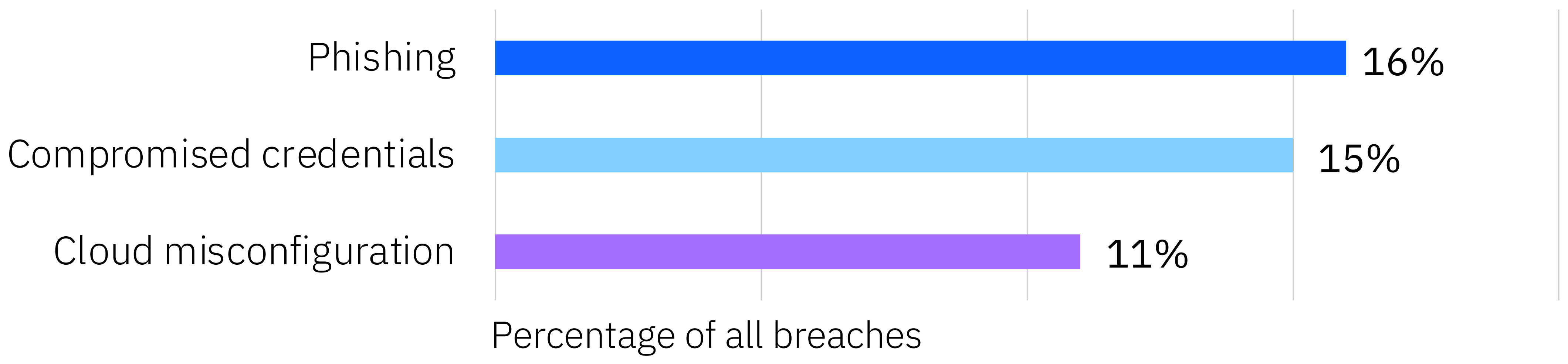
Percentage of public sector organizations with extensive use of security AI and automation

