CYBERSECURITY IN 2022: ADVANCING THE MATURITY OF CANADIAN ORGANIZATIONS

Protecting Digitally Transforming IT in an Era of Increasing Threat

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 ever-increasing and nefarious threats. Risks 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 presents an assessment of the state of IT security and issues facing Canadian businesses today, and offers insight for progressing toward more robust security.

The Rapidly Evolving Threat Landscape and Resourcing Constraints

The number of IT connected devices is exploding.
Even the number of servers, a fairly mature technology, has more than tripled. As the attack surface grows, so do new vulnerabilities and associated cyber risk, as evidenced in a growing number of cyberattacks.

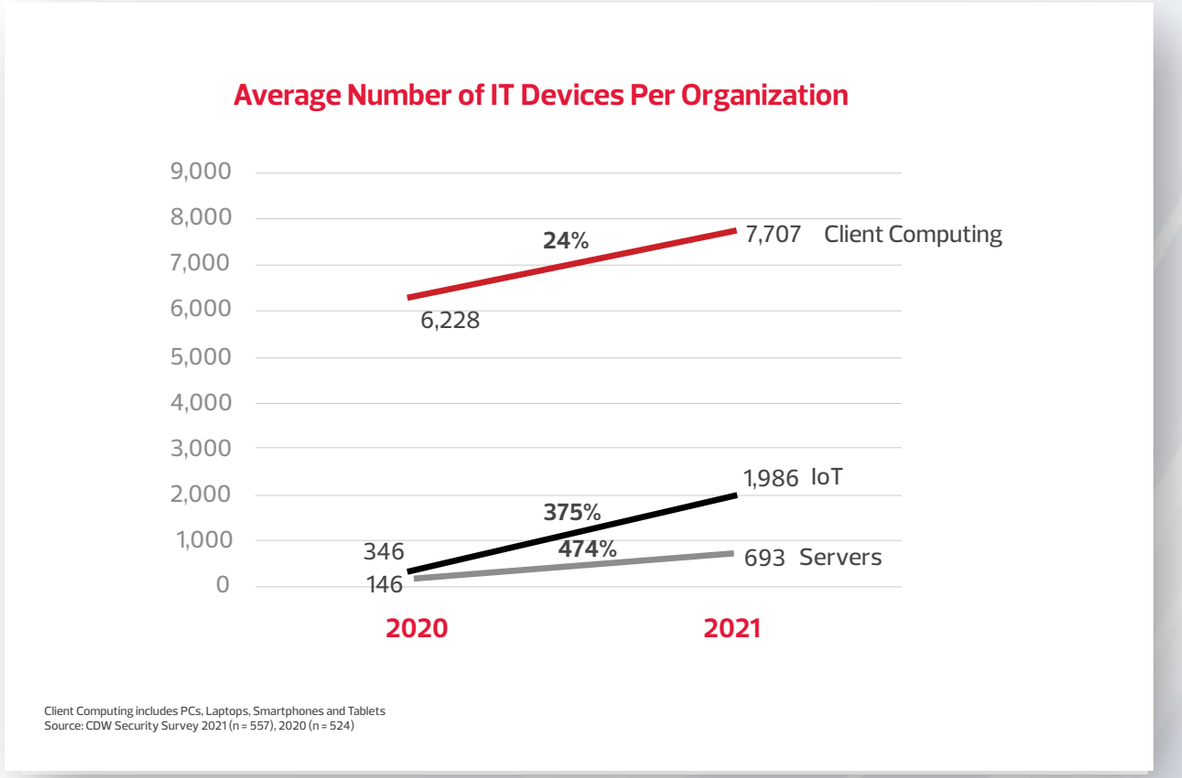
Ninety percent of Canadian businesses surveyed indicated that they have been attacked in the past year.

Regardless of size, industry or location, everybody gets attacked.
Public cloud servers are the new hot target. Cyberattackers are evolving into a well-connected and organized industry, and attacks are more sophisticated than ever before. It takes a lot less than before to compromise an organization's IT infrastructure.

Downtime is costly.
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.

While security is a top concern, many Canadian companies struggle to adequately fund it.
Half of Canadian organizations report 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.

There is a security skills gap.
Fifty-seven percent of organizations report having gaps in resource staffing and/or security skills. 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.



Client Computing includes PCs, Laptops, Smartphones and Tablets
Source: CDW Security Survey 2021 (n = 557), 2020 (n = 524)

A Maturity Model for IT Security

The journey to increased IT security begins with an assessment of your current state and a clear, well-defined final state. CDW has developed a model for assessing an organization's levels of IT security maturity along four dimensions, based on this year's survey.

