RIDGE CANADA

CLIA Cyber Insurance
2024/2025 Outlook

DISCLAIMER

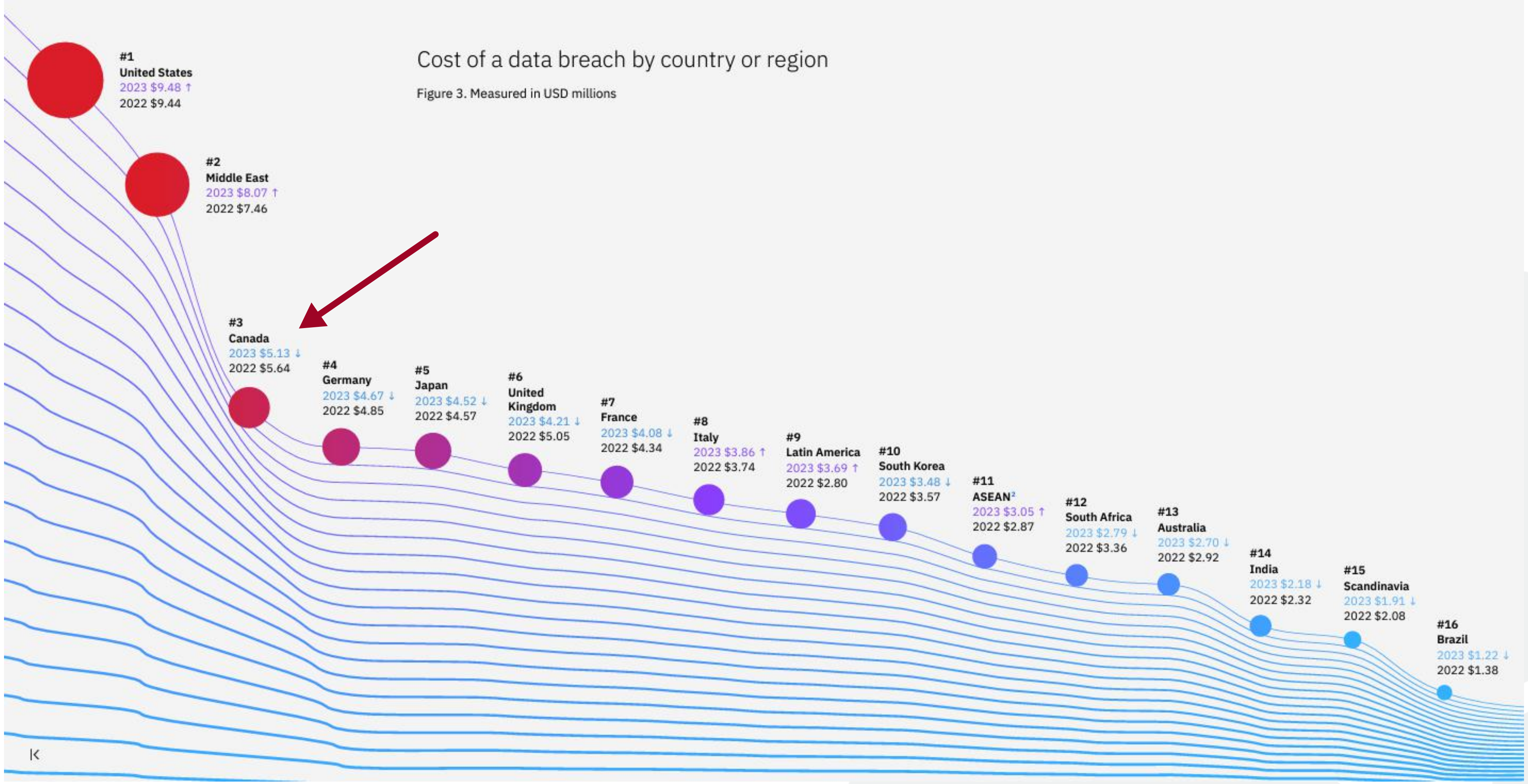
This presentation contains general information only and is not intended to provide an overview of coverages. The information is not intended to constitute legal or other professional advice. Please refer to insurer's policy wordings for actual terms, conditions, exclusions and limitations on coverage that may apply.

