Number of Successful Cybersecurity Breaches Affecting Canadian Businesses More Than Doubled in Past Year, According to CDW Canada Study

Threat detection and response is falling short amidst an increasingly challenging IT environment, with cybersecurity breaches up by 130 percent from 2022

Toronto, ON – June 13, 2023 - CDW Canada, a leading provider of technology solutions and services for Canadian organizations, today released its annual security research, the *2023 Canadian Cybersecurity Study: Emerging Issues and Trends*. The study, conducted with additional support and analysis by IDC Canada, surveyed over 500 IT security, risk and compliance professionals and explains the state of cybersecurity among Canadian organizations, with a focus on the expanding attack surfaces that emerged as a result of the substantial growth of business computing peripherals, servers and Internet of Things (IoT) devices.

The sophistication of cyberattacks, combined with greater entry points created through cloud infrastructure, IoT and endpoint devices has led to an increase in security breaches. The study found that 7 percent to 10 percent of all cyberattack types were successful and observed a significantly greater "hit rate" of success (the number of attacks that result in a breach) achieved than in previous years.

While total cyberattacks in 2023 decreased from 2022, they resulted in a greater number of breaches at organizations, jumping from a 12-month average of 13 in 2022 to 30 in 2023. While organizations are taking steps in the right direction to secure their IT assets, there is room for improvement to protect data and devices spread across various networks.

Cloud is convenient, yet requires specific protections

Public cloud environments - the most impacted IT components affected by security incidents and vulnerabilities - are being created by the increased use of cloud for storing private, sensitive and highly restricted data. It is further compounded by the adopt-first/secure-later approach of hybrid work, which has led to a widening gap between cloud adoption and proper investments to secure it.

More than half (54 percent) of organizations store internal data, greater than one-third (36 percent) store sensitive (confidential) data and more than one-quarter (28 percent) store secret (highly restricted) data in the public cloud. Yet, organizations only spent on average 13 percent of their security budgets on securing cloud environments.

"Cloud infrastructure allows businesses of all sizes to scale and be agile in hybrid and remote work environments," said Ivo Wiens, Practice Lead for Cybersecurity at

CDW Canada. “However, rapid adoption without necessary security practices leaves an organization’s sensitive data easy for cyberattackers to access.”

Detection and response enable business continuity

Threat detection and response is falling short, giving cyberattackers more time to access and steal personal, financial and intellectual data, or disrupt business processes with ransomware.

According to the CDW Canada study with research and analysis by IDC, the average time to detect a cyberincident is 7.1 days, while responding to an attack takes twice as long at an average of 14.9 days. The average time to recover is 25.6 days, putting the average incident management time at approximately 48 days total. This delay puts Canadian organizations at greater risk of reinfection, loss of customer trust and higher incident recovery costs.

Automated processes are key to a robust security practice

Organizations must address the IT security skills gap and implement automated processes to mitigate and minimize the impact of breaches while maintaining an advanced security posture that proactively defuses threats.

The study found that nearly two-thirds (62 percent) of Canadian organizations say the skills gap has reduced their ability to prevent security incidents. Automation can significantly improve efficiency for security operations centre (SOC) analysts – the frontline professionals who monitor, detect and respond to cyberattacks. Automation frees up their time so they can devote more of it to higher-value cybersecurity activities such as investigations and threat hunting. In fact, more than half (59 percent) of respondents say they see automation as a way to improve security staff efficiency.

Keeping up with sophisticated cyberthreats may seem like a massive undertaking, but expertise is available. As a trusted expert in cybersecurity solutions, CDW Canada can help organizations prepare for, defend and respond to the ever-expanding threat landscape.

For more information, download the study here.

About CDW Canada

CDW Canada is a leading provider of technology solutions for business, government, education and healthcare. CDW Canada Corp. helps customers achieve their goals by delivering integrated technology solutions and services that help customers navigate an increasingly complex IT market and maximize the return on their technology investment. Areas of focus include software, networking, unified communications, data centre and mobility solutions. CDW Canada Corp. is on the Channel Daily News Top 100 Solutions Provider list in Canada, and is a wholly owned subsidiary of Vernon Hills, Illinois-based CDW Corporation, 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