Root causes of a data breach



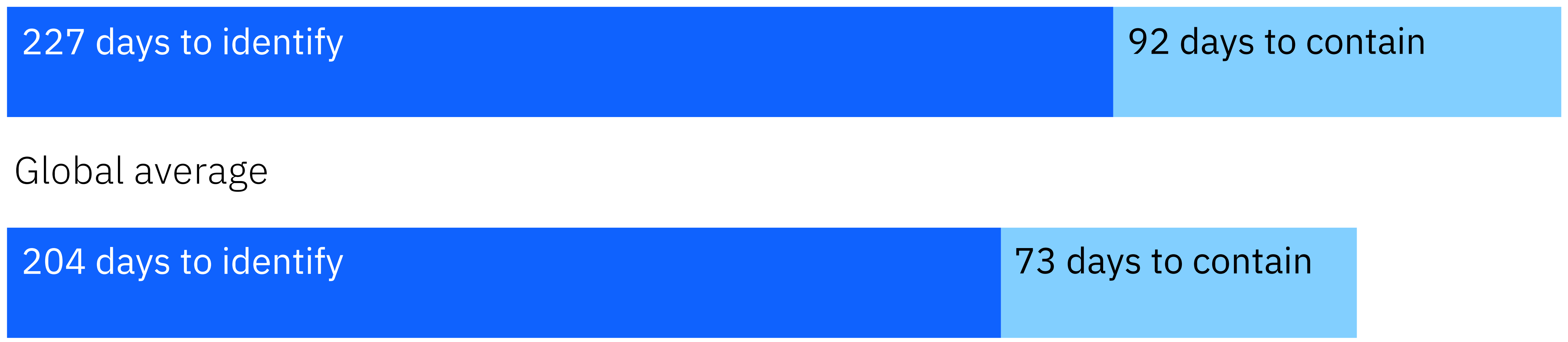
Global highlights

Top 3 initial attack vectors



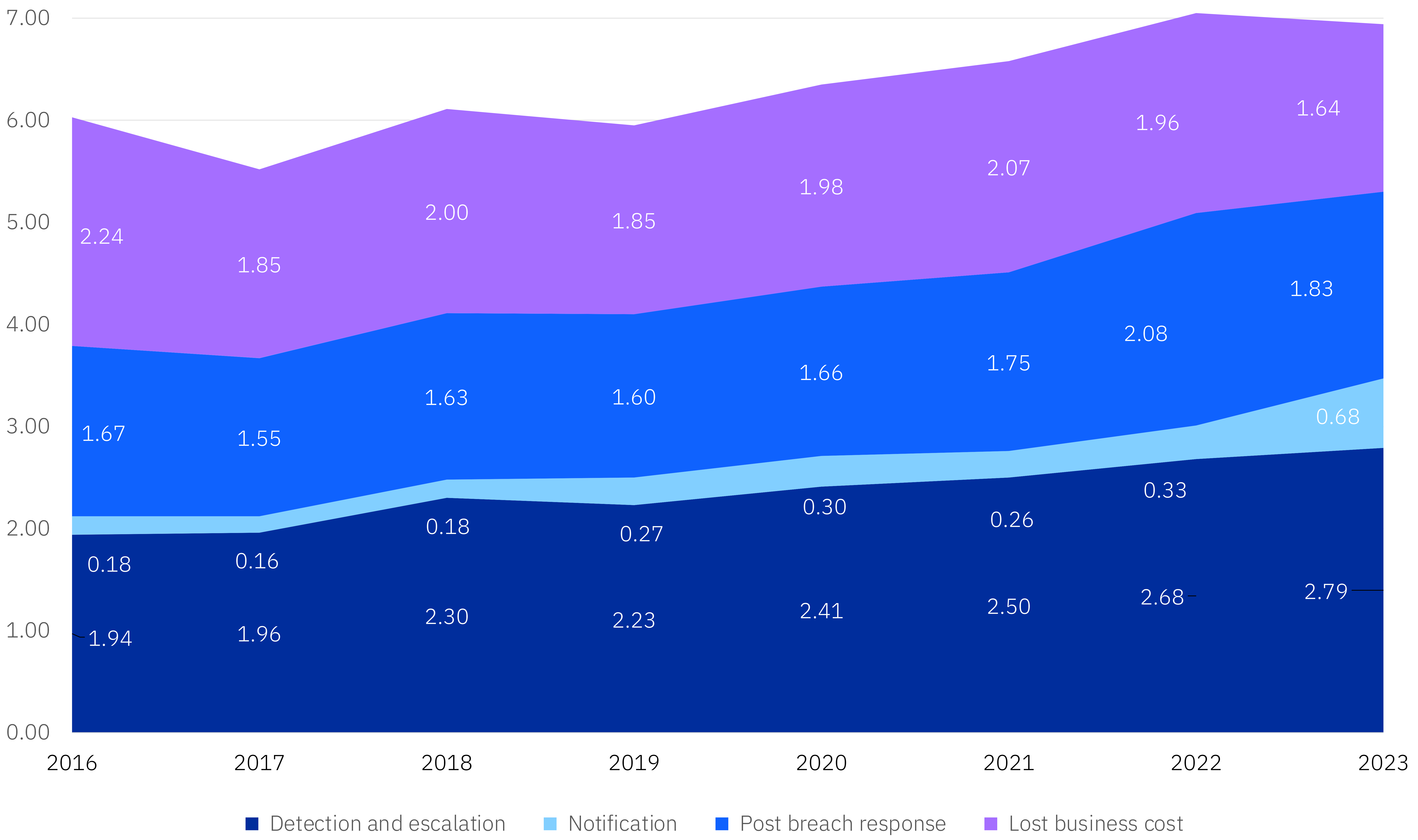
Time to identify and contain

Public industry



