CYBERSECURITY IN 2022: ADVANCING THE MATURITY OF CANADIAN ORGANIZATIONS

TABLE OF CONTENTS

TABLE OF CONTENTS

About This Study

This report presents the findings of the CDW security study *Cybersecurity in 2022: Advancing the Maturity of Canadian Organizations.* The data provided in this report was obtained through a Canada-wide cross-province and cross-industry survey, independently conducted by IDC Canada, of 555 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, 75 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.

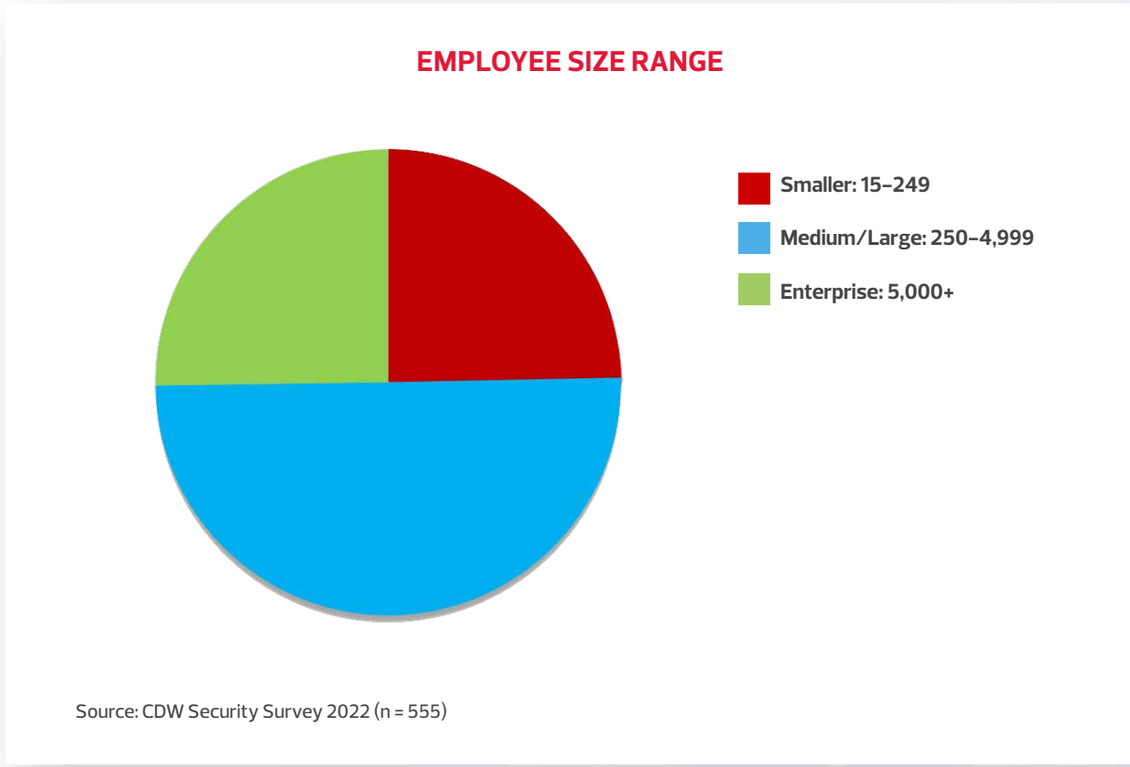
The survey was conducted during December 2021–January 2022 by IDC Canada on behalf of CDW Canada. Appendix A shows a detailed description of the demographics and firmographics of the survey participants.

Organization Size Segmentation

In this report, CDW Canada classifies responding organizations as smaller, medium/large and enterprise organizations. The definition for each is based on its number of employees:

- **Smaller: 15–249 full-time employees located within Canada**
- **Medium/large: 250–4999 full-time employees located within Canada**
- **Enterprise: 5000-plus full-time employees located within Canada**

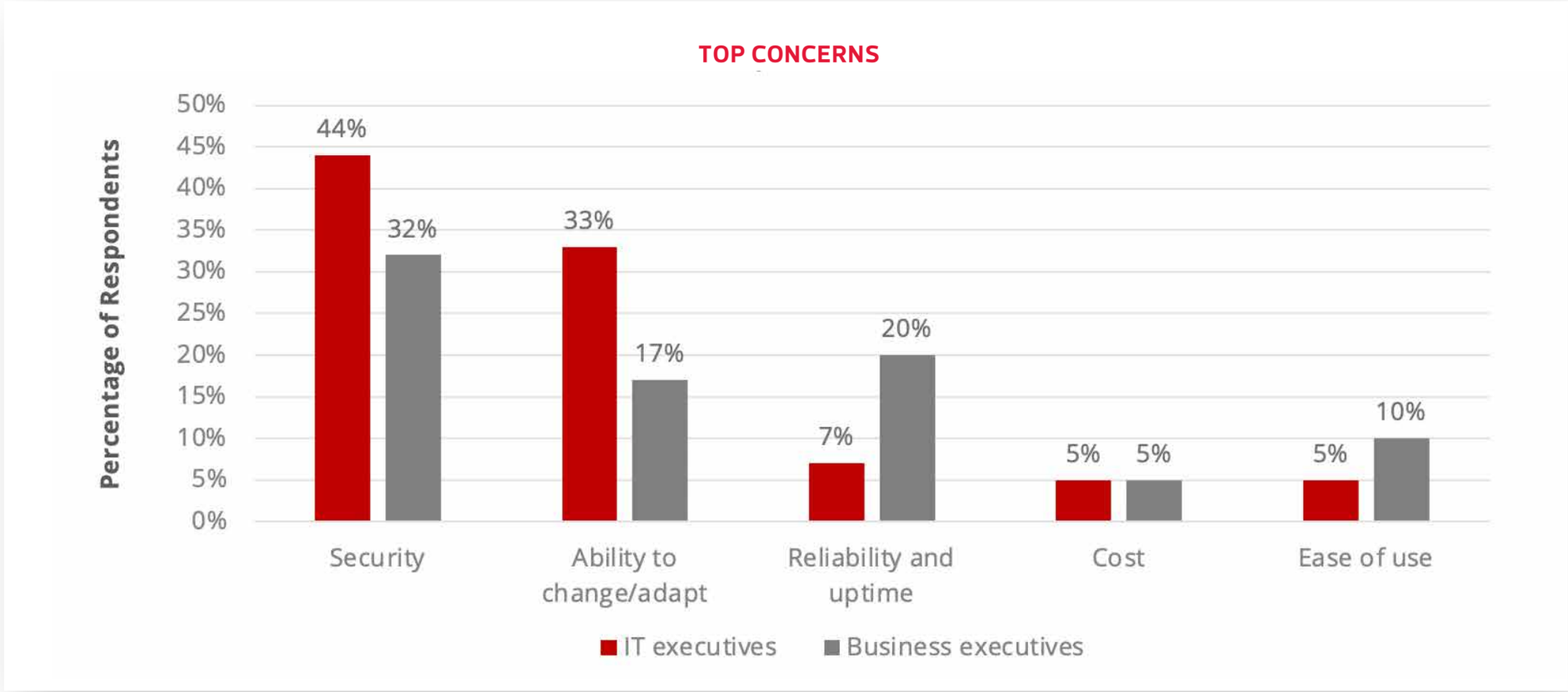
Chart A



Source: CDW Security Survey 2022 (n = 555)

Introduction

Security is the top concern for IT and business executives, as the sheer magnitude of consequences from cyberattacks can severely disrupt both businesses and society. The opportunities created by the modernization of traditional IT into a rapidly evolving, expanding and complex IT environment are counterbalanced by the necessity to secure this IT environment from the ever-increasing frequency and malicious nature of threats. The risk of loss of data, lockouts and disruption of services are top of mind for business leaders in Canada in protecting customer, employee and partner data and ensuring the continuity of business operations.



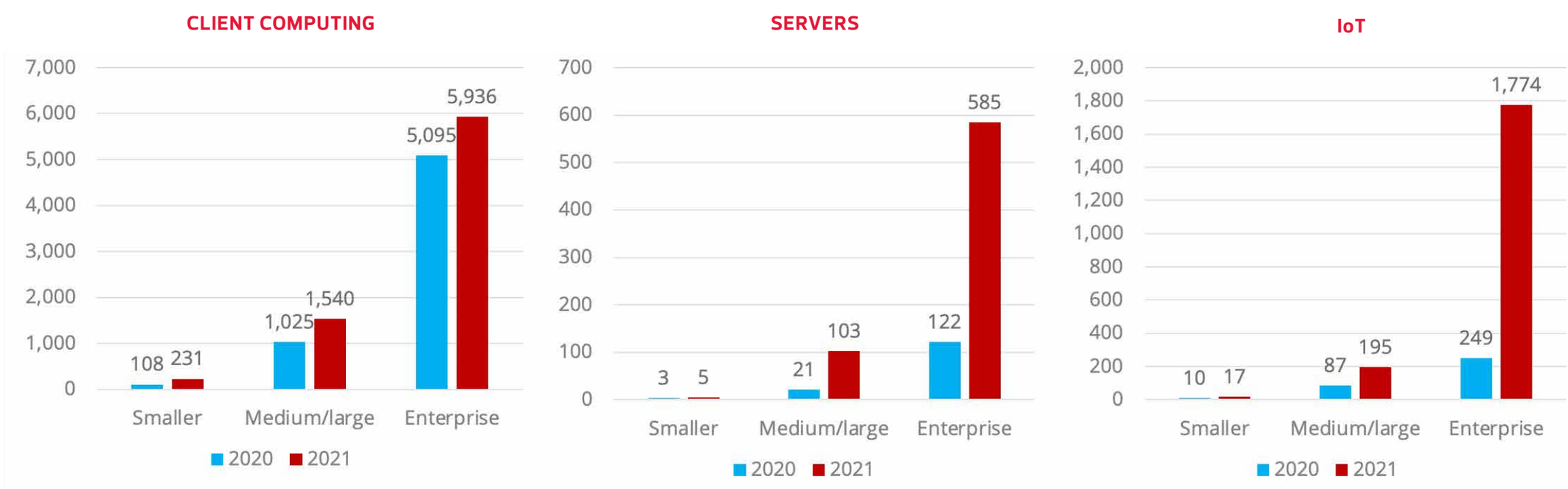
This study is intended to present an impartial assessment of the state of IT security and issues facing Canadian businesses today, and to offer insight for progress toward more robust security.

The Rapidly Evolving Threat Landscape and Resource Constraints Facing Canadian Organizations

Exploding Attack Surface

"Attack surface" refers to all of an organization's physical and digital assets, from servers (physical or virtual) to client computing devices (PCs, laptops, smartphones) to the Internet of Things (IoT) and edge computing devices. In a recent survey of business leaders in Canada, IDC found that the attack surface grew tremendously in 2021 compared with 2020, across businesses of all sizes. The number of IoT endpoints is exploding, and even the number of servers, a fairly mature technology, saw three times the growth. As the attack surface grows, so do new vulnerabilities and associated cyber risk, as evidenced in the growing number of cyberincidents.

Chart 1: Average Number of IT Devices



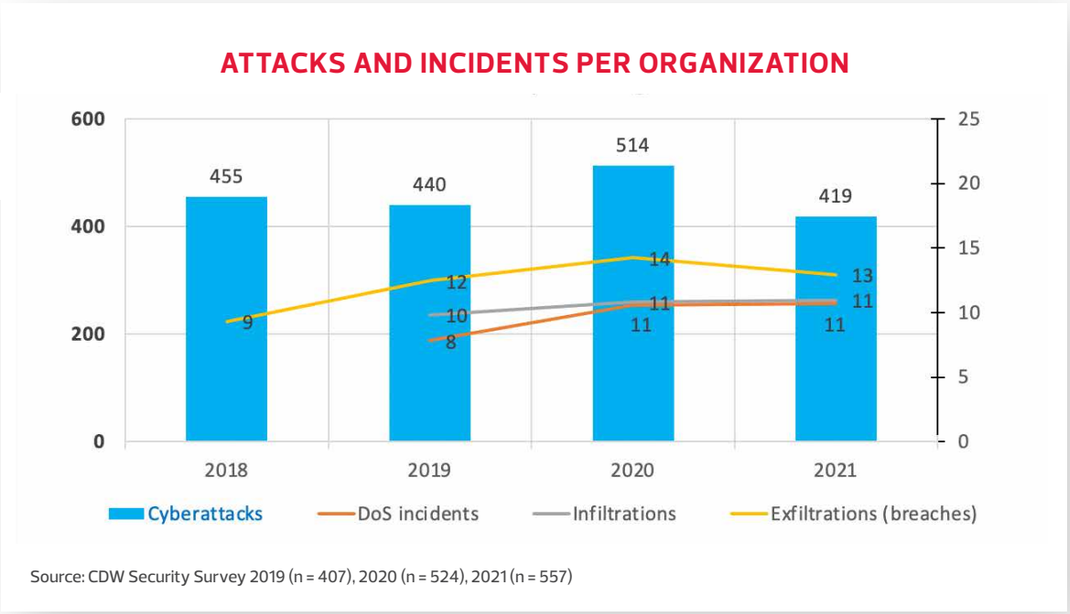
Client Computing includes PCs, laptops, smartphones and tablets
Source: CDW Security Survey 2021 (n = 557), 2020 (n = 424)

Increasing Cyberattacks and Incidents

Ninety percent of organizations reported that they were victims of a cyberattack in the past year, which shows that – regardless of size, industry or location – everybody gets attacked. Public cloud servers are the new hot target (see Chart 11), especially for larger organizations that may make extensive use of public or hybrid cloud infrastructure.

The number of attacks may be decreasing, but the number of incidents, especially denial of services (DoS) and infiltrations, is on the rise. Cyberattackers are evolving into a well-connected and organized industry, and attacks are more sophisticated than ever before. Ransomware as a Service has become an industry, phishing has expanded to targeted "spear phishing," and undetected back doors are installed, allowing repeat attacks. It takes a lot less than before to compromise an organization's IT infrastructure.