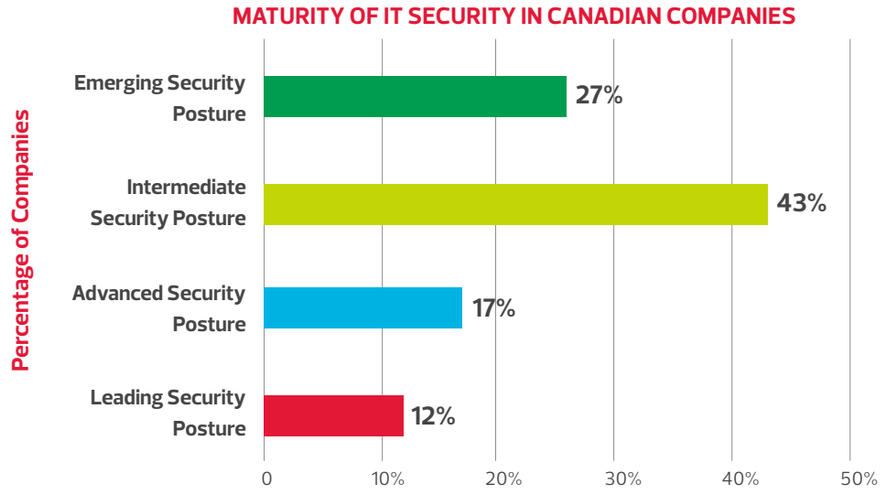
Security Approach	Security Philosophy	Security Investments	Security Processes
Executive leadership (outside of IT) building a culture of security best practices. **Resourcing IT security** – both staffing and development of staff skills **Breadth of investment** in core operations, new initiatives and experimental approaches.	**Zero-trust** adoption **Integration** of IT security processes and tools **Repeatable and consistent** IT security processes and workflows	**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, staff training) **Backups** – security, regularity, authentication

Based on these dimensions, only 12 percent of Canadian companies have a leading security posture.

All organizations should understand their starting point, strengths and weaknesses. This will allow organizations to optimize their processes, investments and culture and transform IT security. All businesses, regardless of size, can implement robust IT security practices.

Business outcomes follow.

Organizations 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 over the past two years compared with all others.



KEY FINDINGS

Cloud Is the New Battleground

- Cloud computing continues to be at the heart of modern IT.
- More than half of Canadian businesses have adopted hybrid or multi-cloud infrastructure.
- Attacks on cloud services by criminals, hackers and nation-states are growing.
- Public cloud is the top attack target, followed by internal applications, networks and web applications.

Shared responsibility creates complexities.

What makes the cloud complex is that the responsibility for security is shared between the provider and the business, and the responsibility changes by cloud deployment model. Factors that make the cloud attractive can also make for challenging or limited visibility and control, and new skills and toolsets are needed to monitor and secure cloud IT environments.

To secure cloud IT environments, organizations must make appropriate investments to close the gaps in cloud governance and risk management, deployment of security controls to prevent threats, monitoring and detecting threats, and automated response.

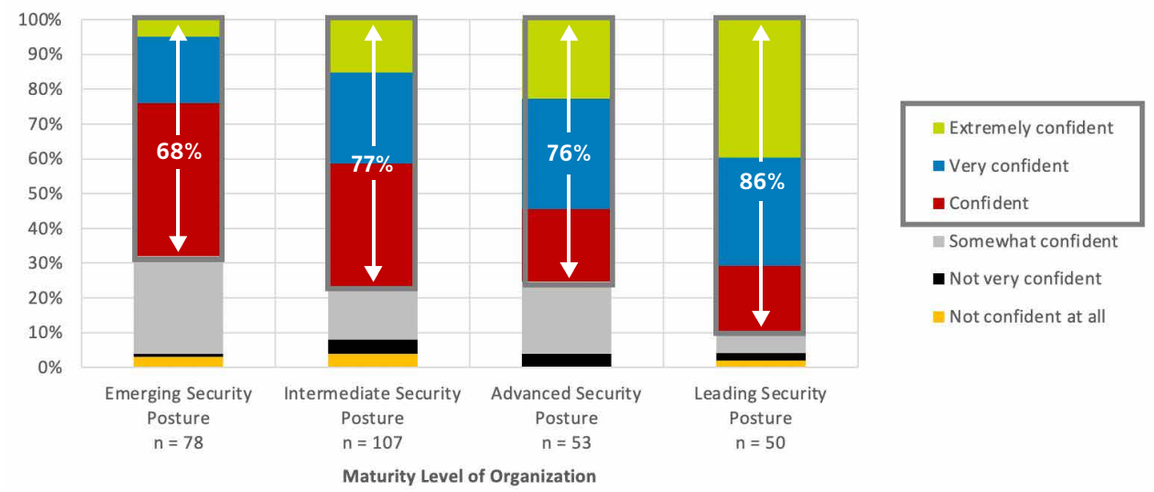
These efforts have a direct payoff.