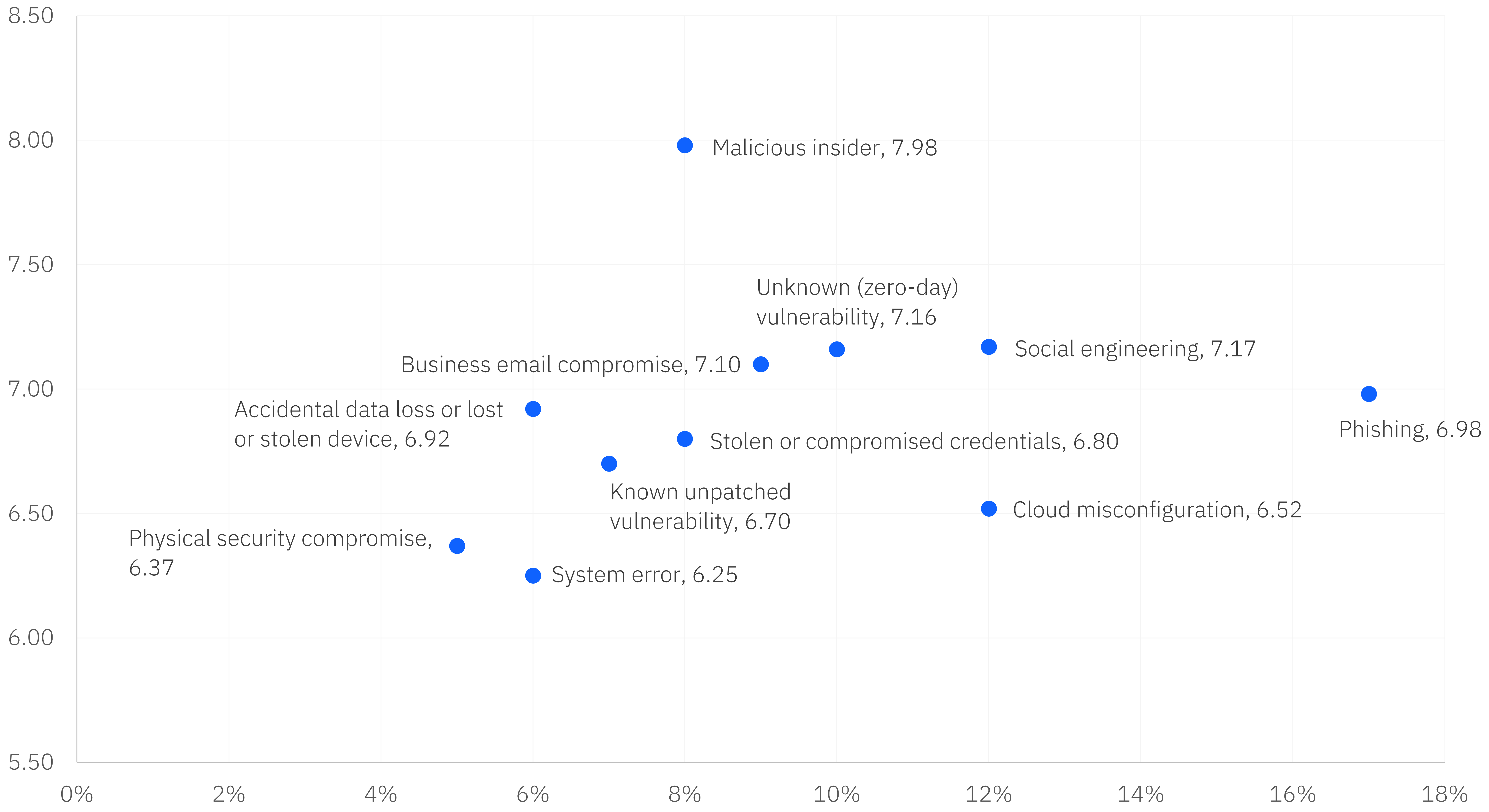
Total cost of a data breach in four categories

Measured in
CAD millions



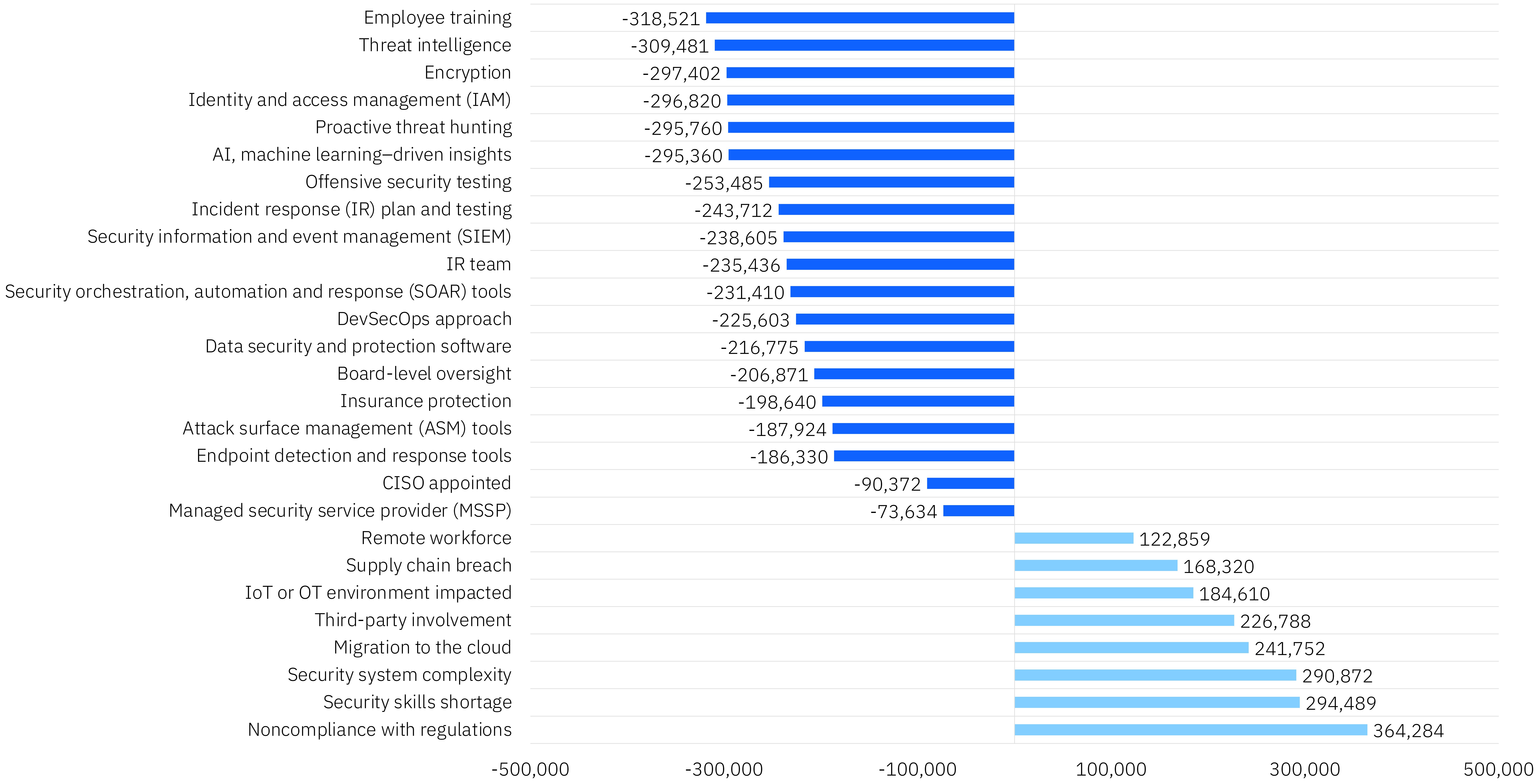
Total cost and frequency of data breaches by initial attack vector