Chart 2



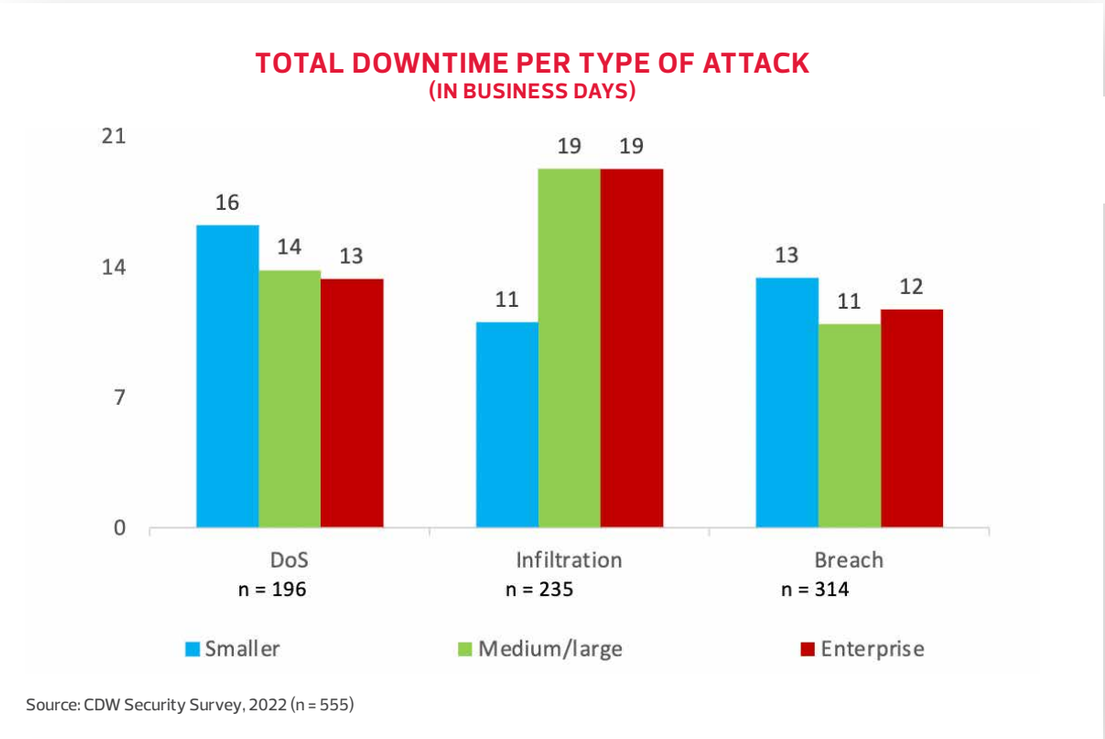
Source: CDW Security Survey 2019 (n = 407), 2020 (n = 524), 2021 (n = 557)

Downtime

For any cyberattack or incident, the magnitude of the restoration and remediation process is huge – downtime is one of the biggest contributors of direct costs associated with cyberincidents. Canadian firms report total downtimes of one to two weeks or more per category of attack. Organizations in the healthcare and manufacturing industries, as an example, reported up to four weeks of total downtime for infiltration attacks; financial services firms reported nearly three weeks for DoS attacks.

Data breaches, where data is exfiltrated from the organization, were the most cited type of attack related to downtime. Downtime seems mostly independent of business size, with the exception that smaller organizations reported less downtime due to infiltration attacks, i.e., the stealthy insertion of malware.

Chart 3

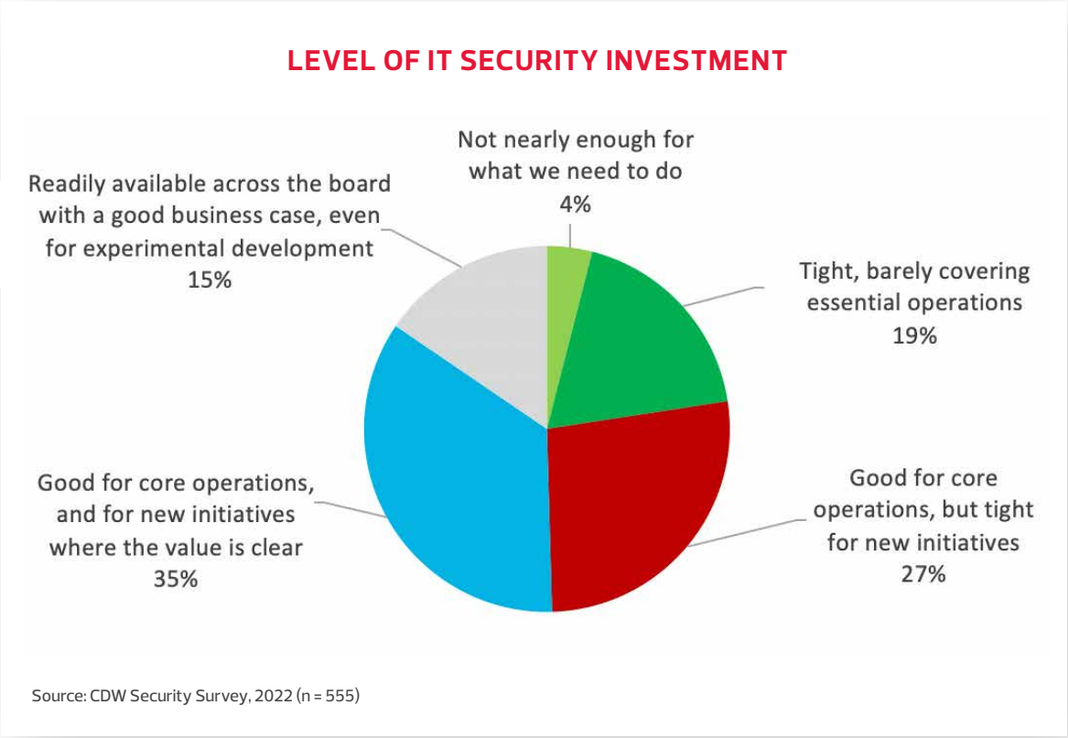


Source: CDW Security Survey, 2022 (n = 555)

Resource Constraints on Security

Two of the top concerns from CEOs[2] , aside from meeting financial goals, are the escalating cost of operations and having adequately skilled staff. While cost cuts may seem a routine response, resource constraints create new and potentially severe problems. Half of Canadian organizations reported having budgets that do not have room for IT modernization and experimentation with the latest innovative security technologies. Nearly one fourth of companies (23 percent) have budgets that do not sufficiently cover core IT security operations. So while security is a top concern, many Canadian companies struggle to adequately fund it.

Chart 4

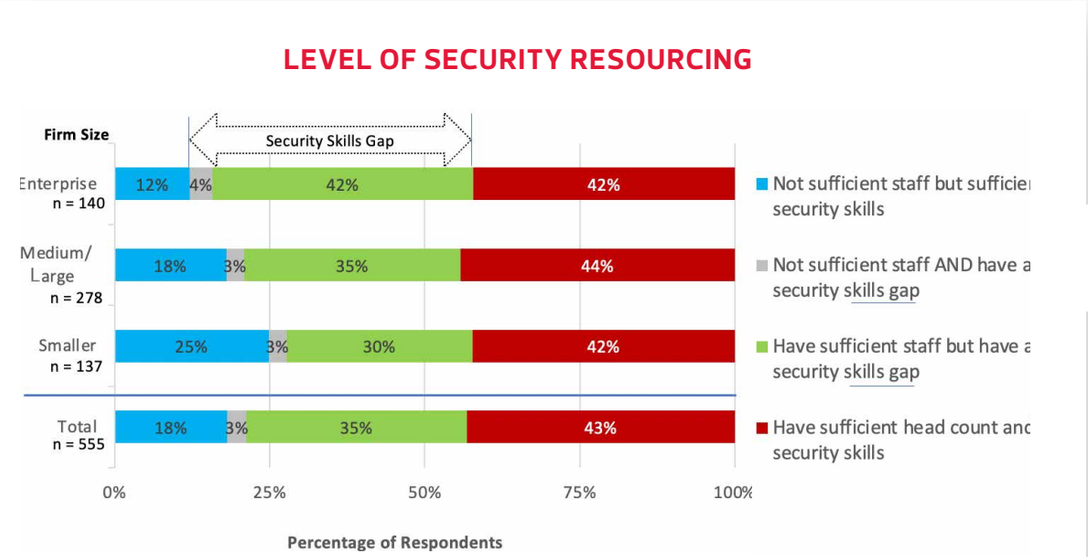


Source: CDW Security Survey, 2022 (n = 555)

Security Skills Gap

Similarly, 57 percent of organizations reported having gaps in resource staffing and/or security skills. Among enterprise organizations, for example, 84 percent have the head count and staff to meet their IT security needs, but nearly half (46 percent) reported a lack of necessary skills within their teams. The skills gap that organizations face in their IT security teams is a significant issue, and it's even more problematic than budgets for head count.

Chart 5



Source: CDW Security Survey, 2022 (n = 555)

2. Canadian Top Executive Survey, 2021: Managing Change, Security and Digital Transformation, IDC, December 2021

A Maturity Model for IT Security

"If you don't know where you're going, any road will get you there." —Lewis Carroll

Business leaders clearly want to get to a more secure IT infrastructure state, but conflicting constraints and the plethora of IT security initiatives can be disorienting. Taking time to review your current position and evaluate the paths forward can prove invaluable to security leaders. The journey to mature IT security begins with an assessment of your current state and a clear, well-defined final state. To this end, CDW has developed a model for assessing an organization's levels of IT security maturity along four dimensions, based on this year's questionnaire.

Throwing more bodies or funds at IT security won't solve the problems. Organizations need to take a step back and realistically review their security maturity, make targeted investments and efficiently progress toward an optimized stage of IT security.

Dimensions of IT Security

Security Approach	Security Philosophy	Security Investments	Security Processes
Executive leadership (outside of IT) building a culture of security best practices	Zero-trust adoption	Level of investment (technologies, processes) to detect and respond to both external and internal/insider IT security threats and the level of threat prevention controls	Adoption and optimization of best-in-class approaches (governance and compliance audits, risk assessments and staff training)
Resourcing IT security — both staffing and development of staff skills	Integration of IT security processes and tools		Backups — security, regularity, authentication
Investment in core operations, new initiatives and experimental approaches	Repeatable and consistent IT security processes and workflows		

IT Maturity of Canadian Companies

Based on these dimensions, responding organizations were placed in the four categories for further analysis.

- **Emerging Security Posture:** Twenty-seven percent of Canadian organizations are placed in this category, at the low end of the maturity scale. The security processes of such organizations are manually intensive and not well documented. A dedicated security team is either unavailable or limited in head count, which leads to undefined roles and responsibilities. The technology stack is elementary and decentralized, with basic configurations, primarily focused on threat prevention and regulatory compliance.
- **Intermediate Security Posture:** Forty-three percent of Canadian organizations are placed in this category, in the lower middle section of the maturity scale. Organizations in this category are beginning to document and standardize procedures and policies. There are clearly defined roles for security staff, which is driving security modernization internally or with the help of external providers. The technology stack is aligned to the overarching security policy, and while the focus is on threat prevention and regulatory compliance, there are point solutions in place for threat detection, response and recovery.
- **Advanced Security Posture:** Seventeen percent of Canadian organizations are placed in this category, in the higher middle section of the maturity scale. Organizations in this category have an organization-wide security strategy in place, with well-defined security policy and governance measures. Many security workflows are automated, and documentation is standardized. The security skills pipeline is robust through internal teams or external service providers. The technology stack is advanced and integrated with centralized management within an organization-wide security architecture. Security configurations are optimized dynamically, leveraging security analytics, orchestration and automation.
- **Leading Security Posture:** Twelve percent of Canadian companies are placed in this category, at the high end of the maturity scale. The security policies and procedures of such organizations are continuously improved through experimentation and innovation. These organizations can rapidly respond to advanced threats through automated and orchestrated processes. The security teams are well staffed, either internally or with external partnerships. The technology stack is optimized based on business context, security policy and architecture, and centralized management. The focus is on threat prevention, detection, response and recovery, encompassing elements of identity management and data security to deliver a robust security posture across on-premises, mobile and cloud IT environments.

All businesses regardless of size can implement robust IT security practices. For Canadian businesses, nearly 30 percent of enterprise businesses (those with 5,000 or more full-time employees) have been assessed as having an advanced level of IT security maturity, compared with only 17 percent of small businesses (fewer than 250 full-time employees). This signals an opportunity for all organizations to progress in IT security maturity.