Organizations that measure higher in IT security maturity have greater confidence in their cloud security efforts and resulting IT security.

DX TECHNOLOGIES USED BY CANADIAN BUSINESSES

Hybrid or Multi-Cloud	52%
OT/IoT	41%
Edge Computing	38%
Private Clouds	35%
DevOps	29%
BYOD (Bring Your Own Device)	28%

CONFIDENCE IN HYBRID/MULTICLOUD IT SECURITY



Source: CDW Security Survey 2022 (n = 288)

Ransomware: The Menace Impacting Canadian Organizations.

Regardless of company size or industry, everyone is on the radar of cyberattackers.

Ransomware is so rampant that it is amongst the biggest cyber risks facing organizations today. Without a thorough forensics investigation, root cause analysis and eradication, ransomware reinfection is possible. These back doors are often sold to other attack groups or reused by the same group for another attack.

73% of Canadian companies surveyed reported having experienced data infiltration attacks with ransom demands in the past year.

Return to trusted state with a response and recovery plan.

An up-to-date and tested response and recovery plan is crucial for attack containment and eradication, root cause analysis, smooth recovery from backups and communication to all key stakeholders. Consequently, recovery from ransomware or any other cyberattack can be optimized, reducing downtime and costs.

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

RESPONSE AND RECOVERY PLANS

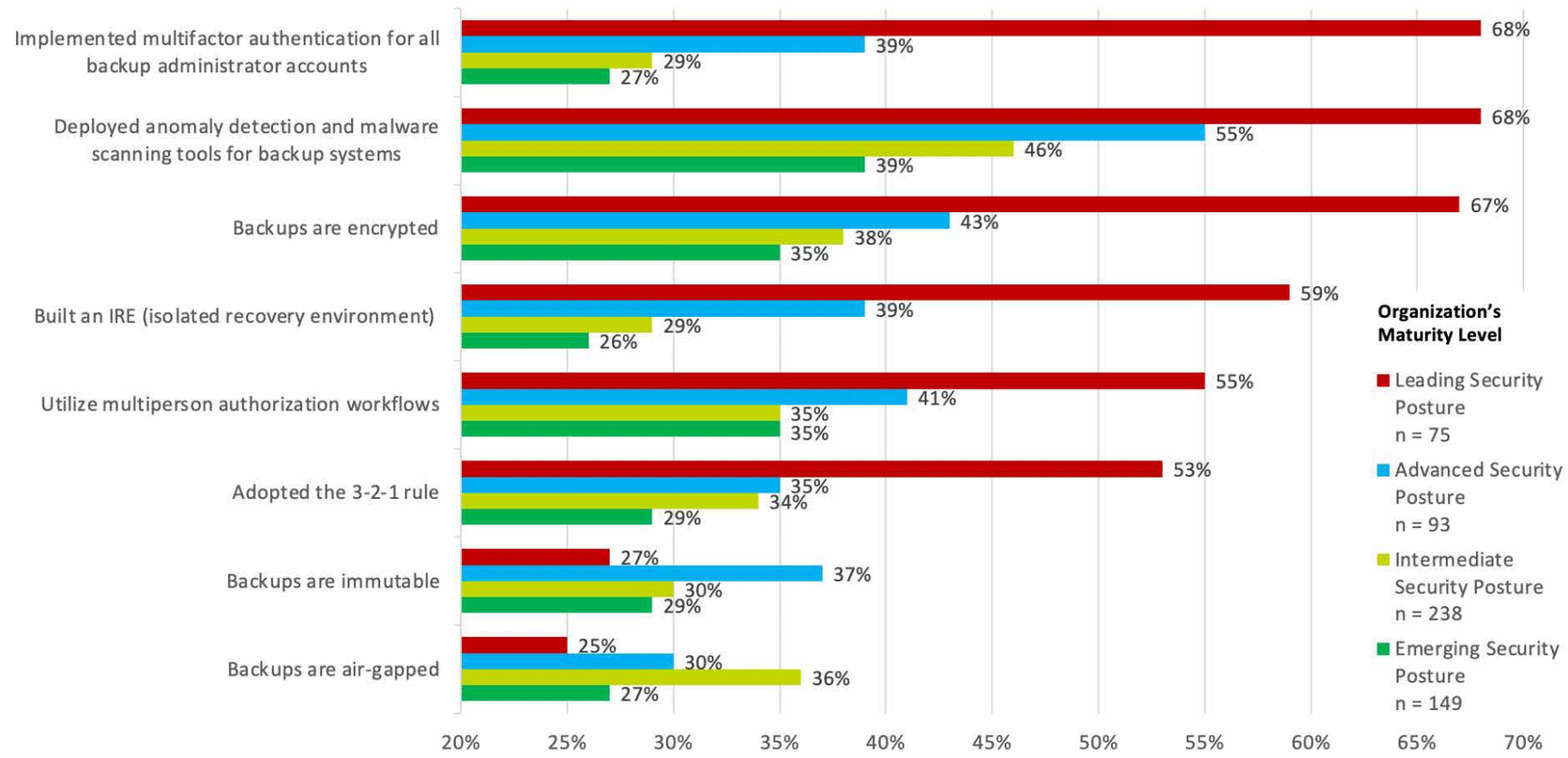
Source: CDW Security Survey 2022 (n = 555)