Measured in CAD millions



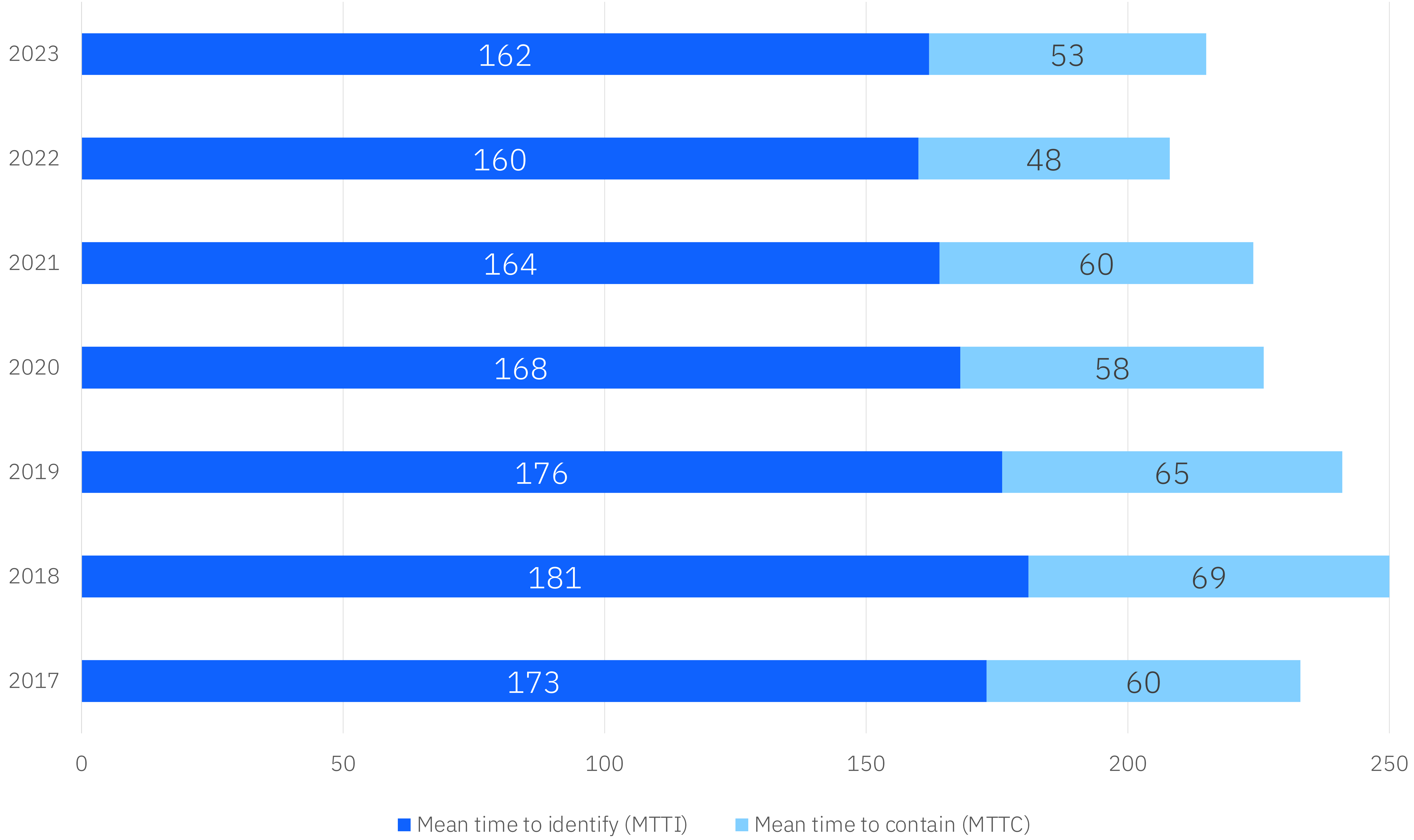
Factors that may increase or reduce the cost of a data breach