Chart 6

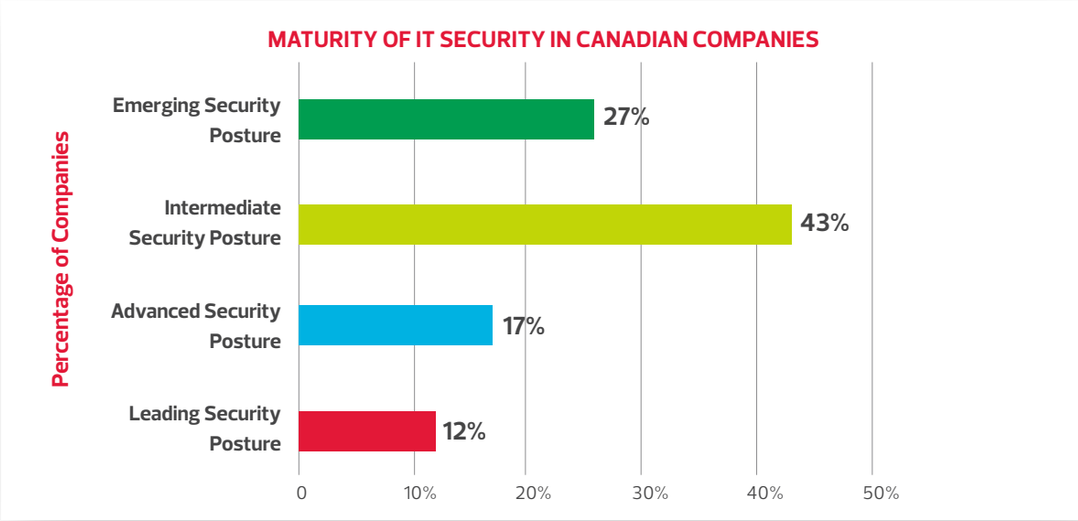
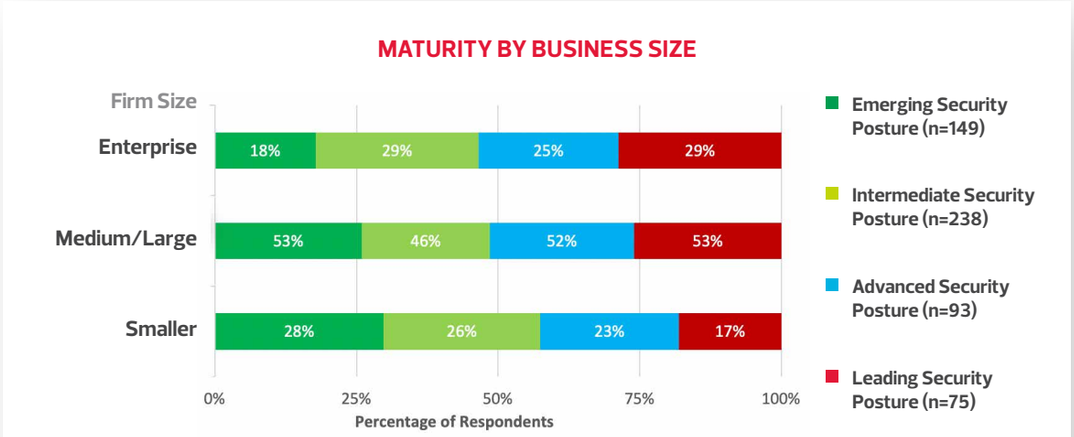


Chart 7



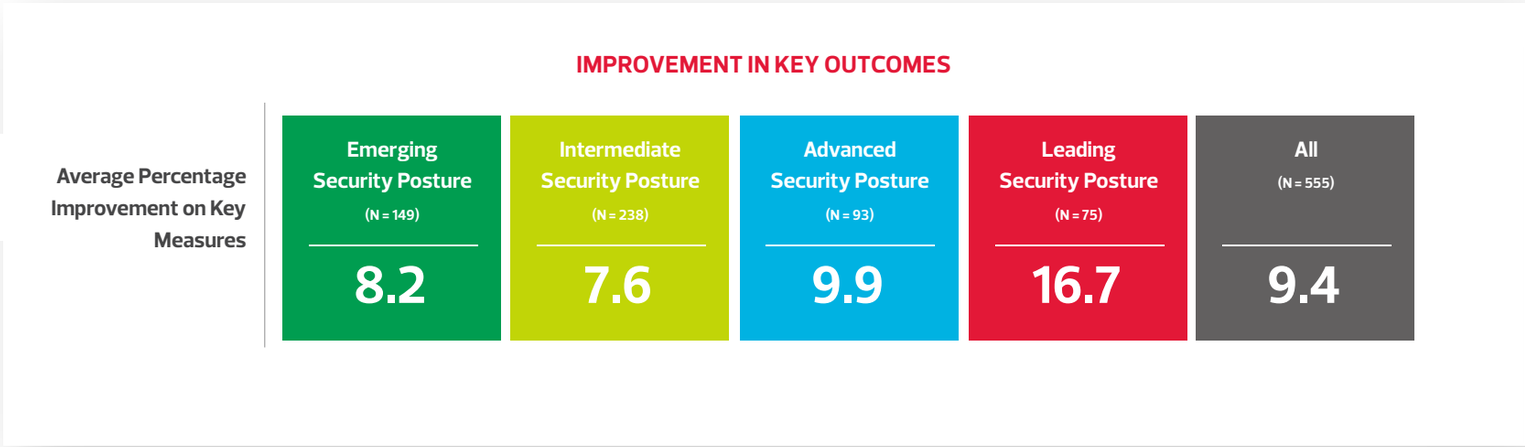
Source: CDW Security Survey, 2022 (n = 555)

Business Outcomes

Canadian companies use a variety of key performance indicators (KPIs) by which they measure business success. Typical KPIs include revenue, profit, customer experience, employee experience and productivity, operating expenditure (OPEX) and capital expenditure (CAPEX) costs, number of and time to market for new products and services, and acquisition of new customers. Businesses with lower maturity scores tend to focus on revenue and profit, while those with higher maturity are able to focus on a broader range of KPIs.

Organizations at the top of the IT security maturity scale reported both higher business outcomes (revenue, profit, regulatory compliance, operational costs, number of new products and services) and higher levels of business improvements over the past two years compared with all others. The ability to manage multiple dimensions pays off.

Chart 8



KEY FINDINGS

FINDING 1: As cloud adoption is on the rise amongst Canadian organizations, it has become the new battleground between adversaries and security teams.

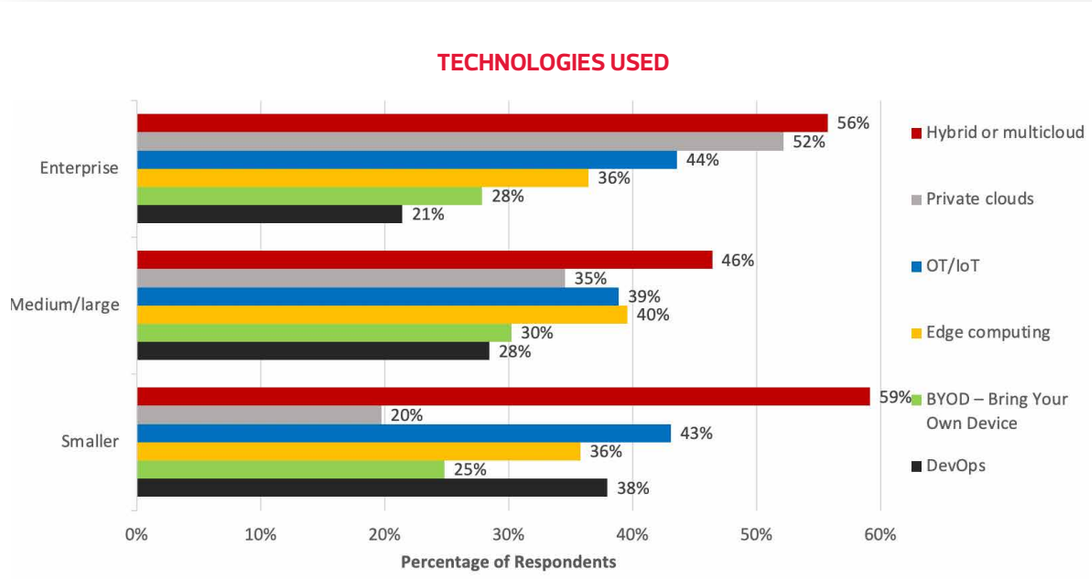
Cloud environments are the IT components most impacted by cyberattacks in Canada, while the confidence level of Canadian organizations to secure hybrid or multicloud environments remains low.

Cloud Is the New Battleground Between Adversaries and Security Teams

Cloud computing and storage continue to be at the heart of modern IT in the digital era, driven by the expansive power of technologies such as IoT, artificial intelligence (AI) and data analytics. As more applications migrate to cloud environments and deliver business data, collaboration and file sharing, applications are increasingly cloud-native or born in the cloud. This broadening attack surface is the new battleground between adversaries and security teams.

More than half of Canadian businesses have adopted hybrid or multicloud infrastructure — it is the most common digital transformation (DX) technology embraced across all business sizes. It is not surprising that private cloud usage is highest in enterprise-sized businesses; notably, smaller organizations responded with the highest usage of DevOps. Organizations need to understand their posture in these DX technologies and prioritize and develop defensive plans.

Chart 9

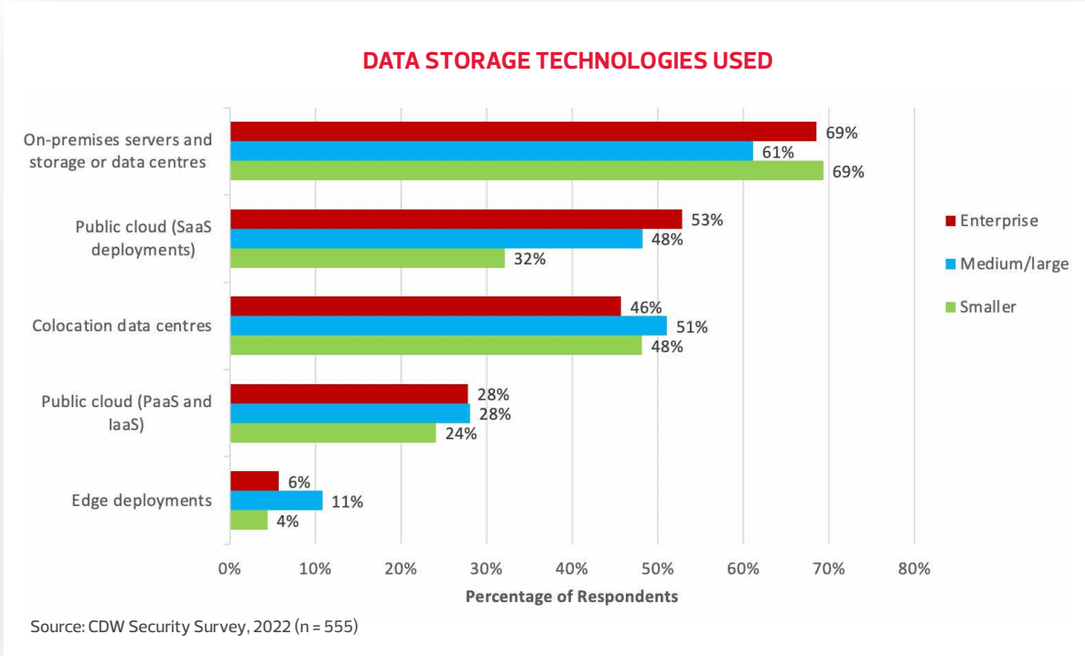


Source: CDW Security Survey, 2022 (n = 555)

Storage Deployment Models

Cloud storage offers advantages at reduced costs, especially for backups and archiving. While Canadian businesses still have on-premises IT data storage, 72 percent of them leverage public cloud infrastructure: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Notably, smaller organizations make less use of SaaS for public cloud storage deployments than their larger counterparts.

Chart 10



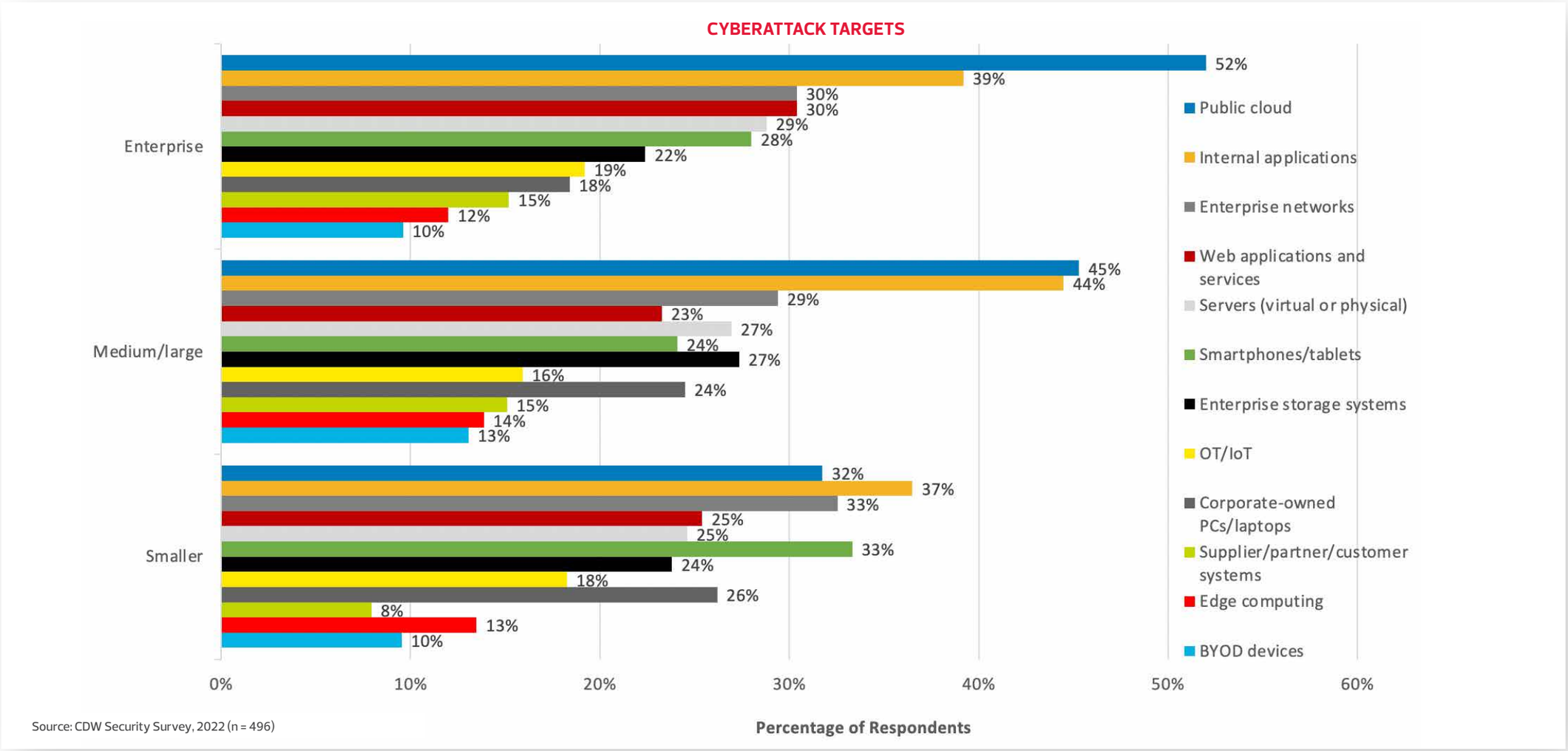
Source: CDW Security Survey, 2022 (n = 555)

As the cloud becomes a significant deployment model for organizations, attacks on cloud services by criminals, hackers and nation-states are growing. Recall the 2020 Sunburst cyber-espionage incident in which nation-state attackers stole security certificates to create their own identities, bypassed multifactor authentication, infiltrated malware into SaaS environments and opened the door for their cybermilitary forces.

Shared Responsibility Creates Complexities in the Cloud

Canadian businesses reported a tremendous variety and number of cyberattacks in the past year. Public cloud is the top attack target overall, followed by internal applications, networks and web applications. What makes the cloud complex is that the responsibility for security is shared between the provider and the business, and the responsibility changes by deployment model (SaaS, PaaS and IaaS). Factors that make the cloud attractive (scalability, rapid and flexible deployment models) can make for challenging or limited visibility and control, and new skills and toolsets are needed to monitor and secure cloud IT environments. Misconfigurations, compromised user accounts and API vulnerabilities are all leading causes of compromised cloud environments.

