Sophisticated Cyberattacks Surge Aided by AI Adoption According to CDW Canada Study

Amidst an increasingly sophisticated threat landscape, IT threat detection and response must be prioritized, with successful cybersecurity incidents up 26 percent from 2023 study

Toronto, ON – April 29, 2024

CDW Canada, a leading provider of technology solutions and services for Canadian organizations, today released its annual Canadian Cybersecurity Study, *Cybersecurity in Focus 2024: Trends, Threats and Strategies*, which explores the current state of cybersecurity among Canadian organizations. The study, sponsored by CDW Canada and conducted with additional support and analysis by IDC Canada, surveyed over 700 IT security, risk and compliance professionals.

The evolving threat landscape highlights a critical shift in 2024. Cyberattacks have decreased, however, the number of successful cyberattacks continues to rise. In the 2023 study, only 7 to 8 percent of cyberattacks escalated into cyberincidents, however, this steadily increased with 9 to 10 percent becoming incidents according to 2024 study findings. Canadian organizations must utilize effective solutions to combat these increasingly successful breaches.

AI has altered the cybersecurity landscape

Cyberattackers are leveraging AI and machine learning tools to orchestrate more successful attacks. AI has automated the process of finding vulnerabilities, enhancing cybercriminals' efficiency and reach. It is also used to execute sophisticated phishing and social engineering tactics. Similarly, AI has the potential to bolster cyberdefence efforts by swiftly analyzing extensive data, recognizing patterns and predicting future threats.

Canadian organizations express growing concerns about the risks associated with AI and its ability to empower adversaries. The majority cite common concerns, including giving cyberattackers the ability to automate the process of discovering and exploiting vulnerabilities (58 percent), identifying new attack vectors (50 percent) and speeding up the development of new malware strains (42 percent).

“The rapid evolution of AI in the cybersecurity landscape demands a proactive approach to defend against evolving cyberthreats,” said Ivo Wiens, Field CTO, Cybersecurity at CDW Canada. “But this also goes both ways. By leveraging the power of AI in their cybersecurity investments, organizations can effectively stay ahead of emerging threats.”

AI can be used to predict threats based on historical data, enable proactive security measures and can automate threat detection and response, which rapidly increases remediation time. It can also help organizations facing talent shortages by employing automation, allowing security teams to manage higher workloads with limited staffing.

Threat detection and response continue to be a missing piece of the puzzle

Organizations that prioritize zero-trust network access (remote access to resources with clearly defined control policies) for threat prevention, without allocating resources to threat detection and response, risk overlooking a vital aspect of their cybersecurity strategies.

According to the study, less than one-third (29 percent) of organizations implementing zero-trust strategies have a policy in place that mandates security monitoring for threat detection. This highlights a gap in organizations’ security strategies and an opportunity to strengthen their cybersecurity posture through threat detection and response.

Security remains a priority amid declining IT budgets

Against the current economic backdrop, Canadian organizations are increasingly adopting cost-cutting measures, leading to a notable decrease in IT budgets, which have declined by more than half (51 percent) compared to 2023. Despite this downward trend, organizations continue to increase cybersecurity spending in proportion to their overall IT budget year-over-year, indicating that cybersecurity remains a priority to reduce potential negative impacts on their business.

The trend of reduced IT spending may lead to “breach fatigue” among IT security teams due to limited resources. This has the potential to negatively impact IT security teams, leading to physical and mental exhaustion, decreased morale and increased likelihood of error.

Given the current environment of tightened budgets, thinly stretched teams and increased cyberthreats, organizations must have robust security measures in place

to safeguard against existing threats and proactively prepare for future risks, ensuring a resilient cybersecurity posture.

“Organizations face a critical decision when allocating IT budget for cybersecurity," said Daniel Pinsky, CSO & Head of Security Governance and Compliance at CDW Canada. "Despite shrinking IT budgets, it's heartening to see Canadian organizations prioritizing cybersecurity to effectively mitigate evolving threats and safeguard critical information. Organizations must ensure cybersecurity teams remain well-resourced to avoid complacency.”

To learn more about the state of cybersecurity for Canadian organizations, download the study here.

Join the conversation online by following @CDWCanada on X (formerly Twitter) and LinkedIn.

About CDW Canada

CDW Canada Corp. is a leading provider of technology services and solutions for business, government, education and healthcare. Established in 2003, CDW Canada is the country’s trusted advisor for cybersecurity, hybrid infrastructure and digital transformation. CDW Canada experts design, orchestrate and manage customized services and solutions, making technology work so people can do great things. Through its services-led approach, CDW Canada simplifies complex technology to empower customers to focus on their business and thrive in a rapidly evolving landscape. CDW Canada is a wholly owned subsidiary of CDW Corporation (Nasdaq: CDW), a Fortune 500 company. For more information, visit www.cdw.ca.

For further information, please contact:

Julie Clivio

VP, Growth & Operations, CDW Canada
647.288.5828 | julie.clivio@cdw.ca