Measured in CAD



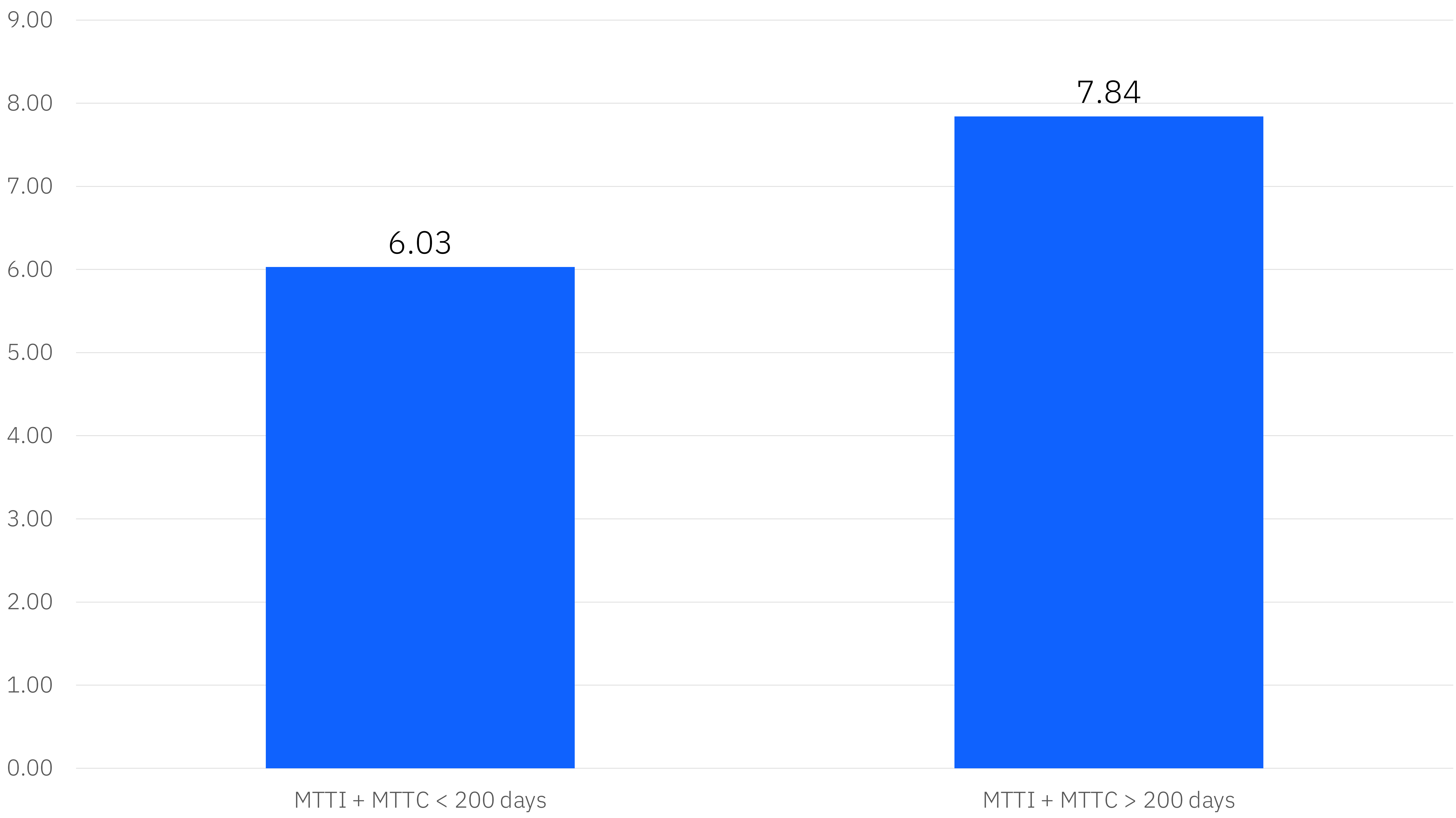
Time to identify and contain a data breach

