CYBERMINUTE
Alberta Cybersecurity Insights

TLP: WHITE

2023 CyberAlberta Year In Review

In 2023, the cyber threat landscape evolved significantly, with new threats and tactics emerging and known threats morphing. To match these changes the CyberAlberta Community of Interest (COI) has seen its own evolution, experiencing significant growth and increased collaboration, leading to more frequent meetings. A clear interest during these meetings has been exploring new trends in cybersecurity as a collective, ranging from discussions on the impacts and benefits of quantum computing to the remedying of the cybersecurity skill gap via advances made in the Work Experience Program and broader distribution of cyber awareness tools.

As of 31 December 2023, CyberAlberta has:
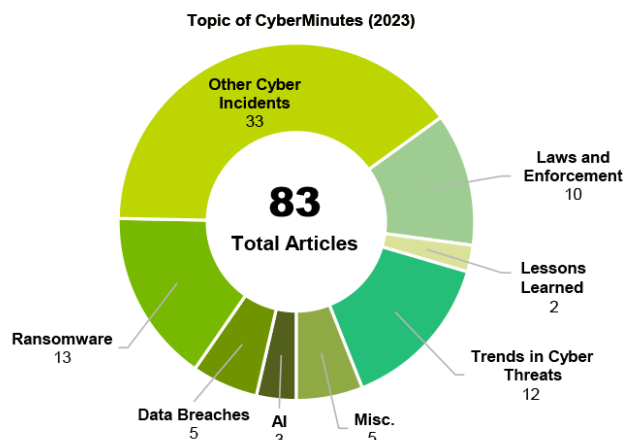
311 members representing **194** organizations

Some trends in cybersecurity explored during COI meetings and via threat intelligence distributed by CyberAlberta include:

- Advancements in **artificial intelligence (AI)** shone a light on new threats for the COI to consider—such as less tech savvy threat actors using AI to assist writing malware—and highlighted how old threats could have new life breathed into them—such as AI voice cloning being used to give credence to a vishing call. The COI explored some of these threats during a presentation on AI personas and simulacra, highlighting some of the ways AI could be leveraged to manipulate individuals and organizations.

- **Ransomware** continues to be one of the most prevalent types of cyber attacks; however, 2023 saw changes in how it was implemented. In January, Hive Ransomware was seized by the FBI and several other seizures occurred through the year. Apparently in response, the threat actors have evolved their tactics, now relying more heavily on double-extortion methods when executing ransomware attacks.

- There were several large-scale **supply chain attacks** this year. Both the MOVEit vulnerability and the breach that saw 24 years of Government of Canada data leaked were the result of threat actors exploiting vulnerabilities that impacted a third-party. The impacts of the MOVEit

Topic of CyberMinutes (2023)

83 Total Articles

- Other Cyber Incidents 33
- Laws and Enforcement 10
- Lessons Learned 2
- Trends in Cyber Threats 12
- Misc. 5
- AI 3
- Data Breaches 5
- Ransomware 13

vulnerability are still being realized, but as of the end of 2023 between 85.1-89.9 million individuals were victimized as a result.

- **New regulations** were implemented in the USA, aligning with their Cybersecurity Strategy, increasing government oversight relating to how organizations handle and prepare for cyber incidents. Similar legal changes are continuing to be considered in Canada, with Bill C-26, an Act Respecting Cyber Security, still on the table.
- Measures that can be taken to **mitigate potential impacts** were some of the most discussed topics in 2023. Employee and organizational cyber hygiene—ranging from things such as training to having patching/updating schedules in place—and cyber preparation – such as incident and disaster response plans being created and tested—were found to be two of the biggest indicators of how much of an impact a cyber incident had on an organization.

Topics of AdHoc CyberAlberta Reports (2023)

New Threat Vectors 3

Exploited Vuln. 2

8 Total Reports

Ongoing Cyber Incidents 3

What this year holds for cyber threats is still being revealed, but experts speculate that many of the same trends we have seen in 2023 will continue and develop in 2024. Known threats, SIM swapping and social media hacking have been seen extensively in January, but newer threats, such as drainers-as-a-service are also on the rise.

To face the threats the new year will throw, CyberAlberta plans to continue collaborating with the wider Albertan landscape to enhance cybersecurity in the province. This includes developing awareness materials for K-12 education and other vulnerable sectors, with the area having made strides in 2023 due to the relationship established with the Alberta Technology Leaders in Education (ATLE). Also on the docket, are plans to continue developing the Cybersecurity Control Framework to help small-to-medium size businesses understand their risks. Lastly, the creation of a Shared Procurement model service to help COI members leverage the Government's buying power for securing their organization's information assets is in development, aiming for release in 2024.

CyberAlberta received **52** COI member requests in 2023, ranging from incident assistance to cybersecurity documentation requests.

In exciting news, CyberAlberta also made strides in its engagement strategy in 2023, transitioning from the EngagementHQ platform to a SharePoint Online site, and now to its own website—www.cyberalberta.ca—going live on February 7th, 2024! This site will serve as a primary cybersecurity information repository for Alberta organizations, hosting a range of resources aimed at improving all of Alberta's cyber stance.