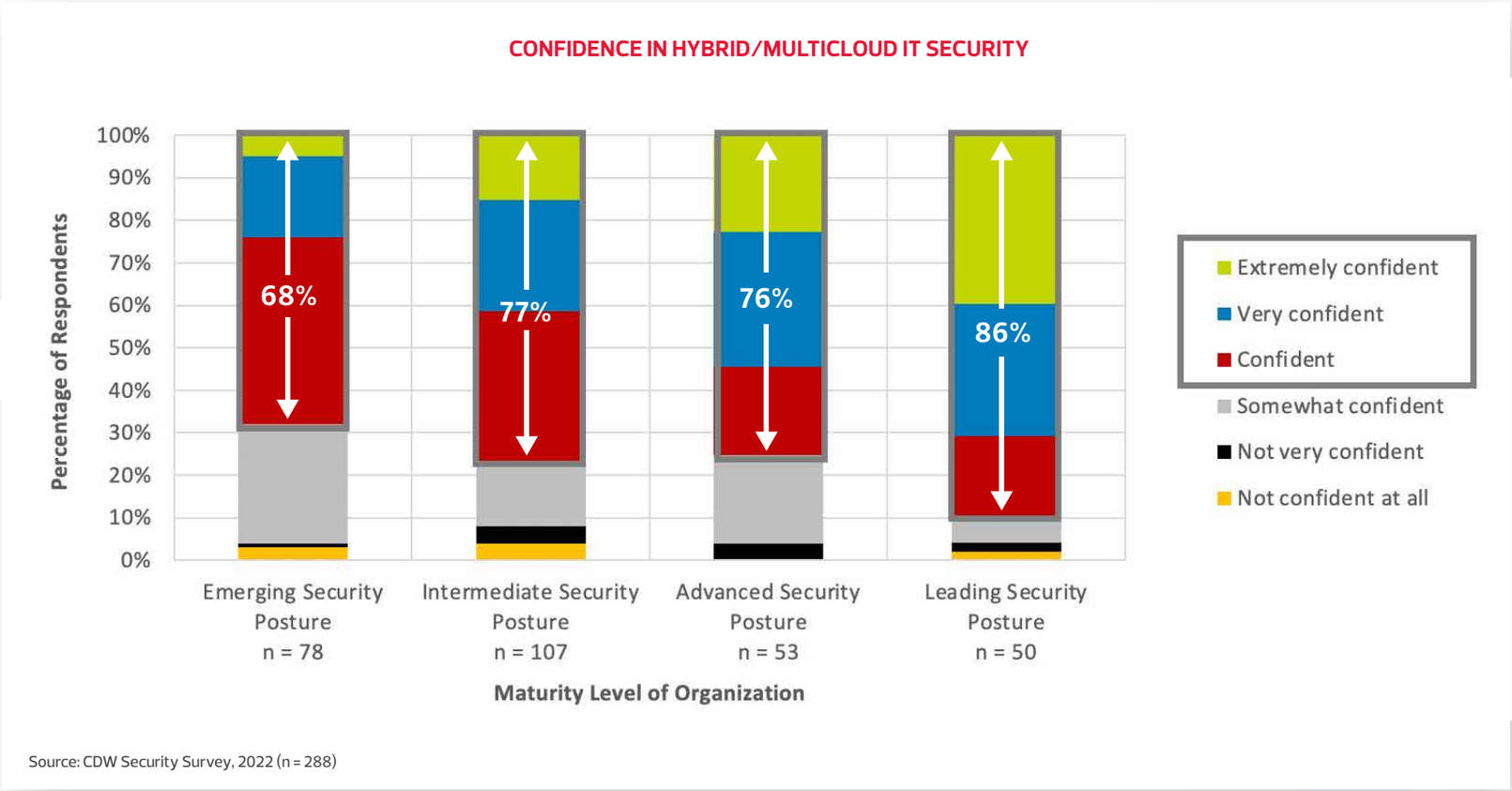
Chart 11



Source: CDW Security Survey, 2022 (n = 496)

Organizations that need to secure cloud IT environments must look at their current security posture and make investments to close the gaps in cloud governance and risk management, deploy security controls to prevent threats, monitor and detect threats, and automate responses. These efforts have a direct payoff: Survey analysis indicates that organizations that have undertaken such initiatives have improved their ratings on the security maturity model and also have reported higher confidence levels in their ability to secure hybrid/multicloud environments.

Chart 12



Source: CDW Security Survey, 2022 (n = 288)

FINDING 2: Ransomware, rampant across organizations of all sizes, is a menace impacting organizations in Canada.

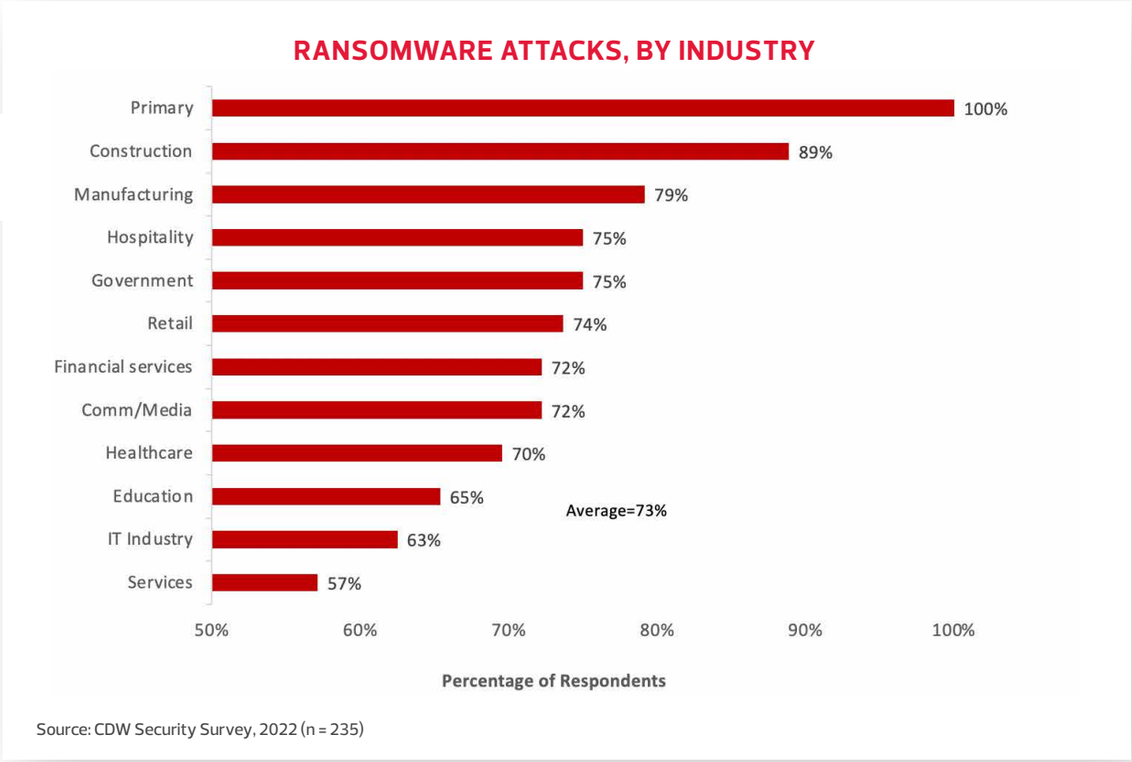
Ransomware is increasingly turning into the top digital risk to Canadian organizations. Moreover, the majority of organizations continue to face the same perils after recovering from similar threats.

Ransomware, the Menace Impacting Organizations in Canada

Ransomware

Seventy-three percent of the Canadian companies surveyed reported data infiltration attacks with ransom demands in the past year. This did not vary by company size — everyone is on the radar of cyberattackers. Any protections that smaller organizations thought they had due to their size or obscurity no longer apply. Small companies may not commonly be victims of targeted ransomware attacks, but they do get caught up in automated ransomware attacks. Among industries, primary (natural resources, including energy), construction and manufacturing were among the industries with the highest reported ransomware attacks, highlighting a need for enhanced IT security practices.

Chart 13



Source: CDW Security Survey, 2022 (n = 235)

Ransomware is so rampant that it is amongst the biggest cyber risks facing organizations today. Its significance can be gauged by the fact that country leaders are discussing ransomware at international summits. In October 2021, the U.S. National Security Council hosted leaders from more than 30 countries at a two-day summit on ransomware, and in October 2020, Interpol held its eighth INTERPOL-Europol Cybercrime Conference addressing global online crime threats, ranging from phishing to ransomware.

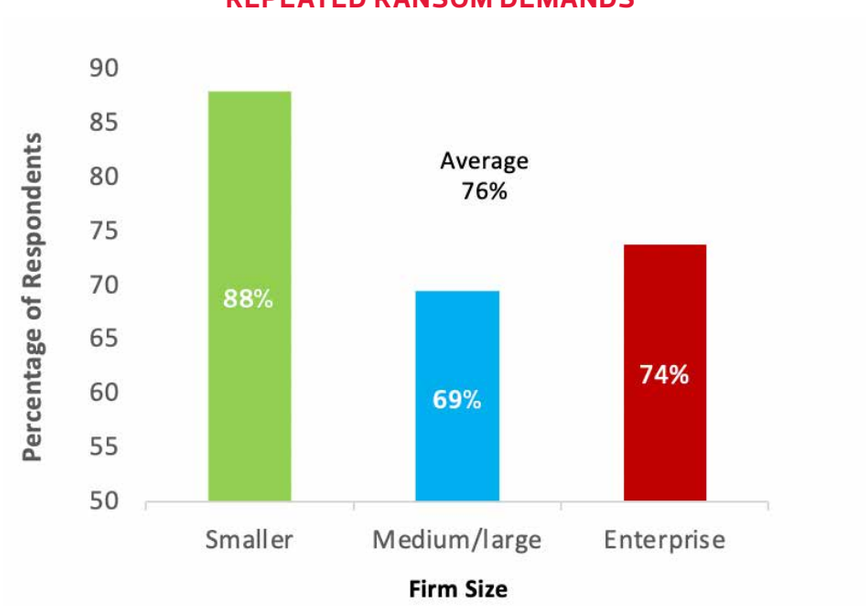
Ransomware is continuously evolving and is no longer limited to ransom demands over encryption. There are new attack models that are making headlines now — for example, multiple extortion, in which ransom is demanded not just for decryption but also for exfiltrated data. How prepared organizations are to respond to ransomware attacks is as critical as their defence mechanisms and their backup capabilities to recover from these attacks. Without a thorough forensics investigation, root cause analysis and remediation (which may span application and systems hardening, patching, security awareness training and deployment of new security technologies), ransomware reinfection is possible.

Repeat Ransomware

Frustratingly, once subjected to ransomware, the vast majority of organizations face the same or similar attacks after recovering. In many cases, multiple attack groups have simultaneous access to an organization's network, so in some cases it is coincidental. However, for the majority, when an organization does not conduct proper forensics investigations, root cause analysis and eradication, there is a possibility that a back door is left unchecked, allowing continued and repeated attacks. These back doors are often sold to other attack groups or reused by the same group for another attack.

Responding to ransomware or any other cyberattack could get chaotic. It can lead to an elevated state of emergency within an organization, and without an incident response and recovery plan, it could hamper decision making or invite regulatory scrutiny into the organization's incident handling.

Chart 14



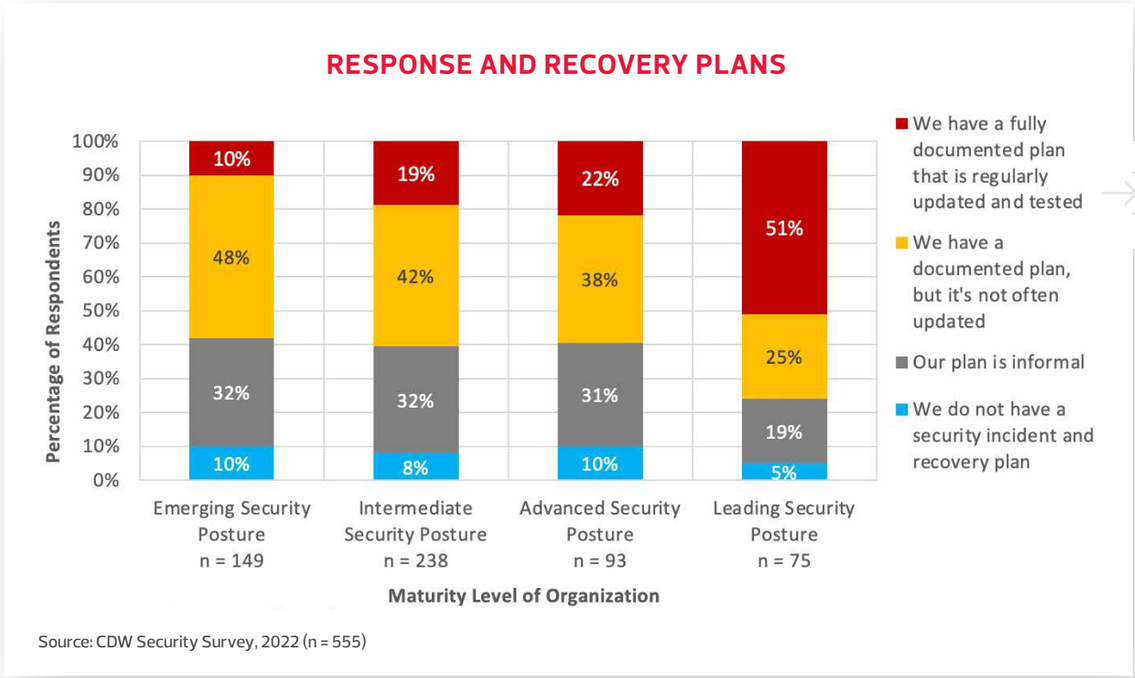
Source: CDW Security Survey, 2022 (n = 172)

Returning to Trusted State

Response plans that are not updated and tested regularly provide little help given the rate at which adversaries are evolving tactics, techniques and procedures. The plans may still be relevant in some parts within an organization, such as communication or escalation protocols, but will fall short for swift containment and eradication.

