Ransomware, third-party partners top the list of this year's cybersecurity threats

New study reveals ransomware and third-party partners are major sources of cybersecurity incidents in Canada

Toronto, ON – April 20, 2020

Ransomware and poor third-party partner cyber hygiene contributed to the majority of organizational cybersecurity incidents in Canada, according to CDW Canada's 2020 Cyber Resilience: An Evolving Perspective study. The study, conducted by IDC on behalf of CDW Canada, examines the evolving nature of cybersecurity threats and the vulnerability of Canadian businesses.

The world as we know it is changing and many organizations are experiencing a shift to remote work. Although this shift will potentially drive a faster digitization of businesses moving forward, our findings revealed cybersecurity is often an afterthought which can have potentially dire consequences for an organization. According to respondents, approximately one quarter of Canadian organizations (20%) continue to be impacted by ransomware attacks. Of those organizations who were victims of ransomware, a surprising 80 per cent reported experiencing subsequent attacks after "recovering" from the initial incident and 63 per cent of victims lost access to data. In addition, an overwhelming four in five organizations (82%) also experienced a security incident due to the poor security hygiene of a third-party partner.

"Ransomware attacks only require a singular vulnerable device, and the size and complexity of an organization's attack surface is strongly linked to ransomware susceptibility. With this year's findings, it's clear that the level of sophistication required to extricate ransomware from a network is underappreciated," said Theo Van Wyk, Head of Cybersecurity at CDW Canada. "Relationships with third-party partners also puts organizations at risk, as these partners are often given access to customer data or propriety information with insufficient security architecture, leading to new breaches."

Ransomware bad actors taking advantage of organizations' expanding BYOD and IoT networks, with a surprising impact on cyber insurance

Ransomware encompasses everything from mass scale phishing campaigns, to targeted attacks leveraging social engineering, remote desktop vulnerabilities and multi-stage attacks using various types of malware to infiltrate an organization's network.

The size and complexity of an organization's attack surface increases the likelihood of a ransomware attack. In general, the more devices that are connected to the network, the higher the probability an attacker can leverage the vulnerability of one of the devices. Organizations that fell victim to ransomware had larger than average attack surfaces, including 37 per cent more servers and 20 per cent more PCs.

As Canadian organizations are expanding their network and increasingly allow for noncorporate internet-of-things (IoT) and bring-your-own-devices (BYOD) for employees, the threat of ransomware also grows. The study revealed that ransomware bad actors took repeated advantage of organizations with both large attack surfaces and relatively weak endpoint detection and response (EDR) solutions covering IoT devices and BYOD. Of those who experienced ransomware, the vast majority had strong EDR adoption rates (92%) but weak coverage extension to BYOD and IoT devices (41%). As the infection entry point for ransomware only requires one vulnerable device, deploying EDR solutions for corporate PC endpoints only is not an effective strategy.

Alongside stiffer penalties and fines that are built into privacy and compliance regulations, more organizations are adopting cyber insurance policies to protect themselves against the repercussions of security incidents. However, this is making ransomware more lucrative for attackers, who see cybersecurity coverage as an easy payday as insurance companies may quickly decide that paying a ransom is the most cost-effective course of action.

"To combat ransomware, companies need proper controls to provide visibility into who is accessing the data and how they are using it. It also means ongoing updates on the use of BYOD devices and training for employees," continued Van Wyk. "Creating a comprehensive plan to return to a trusted state is important to ensure that your team is ready when, not if, a security incident occurs."

Third-party partners post widespread risk on organizations of all sizes

In today's environment, Canadian organizations are working with dozens of third-party partners and suppliers for tactical processes and strategic initiatives. The study revealed that small organizations (15-249 employees) usually partner with an average of 13 third-party partners, while enterprise organizations (5,000+ employees) work with an average of 82. Nearly 100 per cent of the organizations surveyed said they allow third-party partners to handle or access customer data and proprietary business information.

In addition, less than 40 per cent of organizations consider including relationships with third-party partners in their security planning, with enterprise-level organizations being the most impacted. A mere 28 per cent of the enterprise organizations have a cybersecurity plan that comprehensively includes all third-party partners and, even more concerning, seven per cent of organizations surveyed admit third-party partners were not considered in their cybersecurity planning at all.

"To maintain third-party partner relationships and keep data safe, organizations need to ensure that security policies are up to date and limit partner access to the network and data," said Van Wyk. "Organizations should also perform threat risk assessments when possible and use periodic questionnaires when not. It's important to have basic visibility into the security of third-party partners at all times. "AI-based tools are an effective but challenging cybersecurity solution Three-quarters (75%) of Canadian organizations revealed that using AI and machine learning tools increases cybersecurity effectiveness. Despite increased adoption, 66 per cent of respondents felt the tools are challenging to configure and use. Of those who have adopted AI, survey respondents did not see a significant decrease in organizational costs such as staffing. The complexities of process automation and orchestration in enterprise-scale IT environments can impede adoption – especially for enterprise organizations. As a result, smaller and medium organizations (250-4,999 employees) have stronger adoption of AI-based tools.

What the threat landscape means for Canadian organizations by the numbers

While cybersecurity threats are often reported in millions or billions, the reality of today's threat landscape demands significant financial and time investments for organizations of all sizes and at the individual employee level.

In last year's study cybersecurity incidents cost an average of $2,677 per employee to rectify. Even more jarring was that it took Canadian organizations an average of 19.4 employee workdays to respond to and recover from an attack. This year, however, the average cost per employee nearly doubled to $4,024, with organizations spending a remarkable 58.6 workdays related cybersecurity incidents.

Unsurprisingly, the number of attacks and the cost of breaches also continues to rise. Organizations surveyed reported an average of 514 attacks per organization per year, up from 440 attacks in 2019. The average total cost per organization of responding to, and recovering from, cyber security incidents increased to between $5.7 million to $8.4 million, up from between $4.8 million to $5.8 million last year. On average, organizations spent $1.1 million in direct dollars addressing cyberattacks.

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

If you are interested in learning more, download the study here.

About the Cyber Resilience Study

The study was independently conducted by IDC Canada through a Canada-wide and cross-industry survey of 524 IT security and risk and compliance professionals. The purpose was to provide insight into several questions facing IT security departments in Canada, such as how digital initiatives are changing how and where organizations store their data, if AI and machine learning tools increase cybersecurity effectiveness and what strategies companies could adopt to protect themselves in the future. The study was conducted throughout October and November 2019 by IDC Canada on behalf of CDW Canada, prior to the global pandemic. Eighty-seven percent of the IT security respondents 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 and at least 10% of their total employees located in 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 www.cdw.ca.

For further information, please contact:

Jennifer Crisp

Manager, Marketing and Communications, CDW Canada
416.560.3446 | jennifer.crisp@cdw.ca

For media inquiries, please contact:

Maggie Hall

Kaiser Lachance Communications
647.725.2520 Ext. 223 | maggie.hall@kaiserlachance.com