CAA-2026-0012 Cyber Preparedness for Alberta Organizations Amid Iran-Linked Threats

Summary

Current geopolitical tensions involving Iran have increased the overall risk of cyber activity conducted by Iran-linked threat actors. While direct targeting of Alberta organizations remains less likely than for organizations operating in the Middle East, heightened activity of Iran-linked cyber actors increases the probability of opportunistic cyber attacks, indirect impacts, and supply chain disruption. Alberta organizations should take defensive measures to reduce exposure.

Details

Iran-linked threat actors are actively conducting cyber operations intended to disrupt the assets of the United States (U.S), Israel, and their regional partners. This activity has expanded to include countries that publicly support actions taken against Iran.[1] Canada has publicly expressed support for U.S. and Israeli military strikes on Iran[2] while condemning retaliatory actions by Iran and Hezbollah, increasing the likelihood that Canada may be viewed as a secondary target.[3]

Since the initial military strikes on 28 February 2026, Iranian-linked threat actors have claimed responsibility for cyberattacks targeting U.S. networks and critical infrastructure organizations.[4][5] While not all claims have been independently verified, they demonstrate sustained intent and capability and indicate that organizations, across multiple sectors may become targets during periods of heightened geopolitical tension. Iranian-linked media outlets have directly named several major U.S. technology companies—Google, Microsoft, Palantir, IBM, Nvidia, and Oracle—as intended targets.[6]

Assessment

CyberAlberta Threat Intelligence assesses that current geopolitical tensions likely pose an increased risk of cyber activity affecting Canadian and Albertan organizations. While the likelihood of direct impacts remains lower compared to those directly involved with, or near to, the current conflict, the overall risk is elevated due to increased Iranian cyber threat activity. Canadian and Albertan organizations with ties to the Middle East region face a higher risk of direct targeting. While those with a reliance on U.S. organizations and technology face a higher risk of having their own operations impacted by attacks disrupting their supply chain.

[1] https://www.intel471.com/blog/israeli-us-strikes-against-iran-triggers-a-surge-in-hacktivist-activity
[2] https://www.pm.gc.ca/en/news/statements/2026/03/03/statement-prime-minister-carney-evolving-situation-middle-east
[3] https://www.pm.gc.ca/en/news/readouts/2026/03/11/prime-minister-carney-participates-virtual-g7-leaders-meeting-situation
[4] https://thehackernews.com/2026/03/iran-linked-muddywater-hackers-target.html
[5] https://www.reuters.com/technology/stryker-shares-fall-after-report-suspected-iran-linked-cyberattack-2026-03-11/
[6] https://www.wired.me/story/war-on-big-tech-iran-names-israeli-linked-us-firms-as-potential-targets

Recommendations

Alberta-based organizations are advised to review their cybersecurity posture and consider the following actions:

Enhance cybersecurity awareness strategies
- Reinforce employee awareness of phishing and social engineering activity and ensure employees understand how to recognize and report suspected incidents.

Strengthen identity and access controls
- Implement phishing-resistant multi-factor authentication, especially for privileged and administrative accounts to reduce the risk of account compromise if credentials are exposed.
- Implement Privileged Identity Management to secure roles with access to critical systems and sensitive data.

Identify and inventory attack surface
- Maintain a complete and current inventory of systems, applications, cloud services, and third-party dependencies, especially for public-facing assets. Shadow IT remains a frequent entry point for adversaries and should be identified and addressed.
- Ensure public-facing industrial control systems and operational technology are inventoried, with internet access removed if unnecessary, and default credentials are changed.
- Apply security updates and patches promptly across all systems.[7]

Review disaster recovery plans, and incident response playbooks
- Review and test disaster recovery plans, business continuity plans, and communication plans to ensure rapid restoration of critical systems. Test incident response procedures for various cyber scenarios and include contingencies for both direct attacks and indirect impacts caused by partner or supply chain disruptions.

Review and apply cybersecurity best practices and advice
- Review and apply guidance and best practices published by CyberAlberta and the Canadian Centre for Cyber Security (CCCS) to strengthen defensive posture during this period of heightened risk.[8]
- Report suspected cyber activity to CyberAlberta and the CCCS.[9] [10]

[7] https://www.cyber.gc.ca/en/guidance/top-10-it-security-action-items-no2-patch-operating-systems-and-applications-itsm10096
[8] https://www.cyber.gc.ca/en/guidance/cyber-security-hygiene-best-practices-your-organization-itsap10102
[9] https://cyberalberta.ca/report-a-cyber-issue
[10] https://www.cyber.gc.ca/en/incident-management