Backup and Recovery Strategies of Canadian Organizations Fall Short

- Only 36 percent of Canadian organizations were able to fully restore their data and systems from backups when needed.
- Twenty-one percent reported an inability to recover at all.

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 in security incidents. For the affected organizations, assessing the reliability of backups during a cyberattack is a leading cause of slow recovery.

BACKUP MEASURES ADOPTED



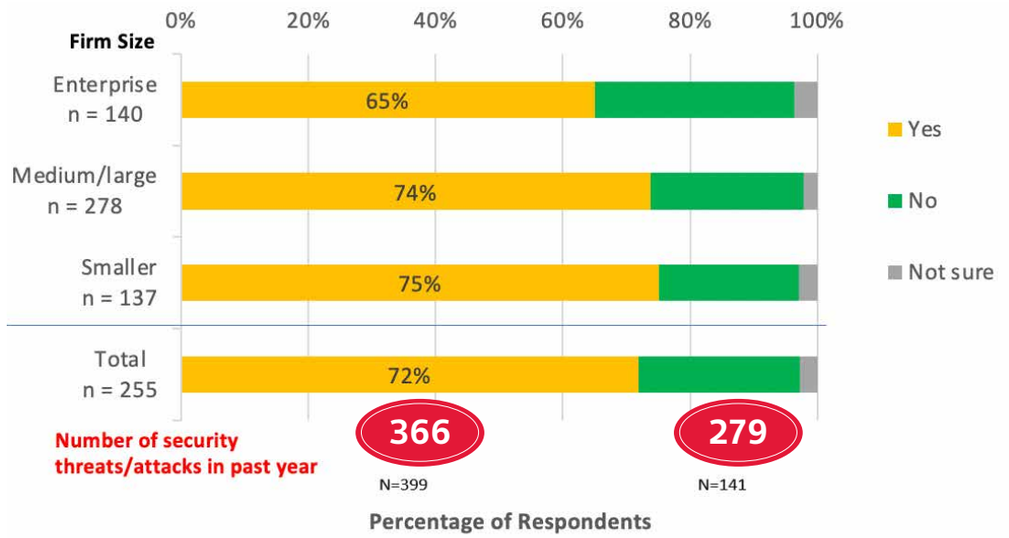
Learn from the best.

Mature organizations have invested in a variety of measures to improve their security, developing and maintaining a robust recovery plan.

