More Than Half of Canadian Businesses Rarely or Never Conduct Regular Penetration Testing

New study from CDW Canada examines the evolving threat landscape and reveals major sources of cybersecurity incidents in Canada

Toronto, ON – May 4, 2021

CDW Canada, a leading provider of technology solutions and services for Canadian organizations, today released its 2021 cybersecurity study, *Innovation in Cybersecurity: Approach, Tools and Technologies*, revealing that regular penetration testing, multi-layer framework-based approaches to cloud consumption and third-party risk management all play a critical role in mitigating cybersecurity incidents for Canadian businesses. The study, conducted by IDC Canada on behalf of CDW Canada, examines the evolving nature of cybersecurity threats and the vulnerability of Canadian businesses in an increasingly digital landscape.

Since the outset of the pandemic, digital solutions have played an increasingly important role in maintaining business continuity for Canadian organizations. Unfortunately, this has led to the cost of cyber compromise reaching an all-time high – averaging $1,257,000 expended per organization – as malicious actors continue to capitalize on the ongoing changes and disruptions facing businesses today. This has increased by 47 percent from $853,000 in 2019, with 99 percent of businesses surveyed having reported a cyberattack between November 2019 and November 2020. While innovation and new technologies are contributing to security effectiveness, the reality is that cyber resilience depends on many contributing factors including adopting the right technologies, conducting thorough analyses of third-party relationships in security planning and applying well-rounded approaches to security governance that support technology adoption.

"New technologies and using existing technologies in new ways breed new risks, and this year's findings highlight that remote infrastructure as well as the extension of processes and workflows to third-party partners are stretching cybersecurity resources to the limit," said Theo van Wyk, Head of Cybersecurity and Solutions Development at CDW Canada. "Failure to consider cybersecurity solutions as part of a business' yearly organizational planning and to maintain them on an ongoing

basis is a problem that can result in millions of dollars in losses. Cyber criminals are becoming increasingly sophisticated, and businesses need to stay ahead of threats to ensure their security posture remains strong at all times."

Regular penetration testing is essential to understanding attack surfaces

As the threat landscape continues to evolve, vulnerabilities need to be regularly identified and managed through regular penetration testing. This is essential for businesses to identify their weaknesses and exploitable attack surfaces across infrastructure, applications, users and employees in order to implement preventative, rather than reactive, recovery approaches.

Alarmingly, the study revealed that more than half (57 percent) of businesses surveyed reported their vulnerability management is informal or that they do not scan for vulnerabilities at all. This is extremely concerning as failing to conduct planned, regular penetration testing leaves businesses exposed to unknown vulnerabilities and potential exploitation. This poses a significant risk that can have devastating and lasting consequences on businesses in both the short and long term.

Supply chain and third-party risk is more critical than ever

The practice of third-party partner and supplier reliance is commonplace in supporting modern business operations. As digitization intensifies and businesses continue to shift between remote and hybrid operating models, organizational processes and workflows are increasingly extending to more third parties and can expose critical security gaps.

According to the study, three out of four businesses surveyed (76 percent) have experienced a security breach due to the poor security practices of a third-party partner between November 2019 and November 2020. This number also increases with business size, likely due to larger businesses having more suppliers, third-party partners and complex IT environments compared to smaller peers. While regularly reviewing third-party partner security can be challenging when working with multiple partners, the survey suggests that ongoing reviews and carefully selecting partners to avoid any potential cybersecurity pitfalls has never been more important to ensuring a strong security posture.

Multilayer security approach for cloud consumption is key to improved security

As businesses continue to migrate data to the cloud, it is important that this is done strategically with security top-of-mind to ensure data is protected every step of the way. Deploying a multilayer framework-based approach to cloud consumption is equally important in ensuring security is maximized and that there is alignment with existing security programs.

The study shows that businesses with larger distributions of data in software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS) are more likely (86 percent) to have a multilayer approach to using cloud security. Despite being attacked more often, these businesses experience fewer infiltration and exfiltration incidents as a result of their multilayer approach to cloud security. This has drastically helped protect against security threats and demonstrates that this approach should be prioritized by organizations of all sizes as the future of work becomes increasingly hybrid.

Join the conversation online by following @CDWCanada on Twitter and LinkedIn.

About Innovation in Cybersecurity: Approach, Tools and Technologies:

The study was independently conducted by IDC Canada a Canada-wide cross-industry survey of 557 IT security and risk & compliance professionals. All survey participants were screened for direct involvement in improving or managing their organization's IT security. Of the IT security respondents, 66 percent were at a supervisor level (infosec supervisor/IT supervisor) or higher. Survey respondents were screened to represent organizations with a minimum of 15 full-time employees, with at least 10 percent of their total employees located in Canada. The survey was conducted throughout October and November 2020 by IDC Canada on behalf of CDW Canada.

About CDW Canada

CDW Canada is a leading provider of technology solutions for business, government, education and healthcare. CDW Canada 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 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 CDW.ca.

For further information, please contact:

Jennifer Crisp

Marketing Manager, Brand and Communications, CDW Canada
437.353.4962 | jennifer.crisp@cdw.ca

For media inquiries, please contact:

Jennifer Farr

Kaiser & Partners
416.910.5221 | jennifer.farr@kaiserpartners.com