Measured in days

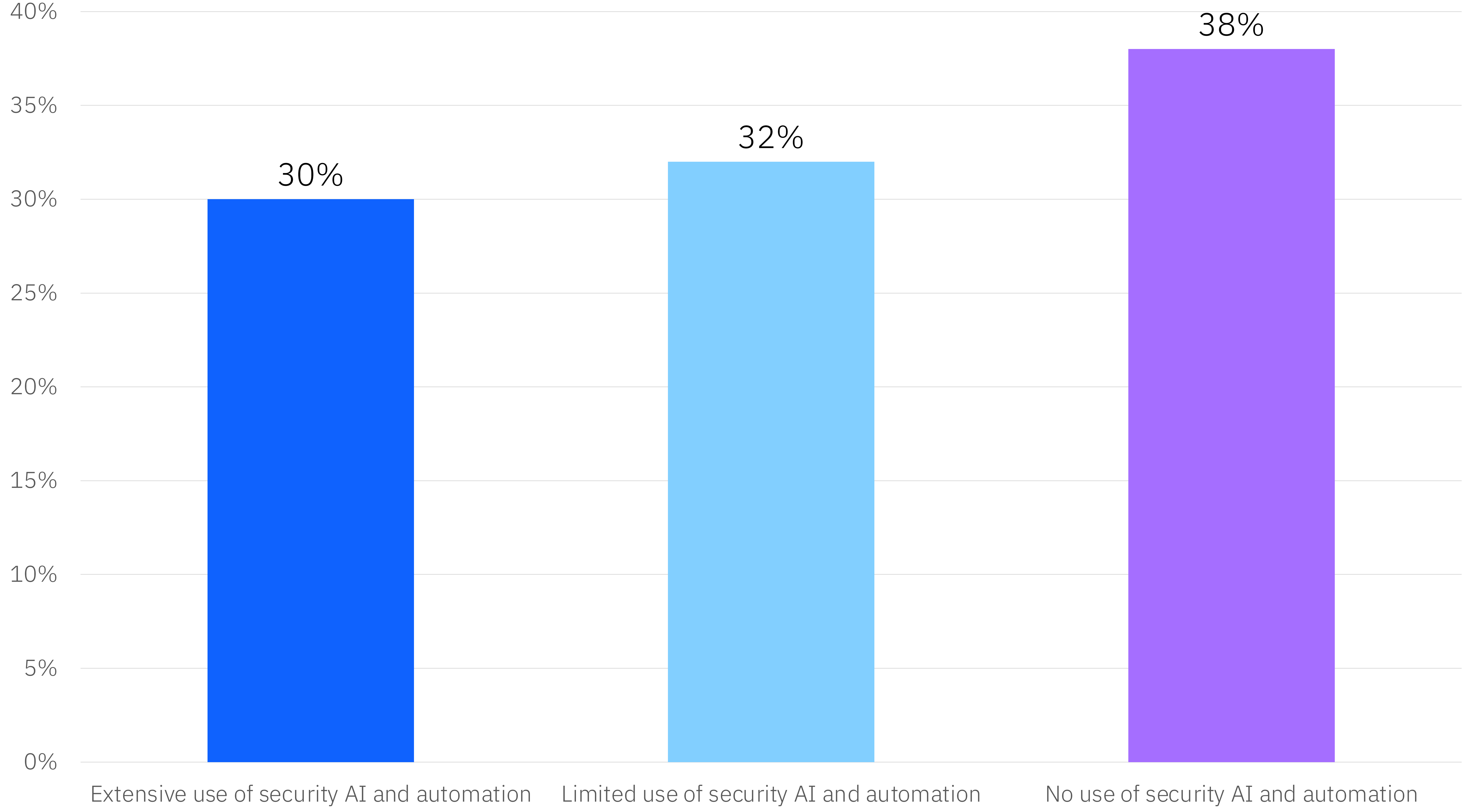


Total cost of a data breach based on the breach lifecycle

Measured in CAD millions

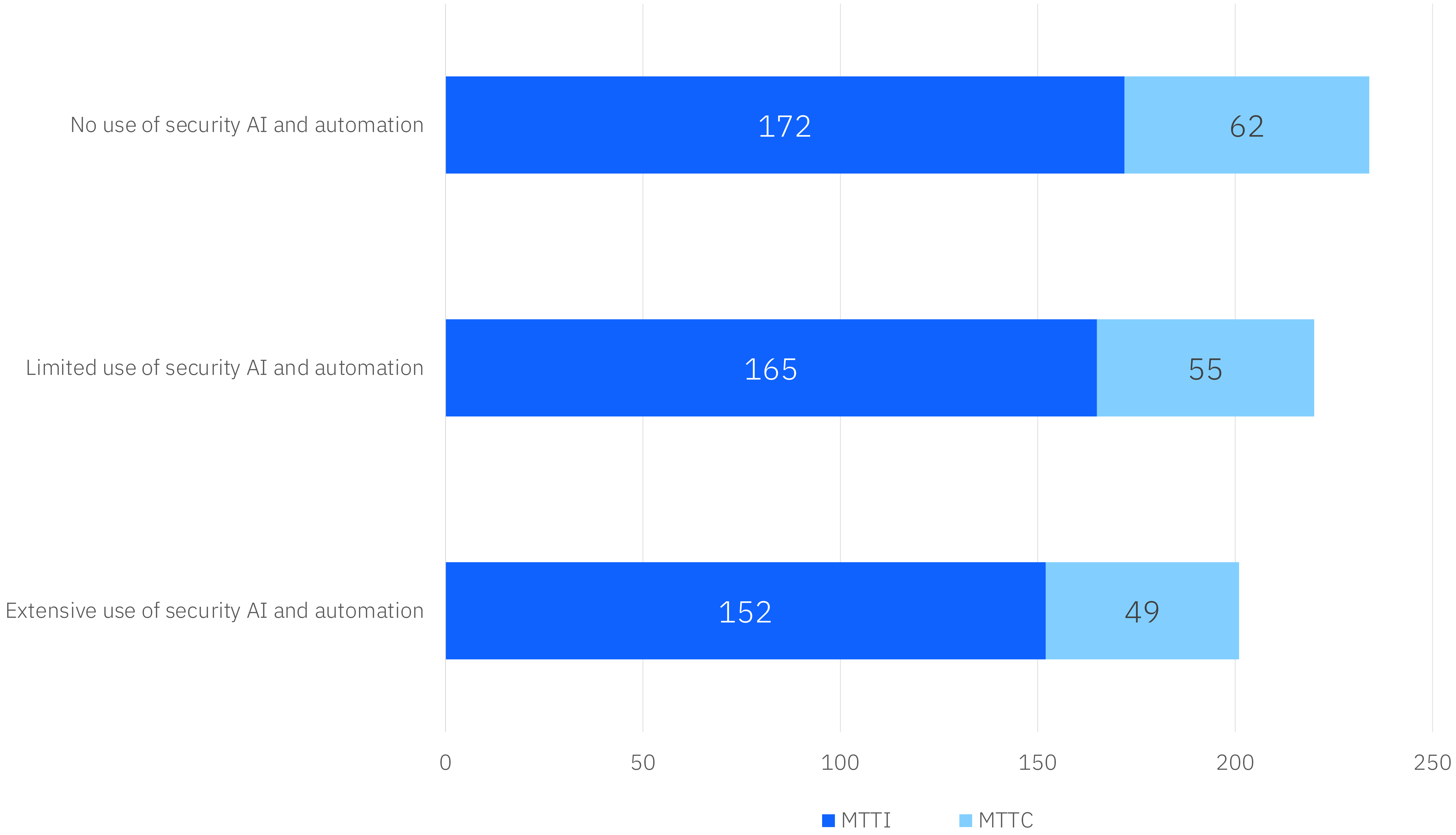