Security-mature organizations maintain a formalized response and recovery plan and invest the time and resources to frequently update and test their plan

Chart 15



Source: CDW Security Survey, 2022 (n = 555)

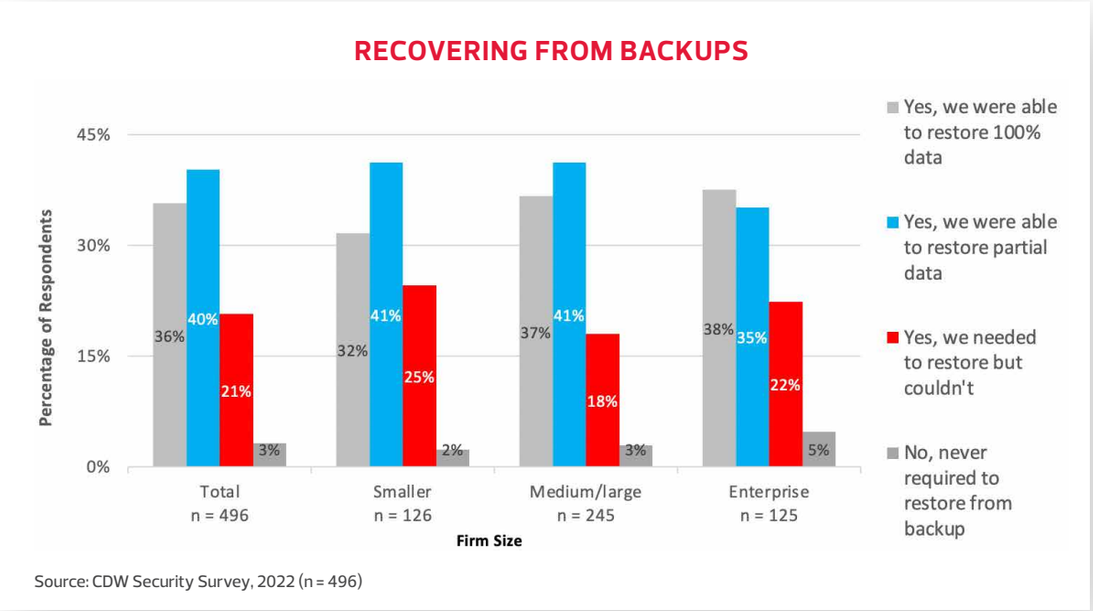
FINDING 3: The current backup and recovery strategies of Canadian organizations are falling short as cyberincidents continue to rise.

Data backups are often considered the last line of defence against cyberattacks, and Canadian organizations have made significant investments to secure their backups. However, many Canadian organizations could not rely on their backups when they needed to restore.

Backup and Recovery Strategies of Canadian Organizations Fall Short

Data protection (backup and recovery) plays a vital role in disaster recovery, but is increasingly becoming important for recovering from cyberattacks. With the rise in adoption of DX initiatives for business operations and across the value chain, a dependable backup strategy is crucial for business continuity in the face of rising cyberattacks. However, the current data protection strategies of Canadian organizations are falling far short of fulfilling that objective.

Chart 16



Source: CDW Security Survey, 2022 (n = 496)

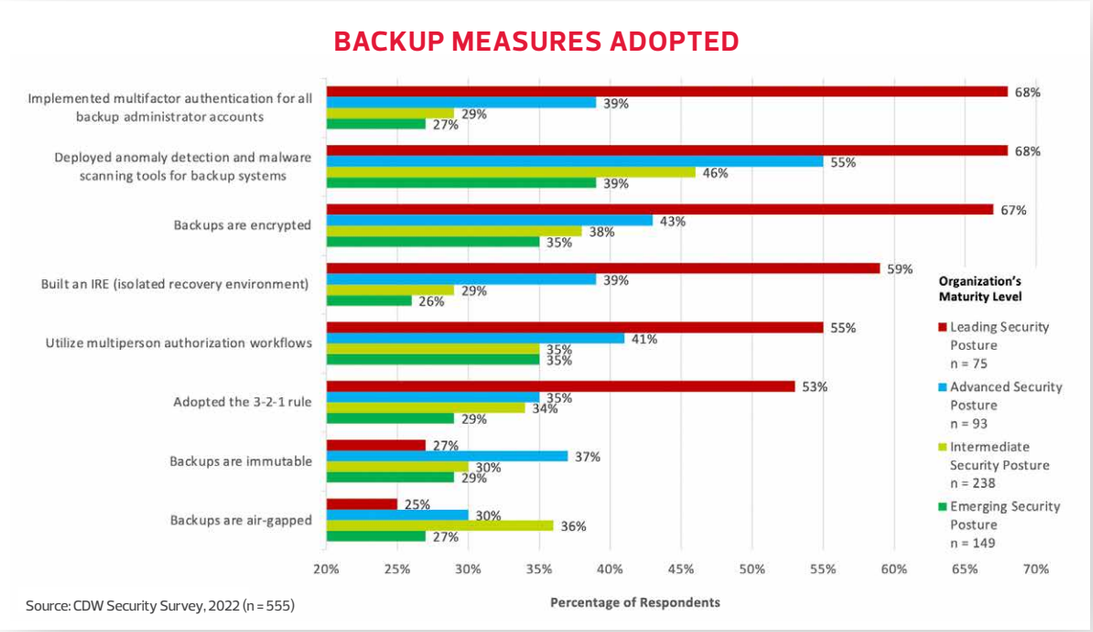
Just over a third of Canadian organizations were able to fully restore their data and systems from backups when needed, and 21 percent reported an inability to recover at all. Not surprisingly, the value of lost time and data is becoming a bigger factor in the cost of security incidents for Canadian organizations.

There are many ways of securing backups. Businesses must review their environments and deploy applicable protection controls over backups in accordance with the criticality of the application, system or data.

Modern, sophisticated cyberattacks, including ransomware, increasingly target backups to put pressure on victimized organizations. Deleting or compromising backups before taking over the production environment is common. Hence, backups present an excellent opportunity for organizations to detect these attacks early. The data protection strategy must align to the organization's recovery point objective (RPO) and recovery time objective (RTO), two key factors in a robust recovery plan.

As we saw earlier, security-mature organizations understand the need to develop and maintain a robust recovery plan. These plans deploy multilayered protection for backups, including anomaly detection and malware scanning and encryption. Strengthening identity and access management for backup and recovery workflows is crucial, and two thirds of organizations in the category of Leading Security Posture have deployed multifactor authentication for all backup administrator accounts. More than half of the organizations in the Leading Security Posture category have also utilized multiperson authorization for backup workflows for enhanced security. The 3-2-1 backup rule doubles the protection of business data by keeping backup copies both locally and offsite — perhaps in the cloud. Air-gapping and immutable backups were the least-cited measures. Assessing the reliability of backups during a cyberattack is a leading cause of slow recovery. Mature organizations have invested in isolated recovery environments (IREs) to ensure that restored data is suitable for production systems, supporting swift and reliable recovery.

Chart 17



Source: CDW Security Survey, 2022 (n = 555)

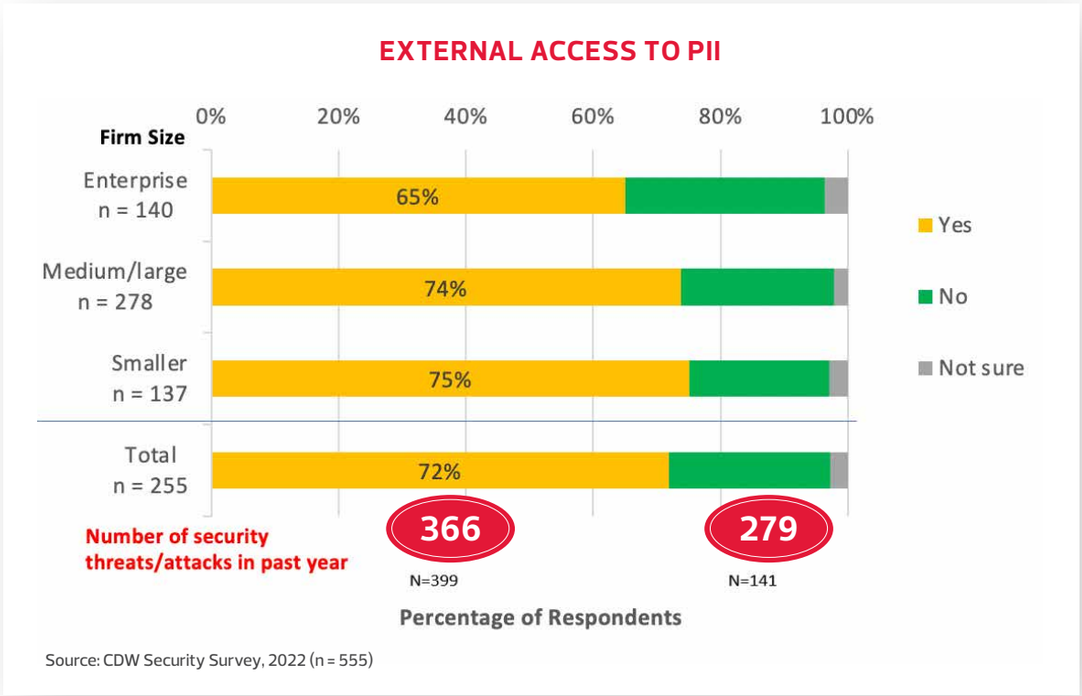
FINDING 4: The exposure of personally identifiable information (PII) to third-party suppliers is common in Canada, and leads to significantly expanded attack surfaces and a higher number of cyberattacks.

Yet the majority of Canadian organizations fail to conduct comprehensive third-party risk assessments as part of their overall cyber risk management.

Overexposure of Personally Identifiable Information Leads to Significantly Expanded Attack Surface

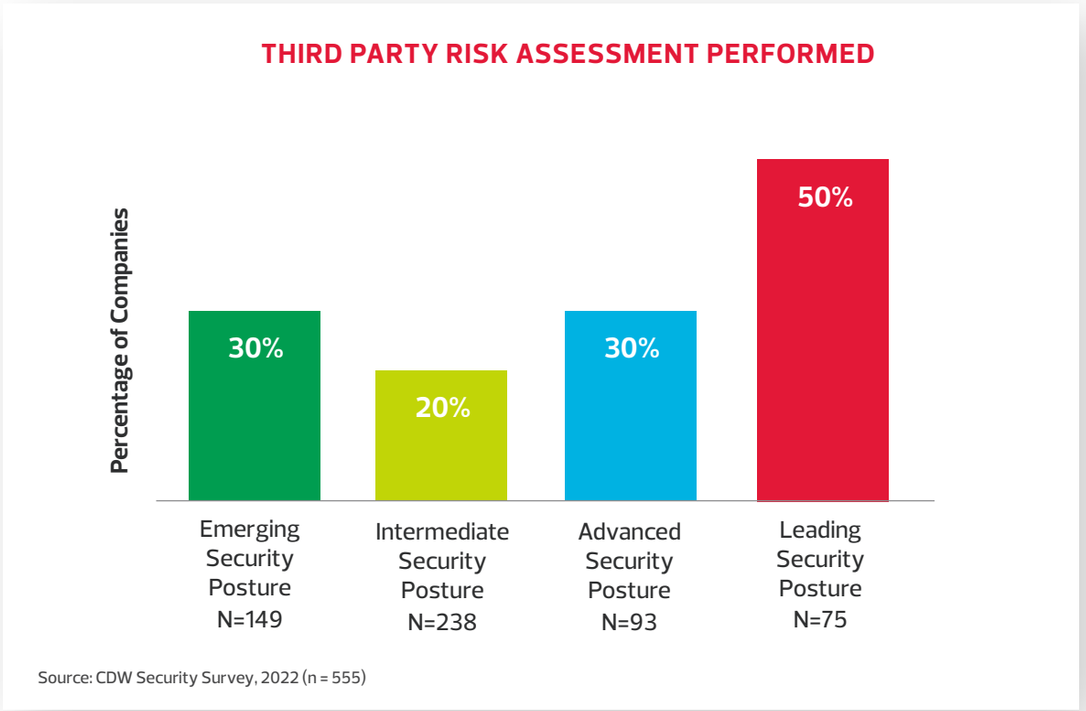
Organizations routinely rely on third parties (vendors, partners, contractors and service providers) that provide specific services. In many cases, the provided services are directly linked to the PII data collected by the organization or may even involve collecting PII on the organization's behalf. Yet many organizations fail to conduct comprehensive third-party risk assessments as part of their overall cyber risk management.

Chart 18



Source: CDW Security Survey, 2022 (n = 555)

Chart 19



Source: CDW Security Survey, 2022 (n = 555)

The majority of Canadian organizations surveyed (72 percent) indicated that their suppliers, partners or customers have access to PII contained in IT, operational technology (OT) or databases. Organizations that have PII accessible to third parties suffered 31 percent more cyberattacks within a span of 12 months compared with those that don't have PII within their IT environment exposed to third parties. Effectively managing this data access is crucial for businesses to identify and mitigate the risks relating to the use of third parties. A security risk assessment and plan containing a comprehensive third-party risk assessment is an indicator of an increased security maturity level.

FINDING 5: Canadian organizations are adopting principles of zero-trust as a preferred security architecture and cloud as a preferred deployment model for securing the digital enterprise.

Cloud is increasingly becoming the focal point of cybersecurity innovation, and Canadian organizations are embracing security in cloud to leverage enhanced capabilities, ease of management and inherent scalability.

Zero-Trust Is Rapidly Becoming a Preferred Security Architecture

The Future Is a Hybrid Workforce

According to Stats Canada, in 2020, 40 percent of employees aged 15 to 69 who had been primarily working from a physical office found themselves transitioning to working from home, and numbers went as high as 70 percent for workers in certain industries. Conditions in 2021 and 2022 found offices beginning to reopen; however, we don't foresee a return to pre-pandemic levels. In 2023, approximately 23 percent of the Canadian workforce will primarily work from home or remotely, and by 2025 this is expected to rise to 27 percent. This hybrid workforce means expanded attack surfaces.