RIDGE
CANADA

The Last Two Years At A Glance

Overall Landscape

Landscape

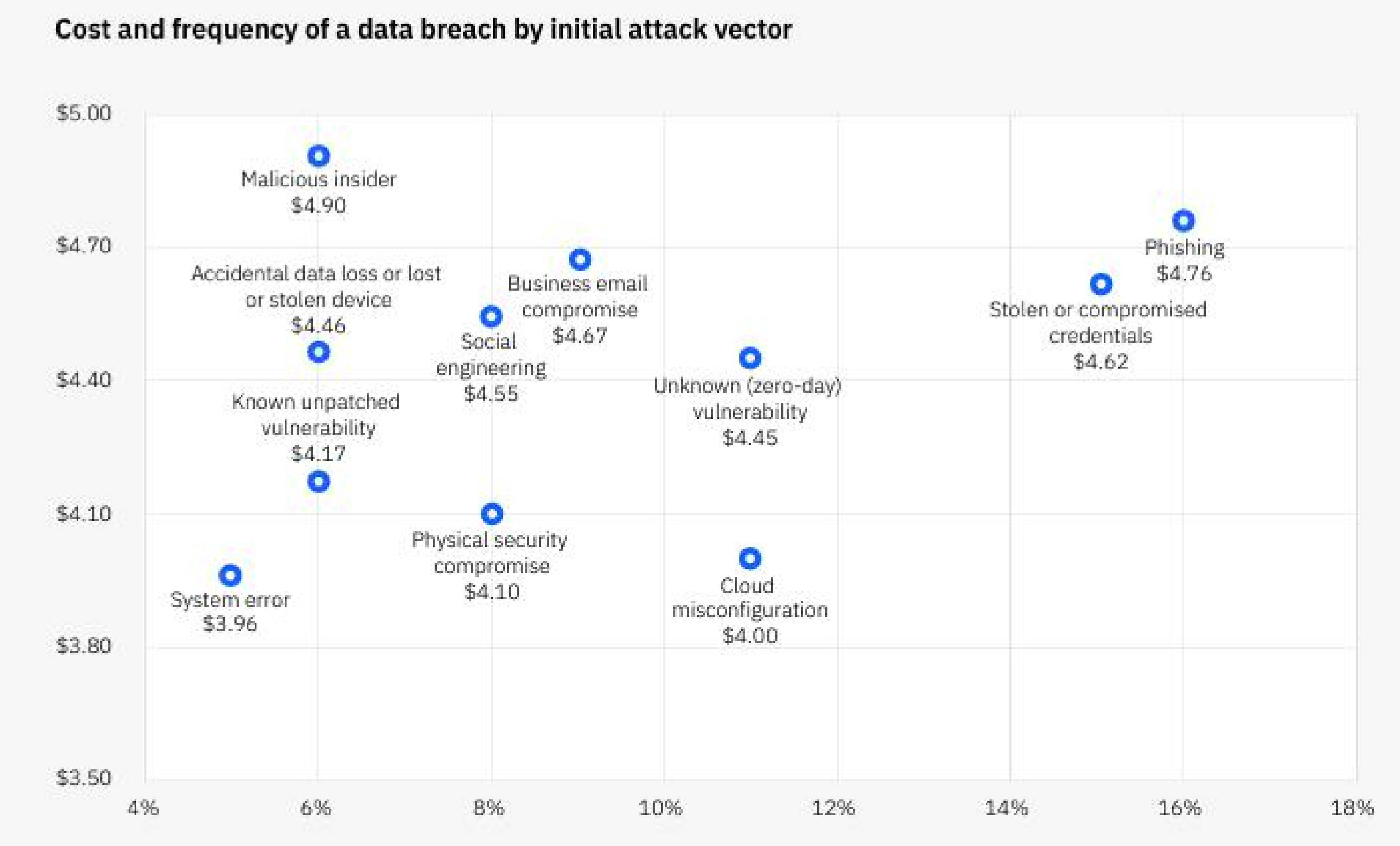


Cost of a data breach by country or region

Figure 3. Measured in USD millions

Source: Cost of a Data Breach Report 2023, https://www.ibm.com/downloads/cas/E3G5JMBP