State of security AI and automation comparing three levels of deployment



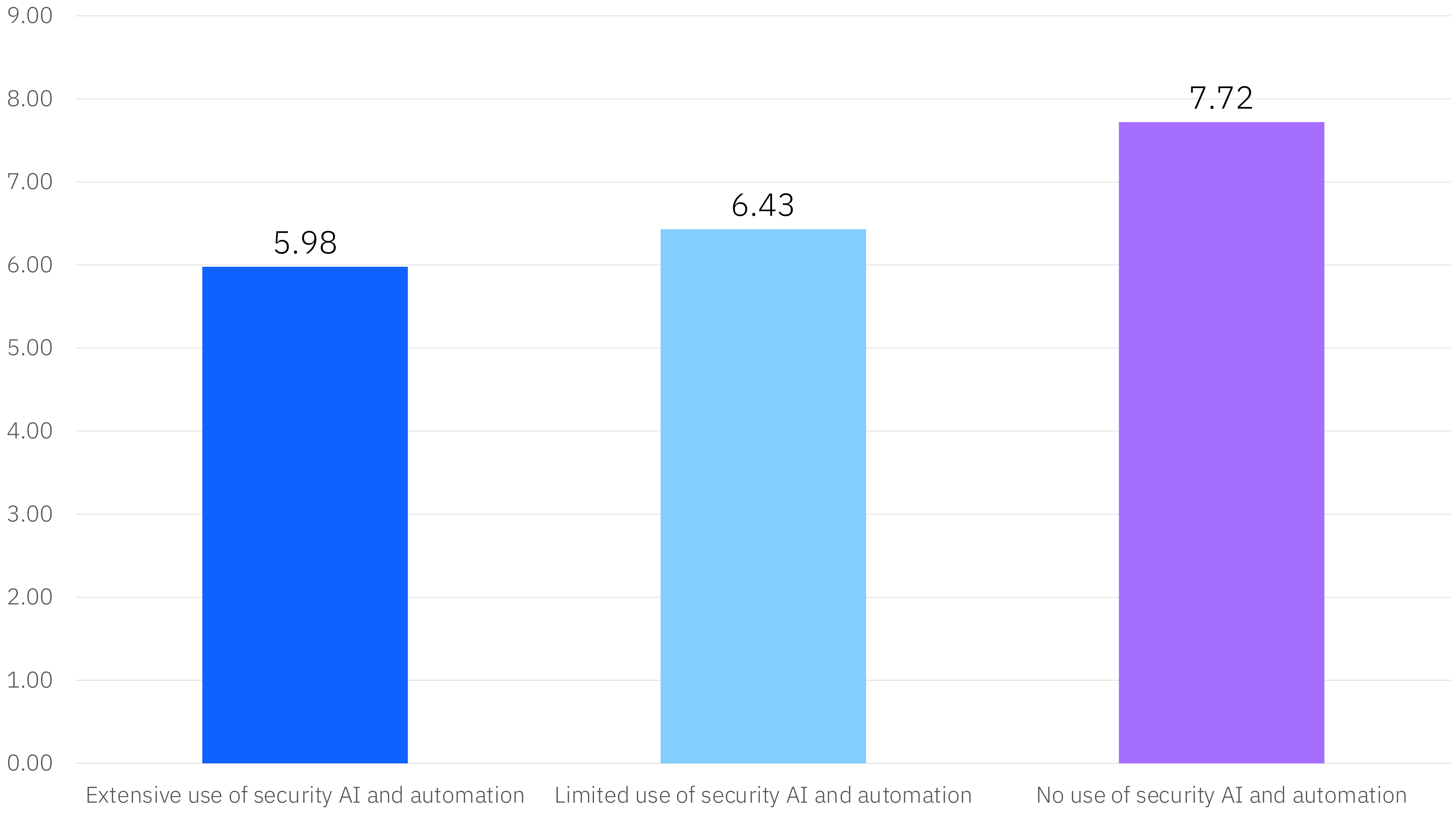
Time to identify and contain a data breach by level of security AI and automation