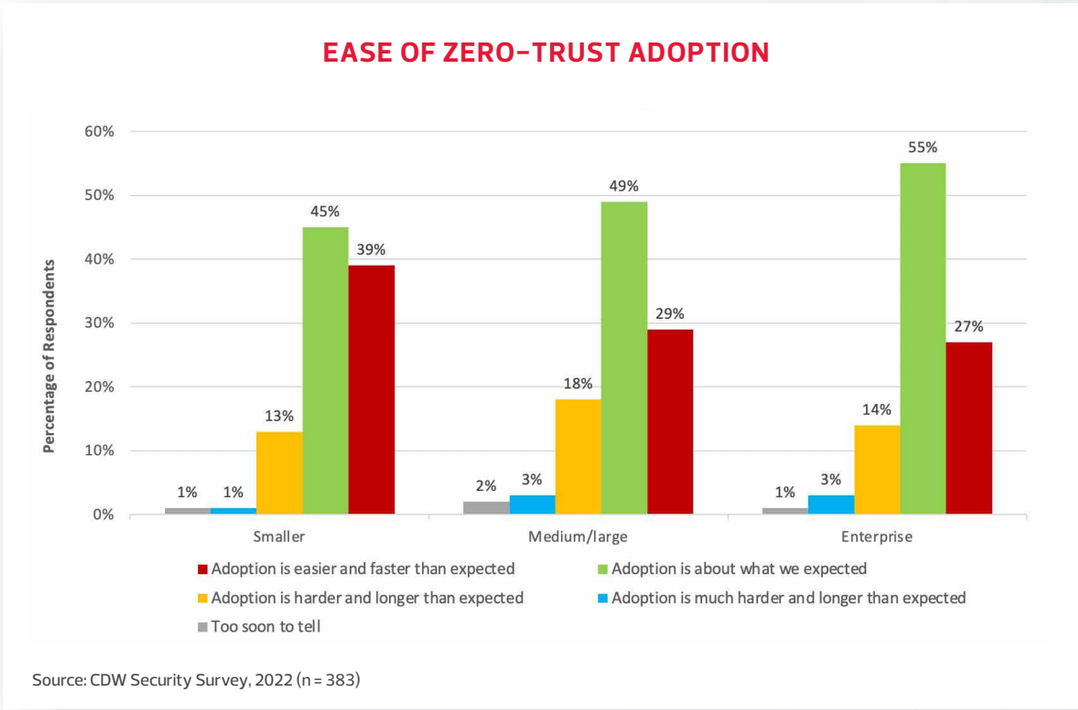
Adoption of Zero-Trust

Traditional security architectures have shown limitations as enterprise resources are now distributed. The historical IT perimeter defined by data centres, main offices and branch offices no longer exists, as the IT environment has spread to the edge and into the cloud. With the adoption of cloud services, the entire IT landscape has changed: Remote work, IoT, users, applications, IT infrastructure and data are distributed across the world, and the new risk has to be assessed correspondingly. The strategy of zero-trust has gained popularity as a scalable security architecture that is readily extendable to devices and networks, enhances visibility and control and aids in faster threat detection and response. It is rapidly becoming widely used, with 30 percent of Canadian businesses surveyed having fully adopted zero-trust across the organization and 40 percent in the process of deploying it; only one in seven is undecided or not considering it. Enterprises are leading the way, with 93 percent either implementing it or planning to in the next year.

As a zero-trust strategy is increasingly becoming an organizational imperative, some organizations may still face challenges in the adoption and management of zero-trust. The most common challenges organizations face include legacy applications and infrastructure, increased governance and management, and lack of standardization.

For the vast majority (80 percent), adoption of zero-trust is faster and easier than expected or as expected; however, it is slightly more challenging for midsize companies. One of the reasons for this could be the lack of an identity and access management (IAM) program in the midsize organization segment. As per IDC's IT Advisory Panel survey 2021, only 48 percent of midsize organizations in Canada have adopted an IAM program, compared with 70 percent of organizations in the enterprise segment.

Chart 20

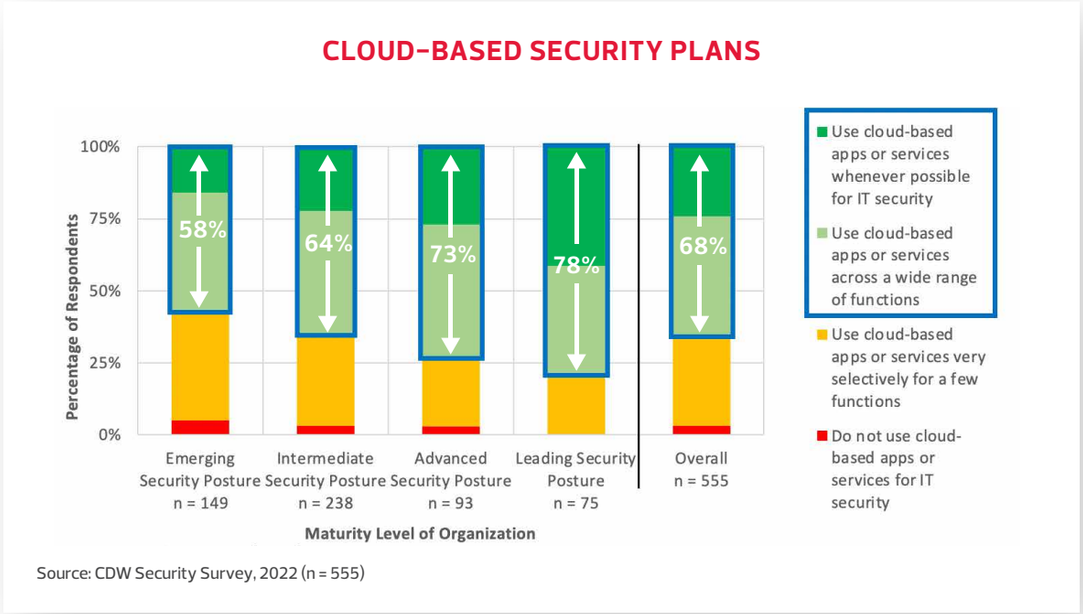


Source: CDW Security Survey, 2022 (n = 383)

Trusting Security Innovation in the Cloud

Over two thirds of all organizations (68 percent) trust IT security in the cloud. Those at a higher maturity scale have a much higher adoption rate of cloud-based security. Advanced technologies such as AI, machine learning (ML) and threat intelligence are being increasingly integrated into security technologies. The volume of security data that needs to be analyzed in real time has exploded, putting immense pressure on on-premises storage and computing capabilities. Consequently, cloud is becoming the centre of cybersecurity innovation, and mature organizations are adopting it to leverage these enhanced capabilities. Also, moving away from appliances to cloud-based security allows organizations to reduce ongoing maintenance, patching and refresh/upgrade and can provide better protection at a lower cost.

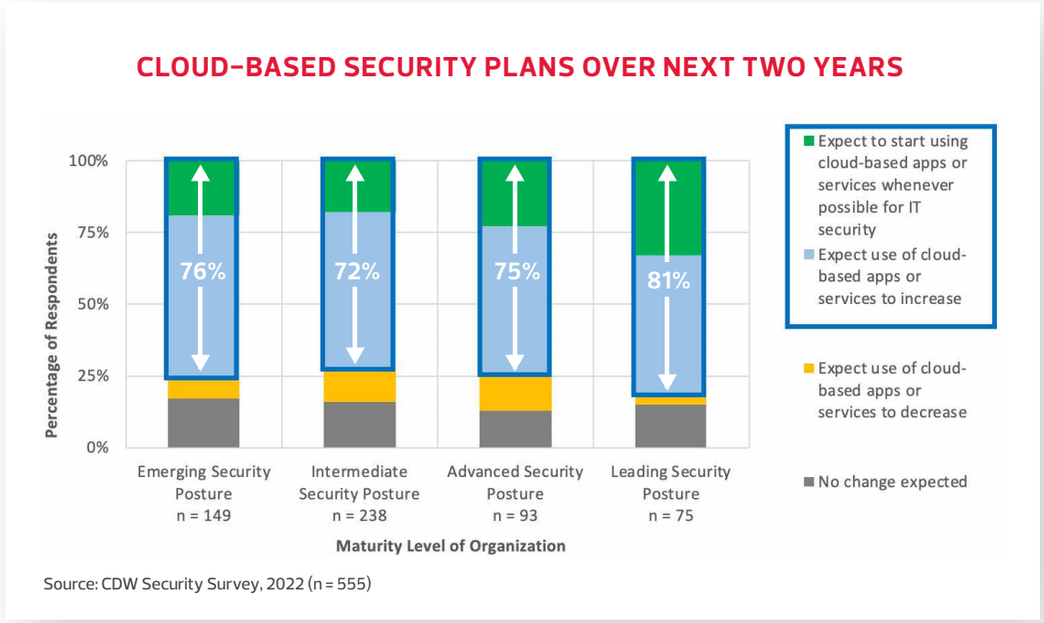
Chart 21



Source: CDW Security Survey, 2022 (n = 555)

Adoption of the cloud for security apps and services will increase across organizations at every maturity level, with a large proportion of high-maturity organizations adopting a cloud-first strategy. This trend is true across business sizes and industries, with the exception that government respondents indicated that they intend to reduce their use of cloud for IT security.

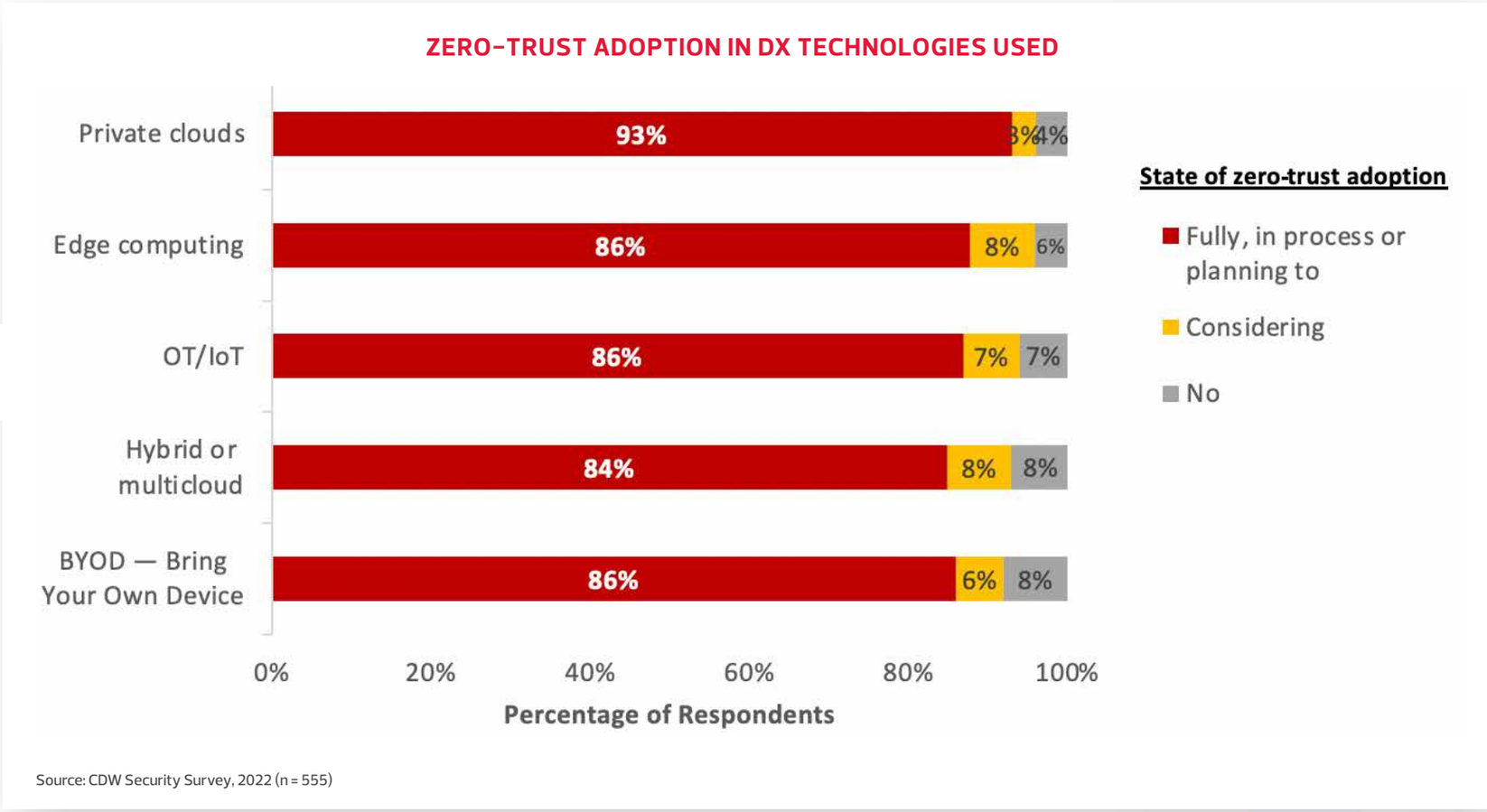
Chart 22



Source: CDW Security Survey, 2022 (n = 555)

The large majority of organizations implementing DX technologies have chosen to adopt a zero-trust architecture. Full implementation of zero-trust is slightly higher in organizations that use private clouds; organizations using edge computing and OT/IoT indicated strong adoption and consideration of zero-trust.

Chart 23



Source: CDW Security Survey, 2022 (n = 555)

FINDING 6: Canadian organizations that have adopted a cybersecurity-infused company culture report a better overall security posture.