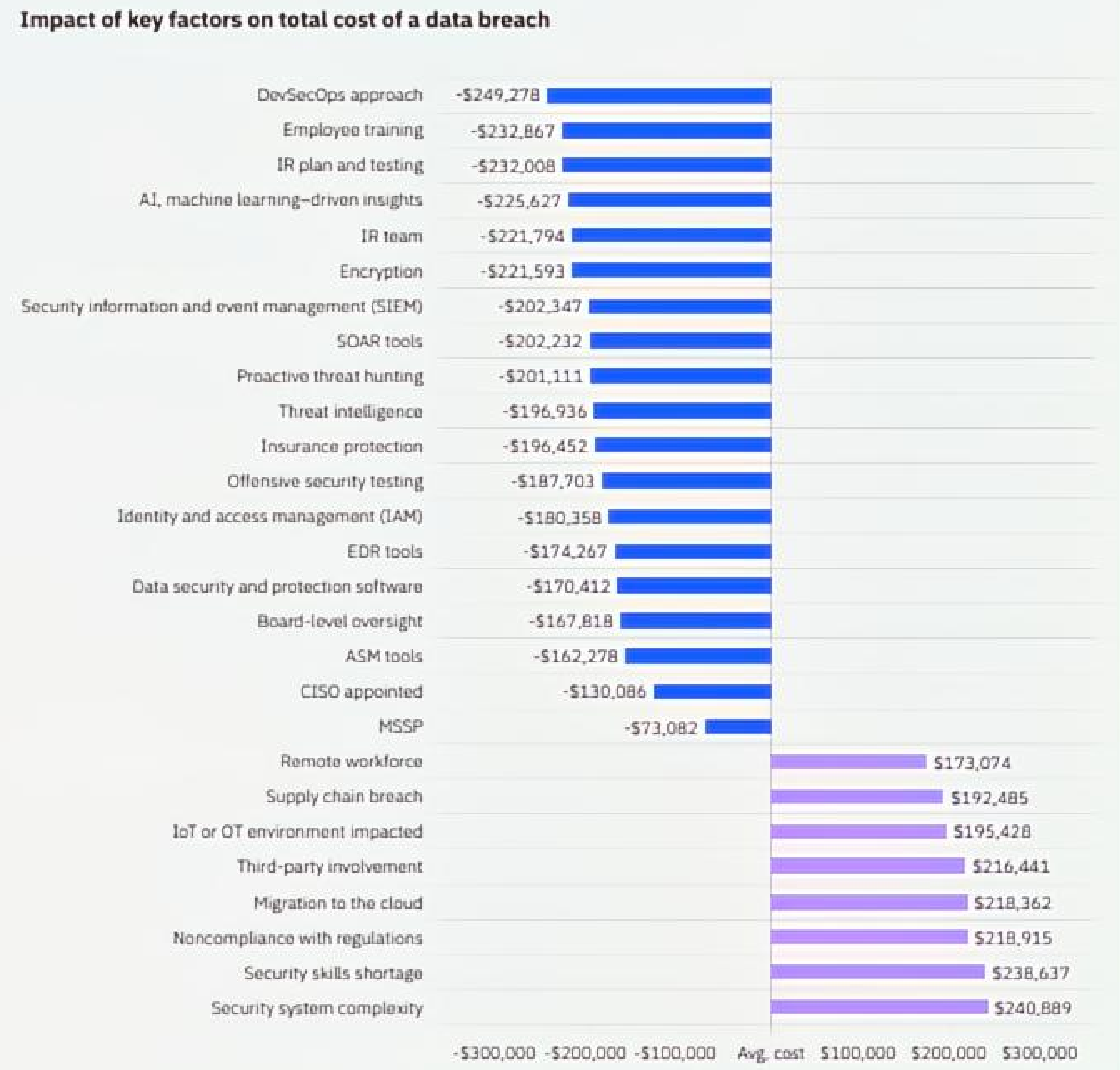
Landscape



Source: Cost of a Data Breach Report 2023, https://www.ibm.com/downloads/cas/E3G5JMBP

Landscape

- Control requirements for program continue to show full value against loss mitigation and cost control
- Two of top three security controls are extremely low cost to implement
- Very effective against main cause of loss across the CLIA program