Measured in days



Cost of a data breach by security AI and automation deployment level

Measured in CAD millions



Recommendations

The following recommendations are actions you should take to secure your organization against malicious threats, including those presented in the report.

Action items:

- □ Manage your assets
- □ Know your adversary
- □ Manage visibility
- □ Challenge assumptions
- □ Act on intelligence
- □ Be prepared

Manage your assets:
"What do we have? What are we defending? What data is critical to our business?" These are the first questions any security team should answer to build a successful defense. Prioritizing discovery of assets on your perimeter, understanding your exposure to phishing attacks and reducing those attack surfaces further contribute to holistic security. Finally, organizations must extend their asset management programs to include source code, credentials and other data that could already exist on the internet or dark web.

Know your adversary:
While many organizations have a broad view of the threat landscape, X-Force recommends organizations adopt a view that emphasizes the specific threat actors that are most likely to target your industry, organization and geography. This perspective includes understanding how threat actors operate, identifying their level of sophistication, and knowing which tactics, techniques and procedures attackers are most likely to employ.

Manage visibility:
After understanding more about the adversaries most likely to attack, organizations must confirm they have appropriate visibility into the data sources that would indicate an attacker's presence. Maintaining visibility at key points throughout the enterprise and ensuring alerts are generated and acted on in a timely manner are critical to stopping attackers before they can cause disruption.

Recommendations

Challenge assumptions:
Organizations must assume that they already have been compromised. By doing so, teams can continually reexamine the following:

- How attackers can infiltrate their systems
- How well their detection and response capabilities fare against emerging tactics, techniques and procedures
- The level of difficulty for a likely adversary to compromise your most critical data and systems

The most successful security teams perform regular offensive testing including threat hunting, penetration testing and objective-based red teaming to detect or validate opportunistic attack paths into their environments.

Act on intelligence:
Apply threat intelligence everywhere. Effective application of threat intelligence will enable you to analyze common attack paths and identify key opportunities for mitigating common attacks, in addition to helping develop high-fidelity detection opportunities. Application of threat intelligence should be coupled with understanding your adversaries and how they operate.

Be prepared:
Attacks are inevitable; failure doesn’t have to be. Organizations should develop incident response plans customized for their environment. Those plans should be regularly drilled and modified as the organization changes, with a focus on improving response, remediation and recovery time.

Having a reputable IR vendor on retainer reduces the amount of time it takes to get skilled responders focused on mitigating an attack. Additionally, including your IR vendor in response plan development and testing is critical and contributes to a more effective and efficient response. The best IR plans include a cross-organizational response, incorporate stakeholders outside of IT and test lines of communication between technical teams and senior leadership. Finally, testing your plan in an immersive, high-pressure cyber range exercise can greatly enhance your ability to respond to an attack.

Thank you.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
July 2023

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

All client examples cited or described are presented as illustrations of the manner in which some clients have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual client configurations and conditions. Generally expected results cannot be provided as each client's results will depend entirely on the client's systems and services ordered. It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs. THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

IBM