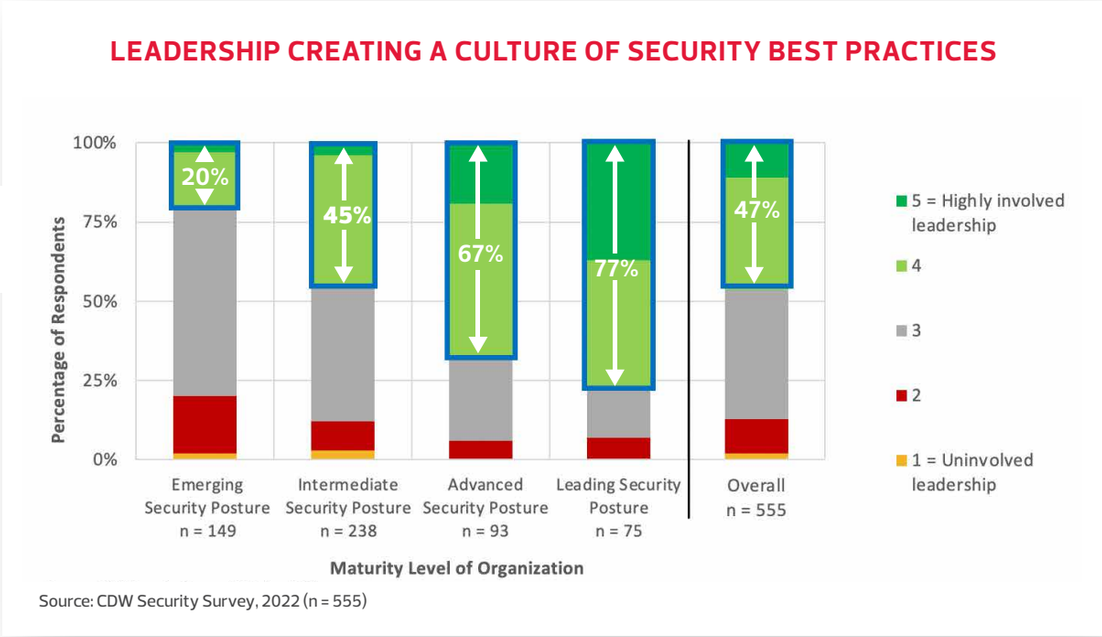
Cybersecurity is no longer only an IT problem but everybody's responsibility. Senior leadership involvement, improved overall security hygiene of users and secured application development are key attributes of a security-infused company culture.

Cybersecurity-Infused Company Culture Improves Maturity

The level of leadership (outside of IT) involved in creating a culture where best practices for security are ingrained in the organization is a determining factor in assessing an organization's level of security maturity. This has been observed in the correlation of maturity to positive outcomes. Business leaders need to understand current and future cyber risks to the organization and their impact to determine the optimum level of protection, including investment and resources. As cyberattacks increasingly make headlines, security has emerged as a critical differentiator amongst competitors across all industries.

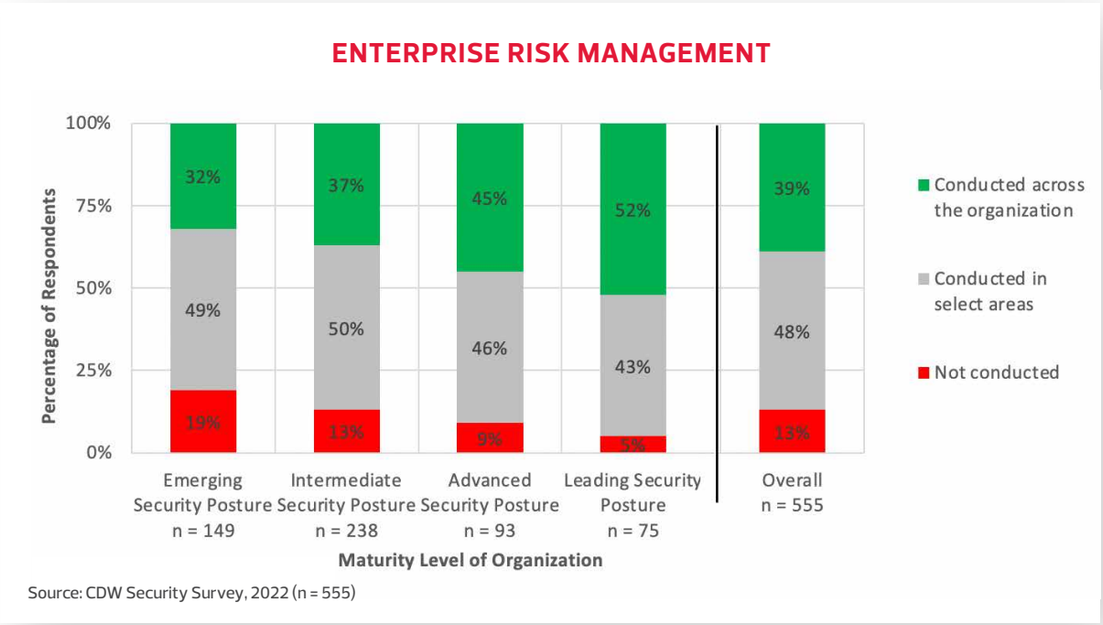
Organizations will continue to evolve and grow, and so will their reliance on cybersecurity. DX increasingly drives business operations, and with it the requirement of cyber risk to be part of enterprise risk management (ERM). ERM is reinforced through a security-infused company culture.

Chart 24



Source: CDW Security Survey, 2022 (n = 555)

Chart 25



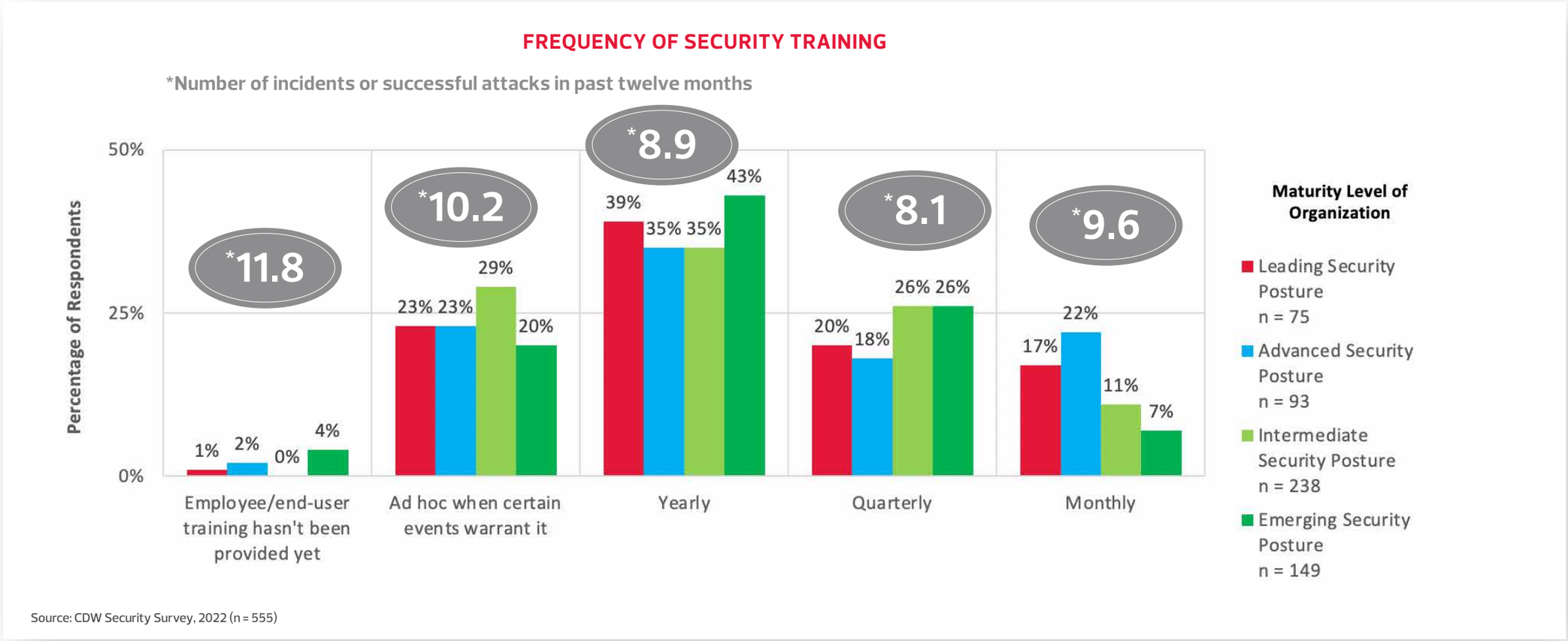
Source: CDW Security Survey, 2022 (n = 555)

Security Awareness Training

Tabletop exercises are beneficial for senior leadership and security teams as they take the teams through simulated security incident scenarios and provide hands-on training for incident preparedness. Attack simulation exercises and cyber ranges are effective ways of training security staff on how to detect and mitigate cyberattacks with the technology they have on the job. Beyond this, everyone in the organization needs to understand how to approach suspicious emails, how to keep company data safe, and how to create strong passwords and manage them. Security awareness training covers these topics and much more to ensure that poor security hygiene does not lead to a breach.

It is most common for organizations to require annual security awareness training to be set up in a constructive manner, as opposed to a blame and shame when running attack simulations – but data indicates a value in increasing this training to quarterly. Organizations that do quarterly security awareness training experienced fewer incidents or successful attacks than any other training frequency. Monthly security awareness training did not result in fewer incidents.

Chart 26



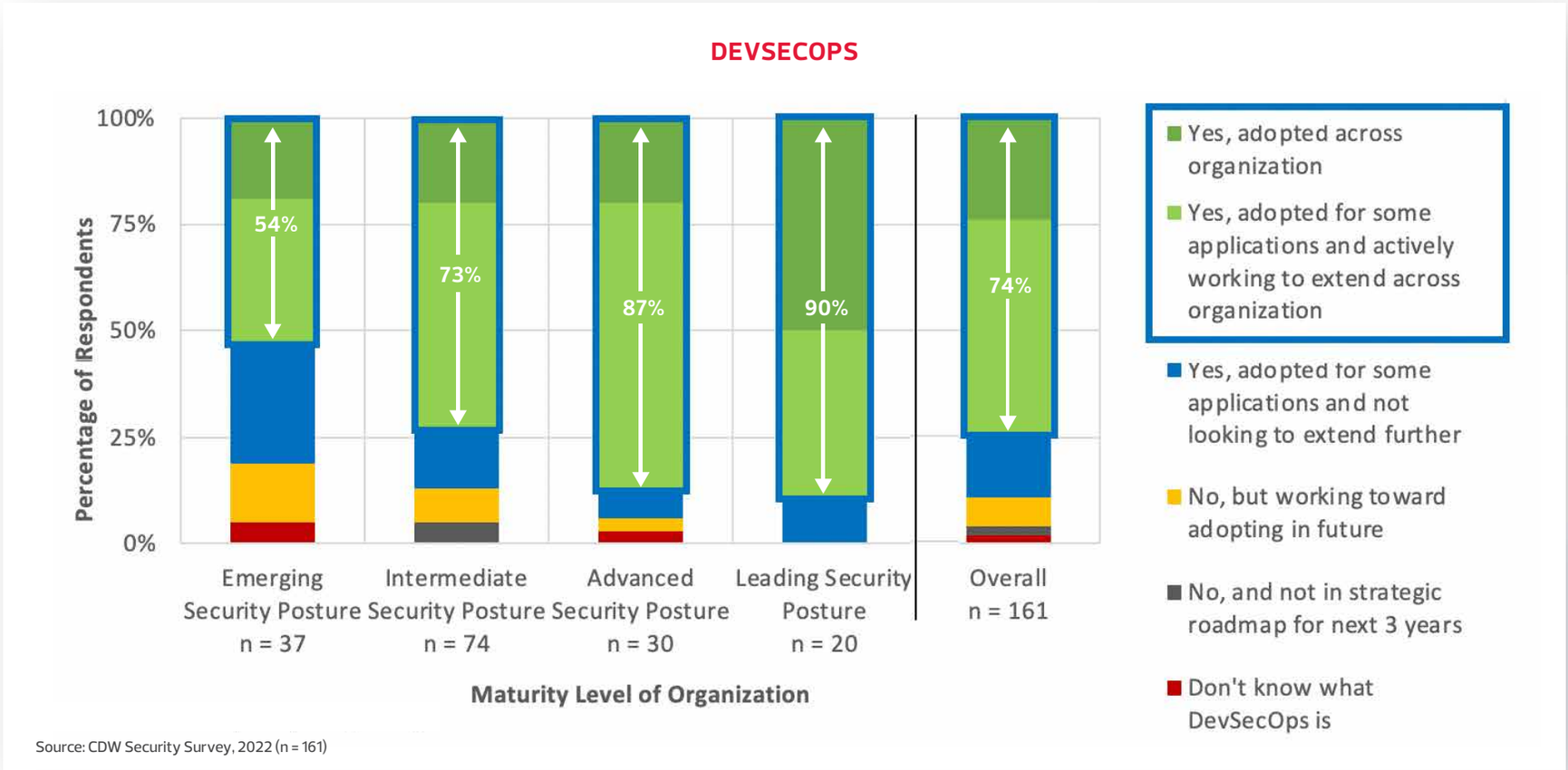
Source: CDW Security Survey, 2022 (n = 555)

Adoption of DevSecOps

Secure Development Lifecycle (SDLC) is foundational to a sustainable DevOps culture. DevSecOps brought along a culture shift in software development, with the aim to embed security into the rapid-release development cycles that are typical of modern application development and deployment (referred to as the DevOps movement). The shift to DevSecOps is intended to embed security testing into the continuous integration (CI) and continuous delivery (CD) pipelines while in parallel building needed security knowledge and skills in the development team.

Of those organizations that have internal DevOps, 73 percent have either adopted organization-wide DevSecOps or are in the process of rolling it out to the entire organization. Nearly all (90 percent) of the most mature organizations employ DevSecOps, and more than half of even the least mature organizations employ it.

Chart 27



Source: CDW Security Survey, 2022 (n = 161)

Recommendations and Call to Action

I. Pause and Assess

It is crucial to pause and assess the cyber risk facing your organization and the ability of your security program to mitigate these risks.

The journey to mature IT security begins with an assessment of your current state, setting a vision of your future state and defining a roadmap to guide you.

The assessment must be multifaceted, evaluating people, processes and technologies. Many organizations have already invested in capable security technologies but have not deployed them in a manner that adequately addresses the risks their organization faces.

No matter where you are on this journey, it's important to evaluate your organization's cyber risk, as well as the capabilities of your existing security controls, processes and available skills — all with the objective of mitigating the business risks of a cyberattack. Only then can IT and security leaders secure business leadership buy-in and sponsorship for a long-term security roadmap that aligns with the business goals.