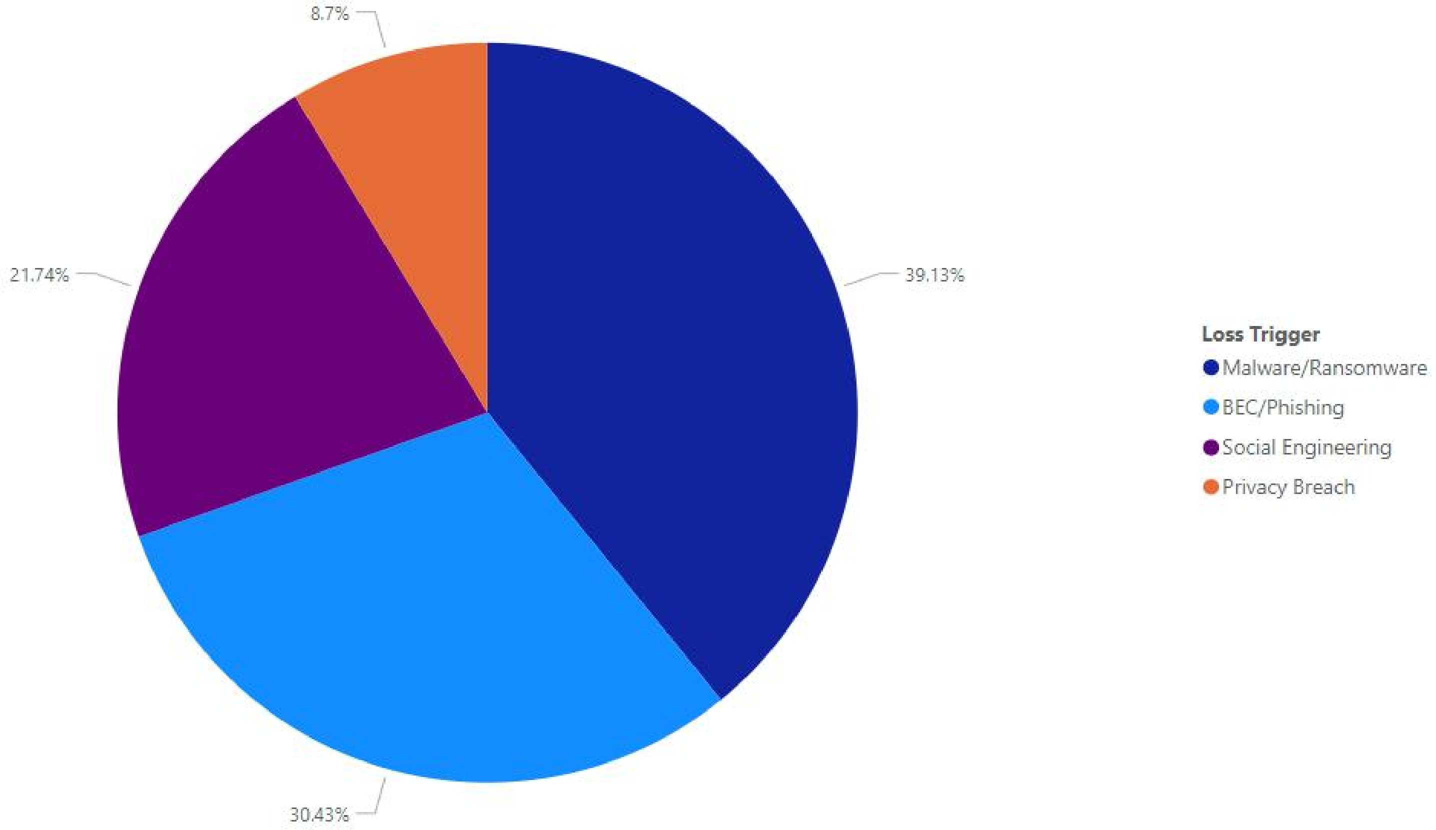


Impact of key factors on total cost of a data breach

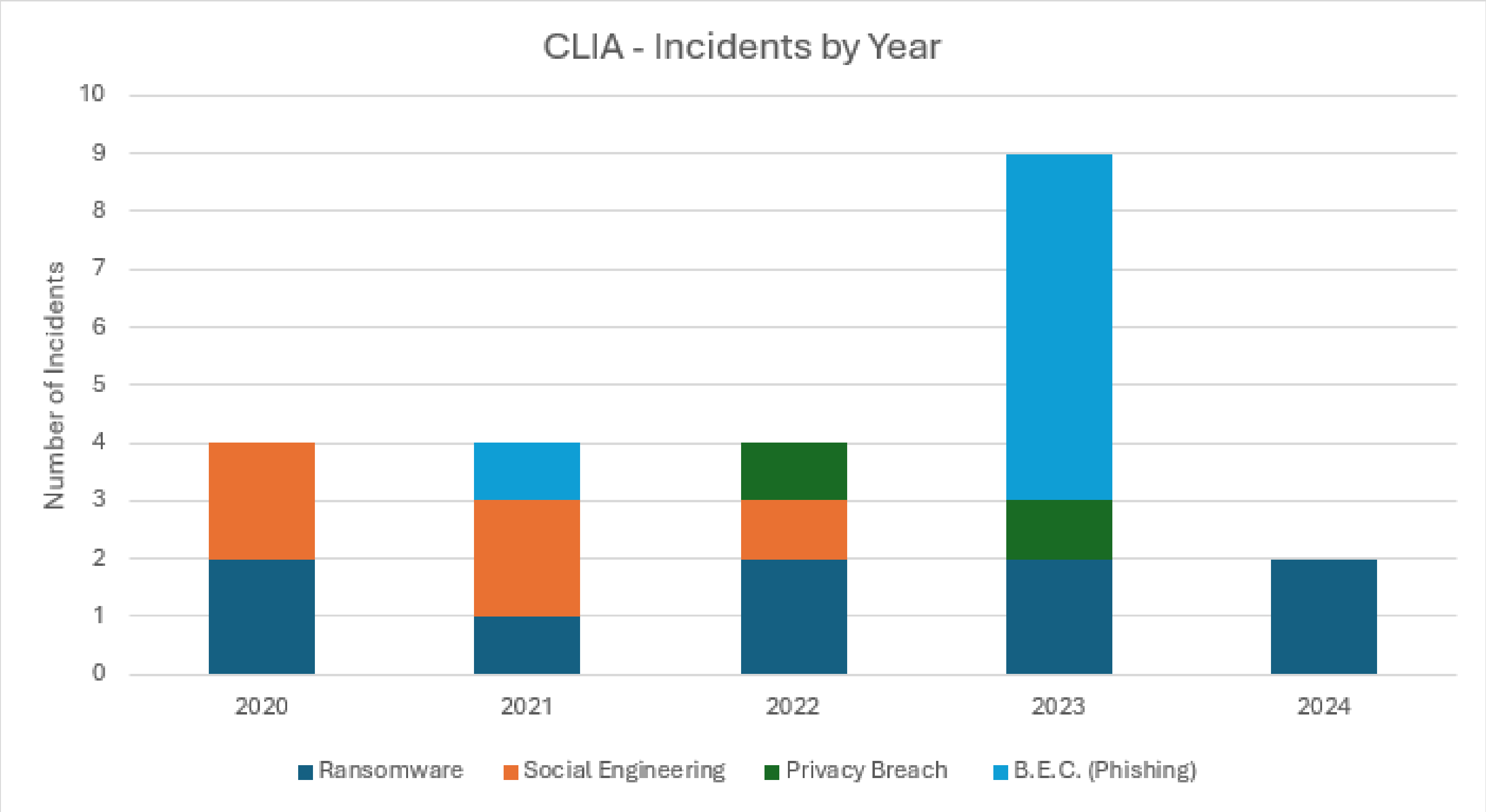
Source: Cost of a Data Breach Report 2023, https://www.ibm.com/downloads/cas/E3G5JMBP