Consider the following as you advance in security maturity:

- Modernizing security can be a big expense; ensuring that money is well spent is critical. Comprehensive risk assessments can equip security leaders with data to educate business managers on the risks associated with the IT systems and to prioritize security investments, both in terms of which systems present the greatest risks and which measures provide more value for your investments.
- Any risk assessment must include identification and prioritization of critical data, assets, applications and services (DAAS). Without this prioritization, it is impossible to allocate security resources where they are needed most.
- Regulatory requirements like security risks must be identified, understood, communicated and prioritized to ensure that new security tools and processes are shoring up existing security and compliance gaps without introducing new ones.
- Modernization efforts with a focus on third-party risk management can help mitigate the threat of noncompliance with new and evolving regulatory requirements like Quebec's Bill 64 or the proposed Bill C-11, which introduce stringent data security and privacy standards that extend to third parties and have harsh penalties for infractions.
- IT environments have become more complex over the years, so risk assessment methodologies must evolve to address new deployment paradigms, and must be updated at the same or a greater rate than IT systems. An assessment by an external security partner provides expertise, the latest methodologies and an objective analysis of cyber risk and security gaps within an organization's digital ecosystem.

Organizations need to create a solid foundation for security transformation, and taking the time to pause and assess is the starting point. A comprehensive understanding of where IT is today and how it will evolve in the future will reduce the number of piecemeal solutions that don't support a holistic security approach and will streamline investments in security processes, technologies and skills acquisition for the future.

II. Rethink Security with Zero-Trust

Users, not their devices or their methods of access, are central to the concept of trust. Enabling those who require access to data and resources puts identity at the core of zero-trust, in order to enable least-privileged access, continuous authentication and authorization, and risk-based access control for enterprise networks, applications and data. Canadian organizations need to develop a comprehensive security policy for access to enterprise resources, consolidate identity management systems to create one single version of truth, and recognize identity and data governance controls.

Recommendations to help achieve this outcome:

- Adopt a security architecture based on the principles of zero-trust, multilayered protection and security stack optimization, to drive integration and automation within security workflows and ease of management.
- Review your environment and create your own unique zero-trust roadmap — there is no single product, solution or SKU that can be purchased. Rightsizing your investments based on your "Pause and Assess" risk assessment is the key to optimal zero-trust adoption; overpaying for unnecessary security carries its own set of risks, while missing key components can be disastrous.
- Adopt multilayered protection to secure customers, users, data and infrastructure to slow down the progression of attacks and to create multiple points for threat detection and response. Multiple point solutions may lead to security stack fragmentation and complexity; hence organizations must evaluate offerings like secured access service edge (SASE) to integrate network management and security capabilities.
- Evaluate the potential for security orchestration, automation and response (SOAR) to streamline threat management across the security operations centre (SOC). SOAR can help optimize the utilization of your human security resources by increasing the visibility of resources and threats and automating alerts, response, reporting and metrics.

Zero-trust requires an organizational commitment to security. A piecemeal or point-in-time approach can increase your operational risks from both security and productivity standpoints.

Vulnerabilities in IT assets — including endpoints, servers, storage systems, applications and even security controls — weaken the design principles of zero-trust. Known vulnerability exploits, misconfigurations and zero-day bombs are among the leading delivery mechanisms for advanced threats like ransomware. Traditional vulnerability assessments are generally limited to vulnerability scans and patching, which may be sufficient for regulatory compliance but fall significantly short of risk mitigation goals. Canadian organizations must adopt a formal, risk-based vulnerability management program that combines asset network information, vulnerability assessment data and threat intelligence for effective prioritization and remediation.

Your organization should conduct adversarial testing like penetration testing and red team exercises to evaluate the impact of vulnerabilities and exposures to your security posture and how they can be exploited by cyber attackers. This is also an effective way of evaluating the remediation practice of your vulnerability management program. It provides an opportunity to re-educate employees, test and adapt/reinforce processes, and understand how and where technologies are succeeding or failing to reduce risk.

III. Embrace Cloud for Cybersecurity

Security solutions like SASE, zero-trust network access (ZTNA), extended detection and response (XDR), SOAR and others are primed for digital transformation and inherently need to be built upon modern architectures. This includes the need for solutions built on cloud-native technologies such as containerization and serverless functions for elastic scalability, with microservices designs and API integrations for the expansion of new features and functionality to meet the needs of the modern, digital workforce and its customers.

- On-premises email security should be migrated to cloud for advanced capabilities like compliant archiving, secure messaging with encryption, email sandbox and phishing protection.
- Organizations that are highly distributed (many branch offices, sites or locations) or ones with a significant share of hybrid workforce could be well served by SASE. The integration of networking and security capabilities provides security teams with ease of deployment and management, scalability of the solution, and faster upgrades and patching — but the transformational value lies in its role in enhancing monitoring, threat detection and response.
- Security monitoring, threat detection and automated response capabilities increasingly rely on AI/ML algorithms. Analyzing telemetry from endpoints, networks and applications to detect advanced threats, alerts aggregation and behavioural analytics require scalable computing and storage capabilities. Implicitly, innovation in detection and response capabilities is increasingly tied to adoption of cloud for such crucial security functions.

A "cloud-first" approach to security not only takes advantage of all that cloud has to offer to build agile, secure and cost-effective solutions but also enables flexibility for transformative initiatives like threat hunting, digital forensics, data loss prevention and enhanced threat detection and response.

IV. Restore Trust in your Backups

The growing adoption of hybrid and multicloud and the increasing number of storage levels offer both operational and security benefits for organizations. In line with this diverse and complex enterprise IT infrastructure, businesses need to modernize their backup and recovery strategy to continue to align with business goals like RPO and RTO.

Recommendations:

- Organizations often target aggressive RPO and RTO objectives but fail to test their backup and recovery strategy to measure its alignment with business objective. Test your backups and recovery plan.
- Adopt a backup and recovery strategy that is tiered with the criticality of data and systems. With the increasing popularity of cloud, backup and storage organizations can achieve higher levels of continuity and retention.
- As modern attacks like ransomware increasingly target backup systems, invest in the protection of backups and administrator controls. Encryption, malware scanning across backups, anomaly detection and multifactor authorization for administrative workflows are crucial to protecting backups from adversaries.

Backup and recovery processes are the last line of defence for organizations against cyberattacks, including ransomware and especially deletion- and encryption-based attacks. Having a unified, modern data backup and recovery solution is crucial to providing quick recovery in the event of a cyberattack. According to IDC's IT advisory panel N2 2022, over 60% of respondents feel that they will not pay a ransom due to their confidence in their backup and DR systems.

V. Create a Culture of Security Ownership

Culture change that evolves from within existing organizational values, principles and processes tends to be the most effective and successful. Raising the level of security maturity will positively affect many areas, but it must include business leadership. Security- and privacy-related KPIs must be reported to leadership and to the broader organization to drive cultural change within the organization. The protection of enterprise systems and data is everyone's responsibility and must be part of an organizational culture that values security as a competitive differentiator.

Additional recommendations:

- Define the elements that make up a culture of security and privacy within an organization. The various parameters could include leadership awareness of security risks, the IT hygiene of staff, third-party selection and management, secure application development and the reporting of security and privacy KPIs in annual reports, marketing collateral, etc.
- Regularly report on KPIs for security culture elements to leadership and the broader organization to reinforce the organizational commitment to drive cultural change. Some of the KPIs to be reported internally for privacy could include:
  - Compliance with regulatory standards
  - Percentage of employees on awareness trainings
  - Number of privacy-related complaints
  - Notifications of privacy breaches
- Track security resource optimization KPIs and indicators of improvement, and report these to business leaders. Example of KPIs could be:
  - Overhead spending on security resources
  - Overhead spending on security training
  - Number of certifications held by security team
  - Voluntary turnover of security team
  - Total number of security events within a time frame

Communicating these KPIs is crucial if security leaders want everyone within the organization to feel accountable for security and drive the cultural change. Periodic communication must be complemented by necessary trainings – for example, tabletop exercises for leadership, attack simulation for security teams and security awareness trainings for everyone in the organization to improve the overall commitment to security within the organization.

Analysis has shown that increased security maturity pays off. Canadian businesses rated at the top in IT security maturity reported both higher business outcomes (revenue, profit, regulatory compliance, operational costs, number of new products and services) and higher levels of business improvements compared with their counterparts.

For high level results, read our executive summary here.

APPENDIX A: DETAILED SURVEY RESULTS

Demographics

A sampling frame of 1,652 Canadian IT security and risk & compliance professionals were selected to receive invitations to participate in this survey. All survey participants were screened for direct involvement in improving or managing their organization's IT security. The following table shows the returns, including the removal of certain participants based on screening and reliability checks. Our final sample consisted of 555 surveys, or a 33.6 percent response rate.

The survey firmographics and demographics are as follows:

Which of the following industry categories best represents the principal business activity of your organization?

	Total
Base: All Respondents	**555**
Business/professional services (e.g., legal, accounting, engineering, architecture, etc.)	5.2%
Personal/consumer services (e.g., travel, beauty, personal training, dry cleaning, etc.)	4.0%
Construction	3.8%
Hospitality	3.2%
IT industry	6.7%
Not for profit	0.0%
Manufacturing	10.5%
Crown corporation or other publicly funded organization	0.0%
Education, K–12	3.1%
Education, college/university	6.3%
Financial services	10.1%
Government	9.4%
Healthcare	9.9%
Primary (e.g., agriculture, mining, forestry, etc.)	0.9%
Oil & gas or field services–related	2.7%
Retail	7.0%
Communications (e.g., cable and telecommunications services, etc.)	2.9%
Media (e.g., radio/TV broadcasting)	2.7%
Printing, publishing, etc.	2.2%
Transportation and warehousing	2.7%
Utilities	4.0%
Wholesale and distribution	2.9%

At your organization, do you play a role in or are you part of the following functions?

	Total
Base: Respondents	**555**
Directing the IT function	46.8%
Improving/managing IT security	100.0%
Setting IT priorities	45.2%
Managing IT budgets	25.9%

Is your company headquartered in Canada — and if so, which of the following areas is it headquartered in?

	Total
Base: All Respondents	**555**
Not headquartered in Canada	13.0%
Western and Central Canada (BC, AB, SK, MB)	24.7%
Ontario	27.7%
Quebec	22.5%
Atlantic Canada (NB, NS, NFLD, PEI)	12.1%

Which of the following best describes the department you work for?

	Total
Base: All Respondents	**555**
C-level executive management, excluding IT	7.4%
C-level IT, including CIO/CTO/CSO/CISO	9.2%
IT/IS/MIS/data centre/IT security	69.9%
Legal/compliance/risk	13.5%

How many full-time employees does your organization have located within Canada?

	Total
Base: All Respondents	**555**
15–24	7.6%
25–99	7.0%
100–249	10.1%
250–499	21.6%
500–999	14.6%
1000–4999	13.9%

Which of the following ranges would your organization's annual revenue (or budget for government) fall under?

	Total
Base: All Respondents	**555**
Less than $10 million	1.6
$10 million–$25 million	10.1
$26 million–$99 million	11.9
$100 million–$499 million	34.1
$500 million–$999 million	27.0
$1 billion or more	15.3

APPENDIX B: DEFINITIONS

Analytics: Using statistical analysis to discover and interpret patterns in data.

Artificial intelligence (AI): Mimicking the natural intelligence of humans using machine learning and statistical models.

BYOD (Bring Your Own Device): In the workplace context, the practice of allowing employees or other personnel and/or third-party partners to use their personally owned devices for work purposes, including connecting to the organization's network and accessing work-related systems.

Continuous delivery (CD): Automates the deployment of all source code changes to a testing or production environment after the build stage.

Continuous integration (CI): The practice of automating the integration of code changes from multiple developers into a single repository.

Denial of Service (DoS): An attack in which multiple compromised systems are used to attack a single target. The flood of incoming messages to the target system forces it to shut down and denies service to legitimate users.

DevOps: Combines software development (Dev) and IT operations (Ops) to shorten development lifecycle with continuous delivery and integration.

DevSecOps: Augmentation of DevOps; aims to automate integration of security at every phase of software development.

Edge computing: A distributed IT architecture that enables client data processing at the periphery of the network, as close to the originating source as possible.

Exfiltration: The unauthorized removal of data or files from a system by an attacker.

Infiltration: Unauthorized access to any computer network or system resource. Attackers gain access to an organization's network, infrastructure and/or data, but no data is exfiltrated.

Isolated recovery environment (IRE): A dedicated, secure recovery environment that enables verification and recovery of data from backups.

Machine learning (ML): Using algorithms to create models capable of classification. An algorithm uses training data to build a model capable of classifying new instances in test data based on patterns it "learned" in the training data.

Phishing: Disguising malicious intent within a digital forgery of a communication from trusted entities such as banks, government agencies, charities, etc., to gain sensitive information from individuals. Phishing attacks are usually carried out at scale, looking for targets of opportunity instead of a specific individual.

Recovery point objective (RPO): A target for a point in time from which backup files can be restored.

Recovery time objective (RTO): A target time to recovery after a service interruption caused by a natural disaster, power outage, cybersecurity incident, etc.

Secure access service edge (SASE): A network architecture that combines software-defined wide area networking (SD-WAN) and security into a cloud service permitting scale-up/down flexibility and usage-based billing.

Security orchestration, automation and response (SOAR): A group of security controls, usually managed using a single pane of glass, that aids analysts in responding to security threats. Depending on the implementation, a significant amount of artificial intelligence may be built into the solution, allowing low-level alerts and events to be responded to automatically without human intervention.

Secure Development Lifecycle (SDLC): Involves integration of security testing into existing development processes.

Shared responsibility model: A cloud security framework that dictates the security responsibilities of a cloud services provider (CSP) and its users to ensure accountability. How CSPs' versus a user organization's responsibilities are defined varies between CSPs and the services being provided (SaaS, PaaS, IaaS), so it is imperative that user organizations clearly understand what security responsibilities their CSPs will take ownership of versus responsibilities the organization will retain.

Spear phishing: A phishing attack created to target a specific individual or organization.

Zero-trust architecture: Unlike traditional perimeter security architectures, which trust all individuals and applications inside the perimeter, zero-trust architectures trust no one on either side. Identity and access management is a critical component of zero-trust architectures.

ABOUT CDW

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.

ABOUT IDC CANADA

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services and events for the information technology, telecommunications and consumer technology markets. IDC Canada is part of a network of over 1100 analysts providing global, regional and local expertise on technology, industry opportunities and trends with more analysts dedicated to understanding the Canadian market than any other global research firm.

CDW PEOPLE WHO GET IT™

IDC

Research independently conducted by IDC Canada | Published May 2022