Loss Impact

Count of YOA by Loss Trigger

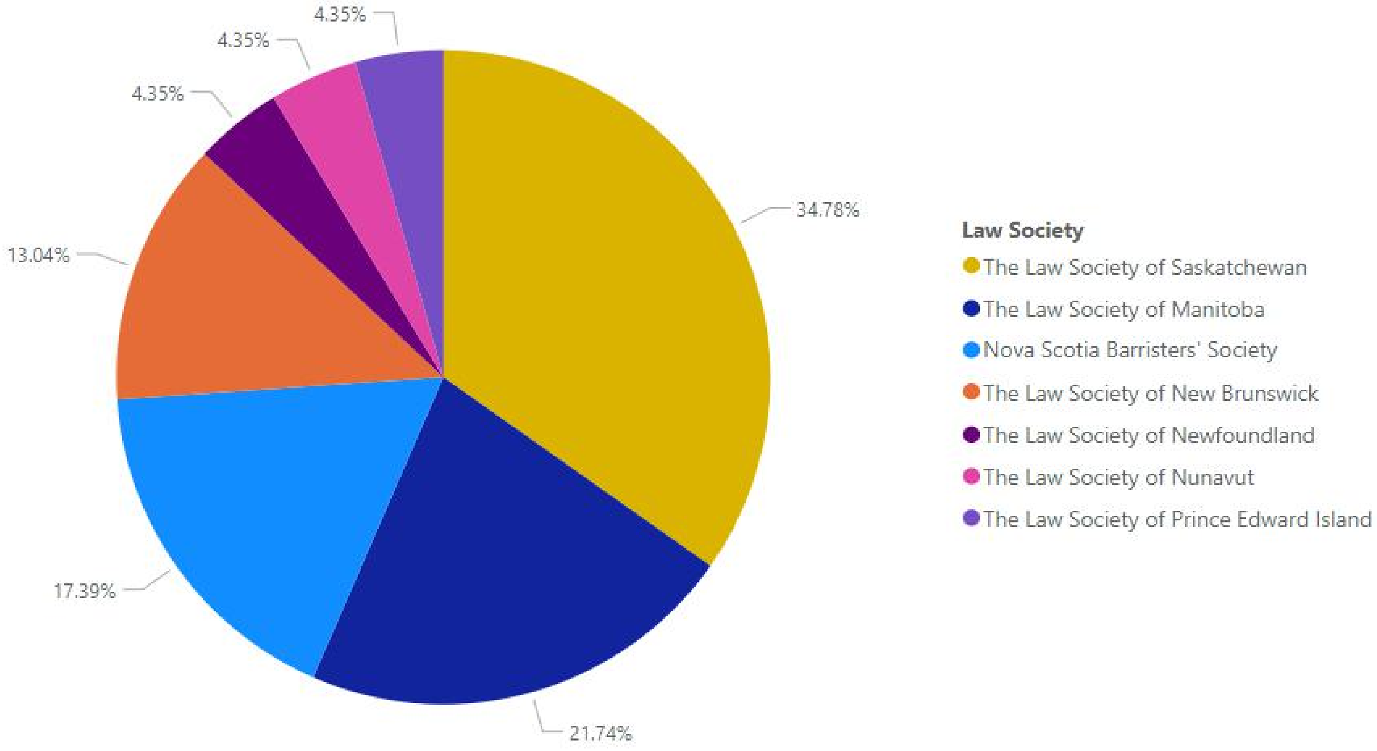


Loss Impact


CLIA - Incidents by Year
Number of Incidents
10
9
8
7
6
5
4
3
2
1
0
2020
2021
2022
2023
2024
Ransomware
Social Engineering
Privacy Breach
B.E.C. (Phishing)

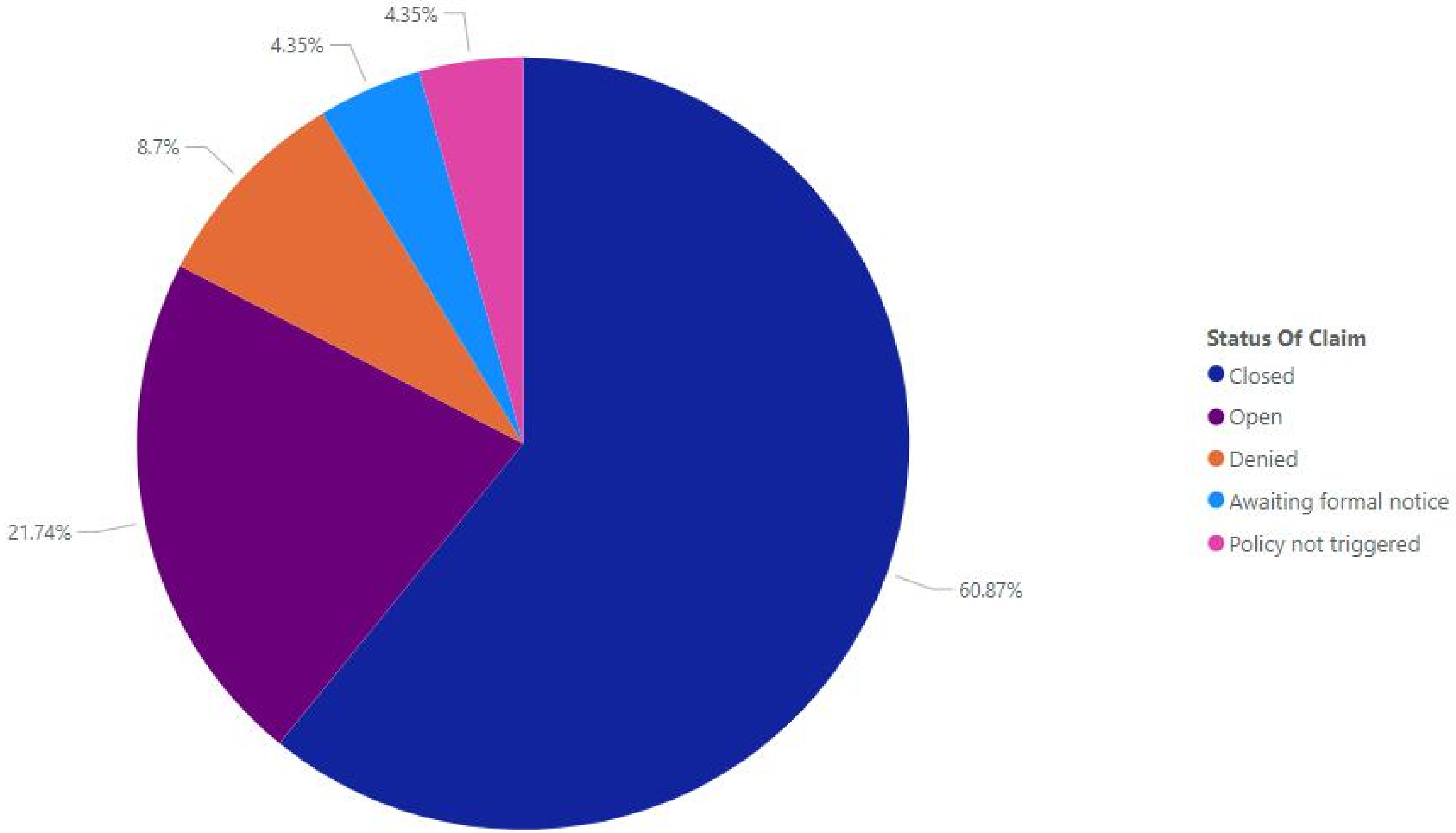
Loss Impact

Program Claim Count by Law Society

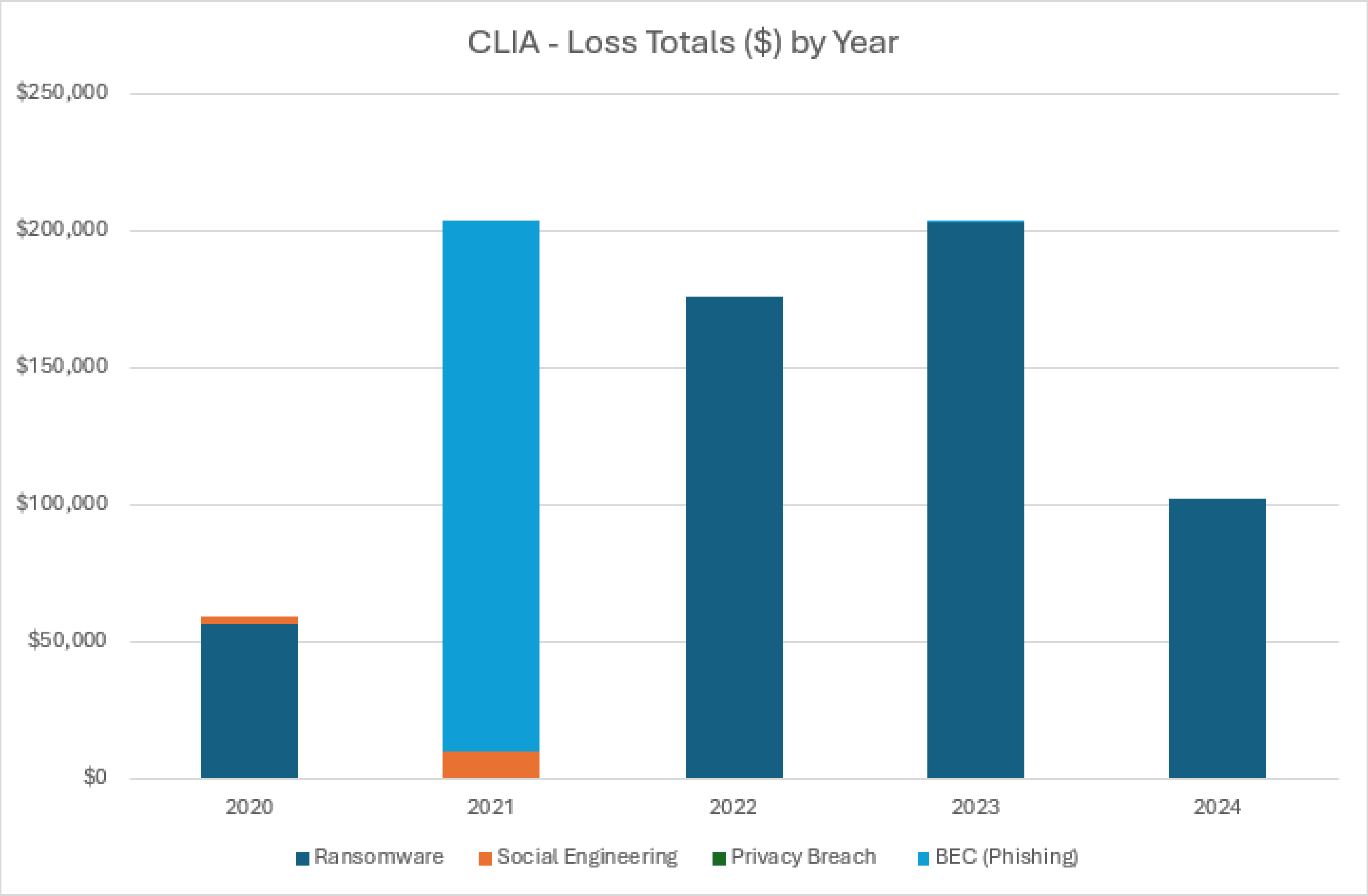


Loss Impact

Count of YOA by Status Of Claim



Loss Impact

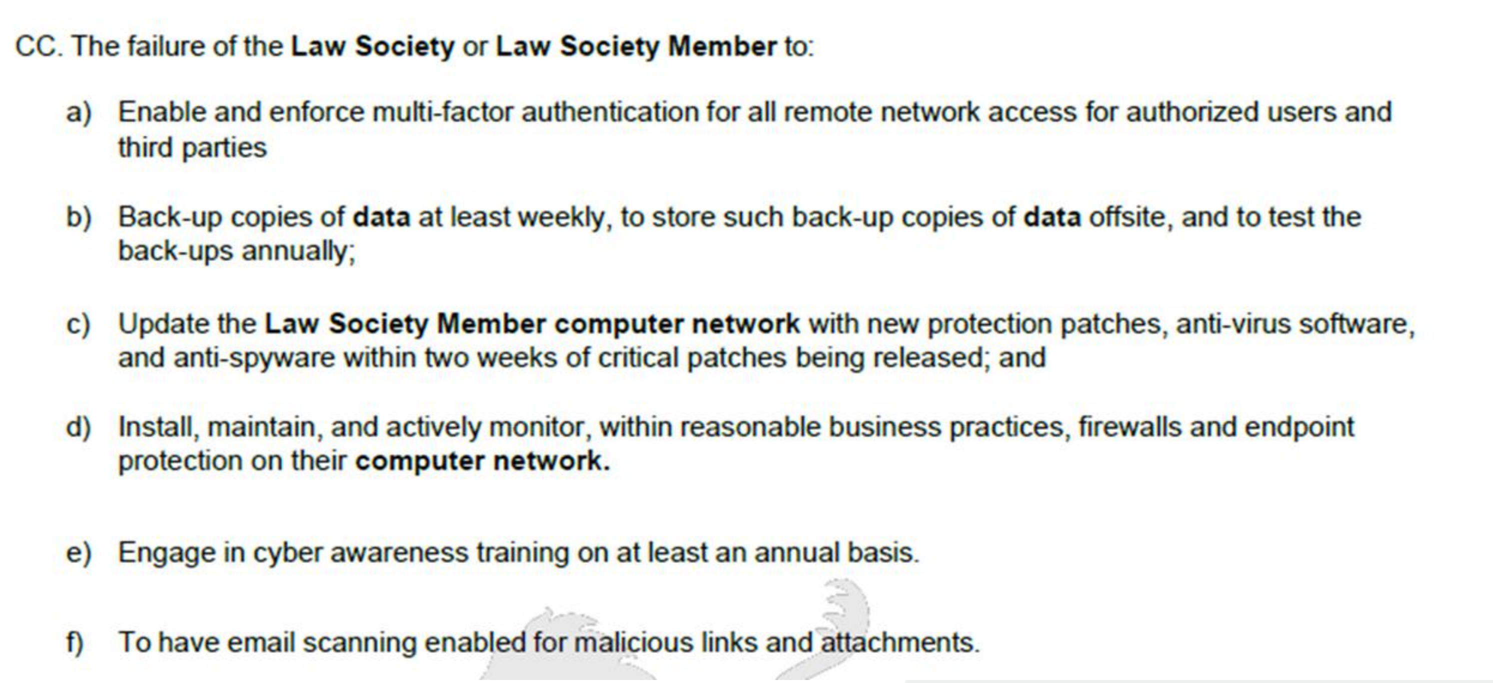

CLIA - Loss Totals ($) by Year
$250,000
$200,000
$150,000
$100,000
$50,000
$0
2020
2021
2022
2023
2024
Ransomware
Social Engineering
Privacy Breach
BEC (Phishing)

Upcoming Year

Minimum Hygiene Requirements

We have known certain measures and controls to be very effective against threat actors, and against attack patterns that are targeting law firms. Firms have sensitive information, and customer dollars in trust. You are targets.

- Hygiene requirements to bring a claim are:



CC. The failure of the **Law Society** or **Law Society Member** to:

a) Enable and enforce multi-factor authentication for all remote network access for authorized users and third parties

b) Back-up copies of **data** at least weekly, to store such back-up copies of **data** offsite, and to test the back-ups annually;

c) Update the **Law Society Member computer network** with new protection patches, anti-virus software, and anti-spyware within two weeks of critical patches being released; and

d) Install, maintain, and actively monitor, within reasonable business practices, firewalls and endpoint protection on their **computer network.**

e) Engage in cyber awareness training on at least an annual basis.

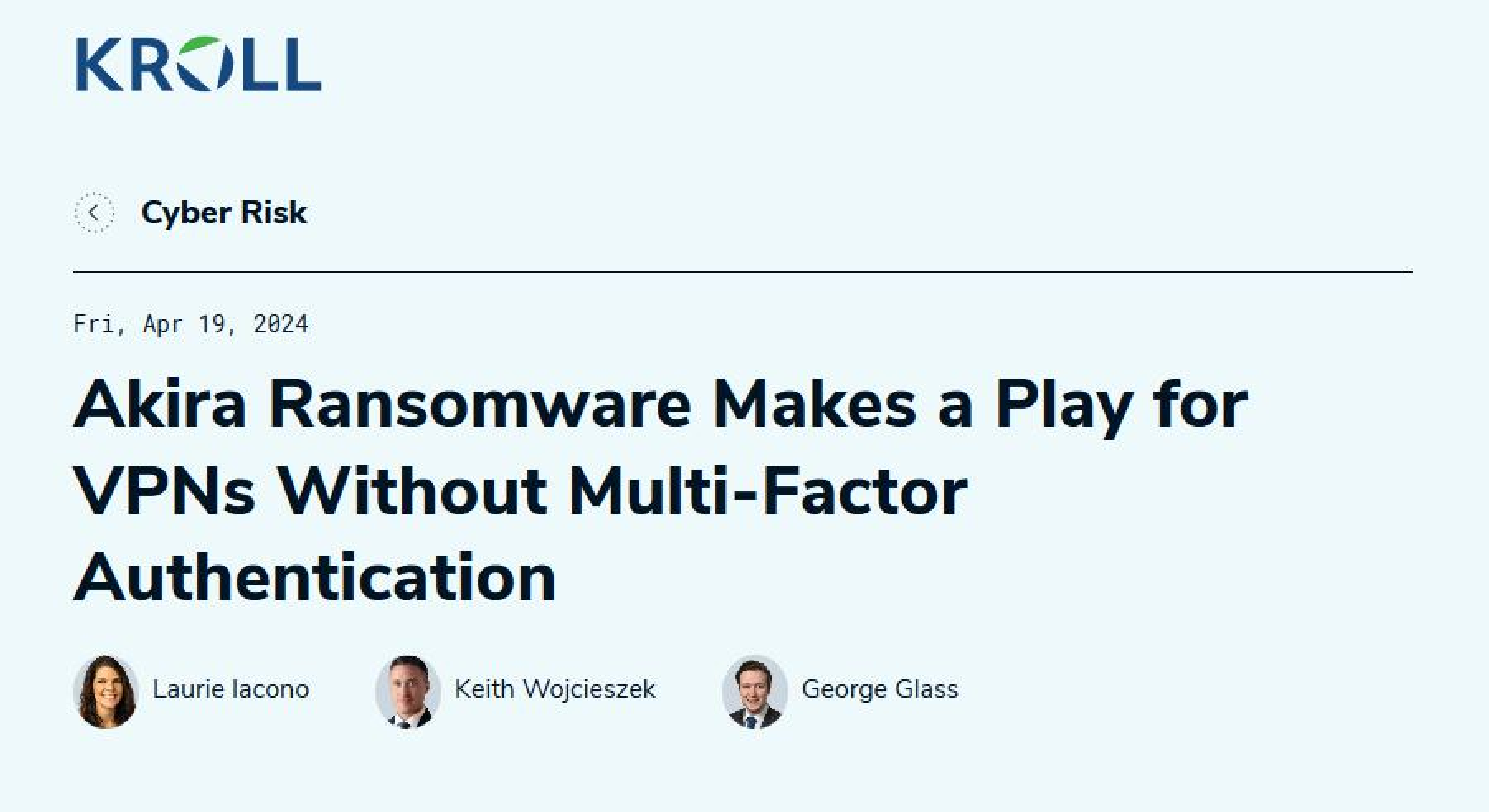
f) To have email scanning enabled for malicious links and attachments.

Status Update

Rates have stabilized (for the time being) across the Canadian landscape in target sectors that have performed well historically. Reinsurance rates anticipated to increase in early 2025 based on overall industry loss ratios.

- The incidence rate is up significantly over the past year, and we have seen the frequency impact continue into 2024 term (post July 1)
- Severity on total limits is also ticking up, as ransomware continues to be a scourge
- A firm can do everything correctly and still fall victim to ransomware - there are no silver bullets!
- Akira and BlackBasta are active ransomware groups who are impacting small firms across Canada via different attack patterns

Active Threats



Cyber Risk

Fri, Apr 19, 2024

Akira Ransomware Makes a Play for VPNs Without Multi-Factor Authentication

Laurie Iacono   Keith Wojcieszek   George Glass

Source: https://www.kroll.com/en/insights/publications/cyber/akira-ransomware-deep-dive

Active Threats

Who Is Black Basta?

Black Basta (AKA BlackBasta) is a ransomware operator and Ransomware-as-a-Service (RaaS) criminal enterprise that first emerged in early 2022 and immediately became one of the most active RaaS threat actors in the world, racking up 19 prominent enterprise victims and more than 100 confirmed victims in its first few months of operation. Black Basta targets organizations in the US, Japan, Canada, the United Kingdom, Australia, and New Zealand in highly targeted attacks rather than employing a spray-and-pray approach. The group's ransom tactics use a double extortion tactic, encrypting their victim's critical data and vital servers and threatening to publish sensitive data on the group's public leak site.

Black Basta's core membership is thought to have spawned from the defunct Conti threat actor group due to similarities in their approach to malware development, leak sites, and communications for negotiation, payment, and data recovery. Black Basta has also been linked to the FIN7 (AKA Carbanak) threat actor through similarities in their custom Endpoint Detection and Response (EDR) evasion modules and overlapping use of IP addresses for command and control (C2) operations.

Source: https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/black-basta

What to Expect

Insurance markets that make commercial decisions to seize market share will be left in the same state as we were heading into 2021, as the loss patterns have not materially shifted. However, the frequency has increased, and is expected to increase further.

Attribution on threat actors continues to be comically low. The evolution of our legislation relating to this particular risk to Canadian business has also not moved since 2018, and in the short term - looks only to impact critical infrastructure (C-26)

Consolidation and the push for market share has started to impact known forensics vendor rate cards. Computer Forensics costs have increased slightly, but we have seen a large increase in rates for uninsured losses. Having access to predetermined rates, regardless of coverage, will be more of an advantage into 2025.

☎ 1-(647)-643-4737

✉ contact@ridgecanada.com

🌐 www.ridgecanada.insure

📍 8 King Street East, Suit 205
Toronto, ON, M5C 1B5

RIDGE™
CANADA