Overexposure of Personally Identifiable Information Expands Attack Surface

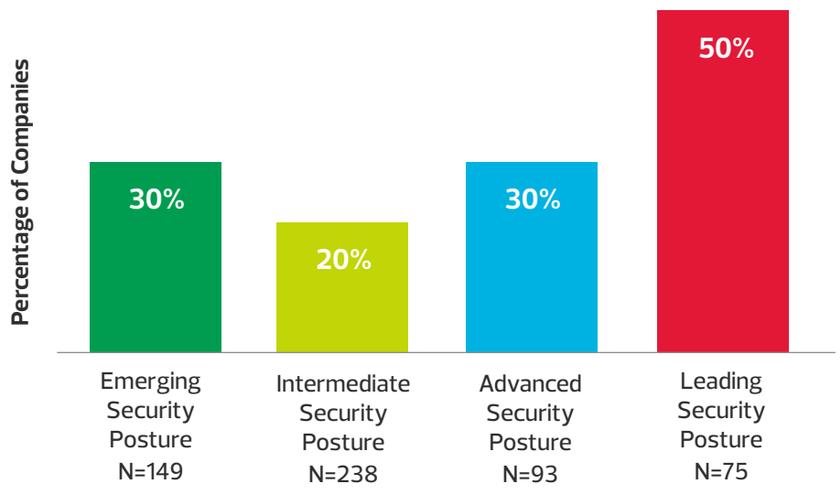
Organizations that have personally identifiable information (PII) accessible to third parties suffered 31 percent more cyberattacks within a span of 12 months compared with those that don't have PII within their IT environment exposed to third parties.

EXTERNAL ACCESS TO PII



Source: CDW Security Survey 2022 (n = 555)

THIRD PARTY RISK ASSESSMENT PERFORMED



Source: CDW Security Survey 2022 (n = 555)

72% of Canadian organizations surveyed indicated that their suppliers, partners and contractors have access to PII contained in IT, operational technology (OT) or databases.

Effectively managing access to PII data is crucial for businesses to identify and mitigate the risks relating to use of third parties. A security plan containing a comprehensive third-party risk assessment is an indicator of an increased security maturity level.

Zero-Trust Is Becoming a Preferred Security Architecture

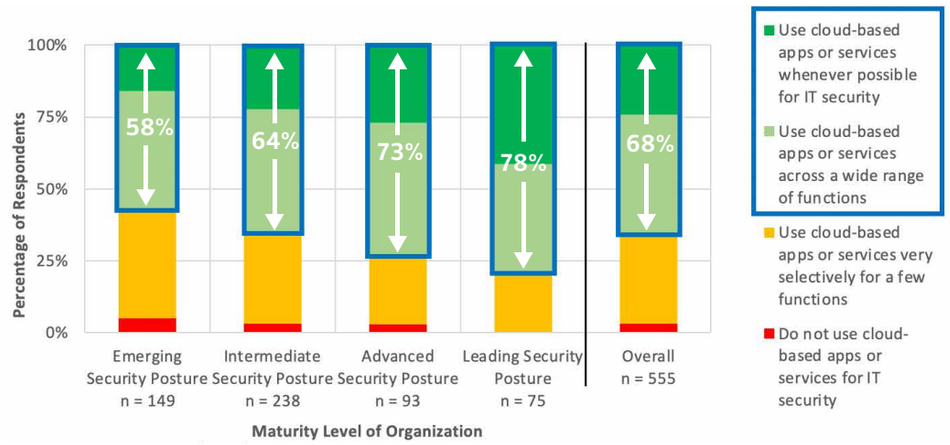
The future is a hybrid workforce, and a hybrid workforce means expanded attack surface.

According to Stats Canada, in 2020, 40 percent of employees found themselves transitioning to working from home, and numbers went as high as 70 percent for workers in certain industries. 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[1].

Zero-trust strategy is becoming widely used.

- Thirty percent of Canadian businesses surveyed have fully adopted zero-trust across their organization.
- Forty percent are in the process of deploying it.
- Only one in seven (14 percent) is undecided or not considering it.
- Enterprises are leading the way, with 93 percent either implementing it or planning to in the next year.
- Organizations adopting numerous digital transformation technologies have all chosen in favour of zero-trust architecture.

CLOUD-BASED SECURITY PLANS



Source: CDW Security Survey 2022 (n = 555)

Over two thirds (68 percent) of all organizations trust IT security in the cloud.

Those at a higher maturity scale have much higher adoption rates of cloud-based security. Advanced technologies such as artificial intelligence (AI), machine learning (ML) and threat intelligence are being increasingly integrated into security technologies.

[1]IDC's Canadian Return-to-Office Forecast, November 2021

Cybersecurity-Infused Company Culture Improves Maturity

Cybersecurity is no longer only an IT problem but everybody's responsibility.

- Leadership *outside of IT* being 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.
- Business leaders need to understand cyber risks and their impact to determine the optimum level of protection, which includes investment and resources.

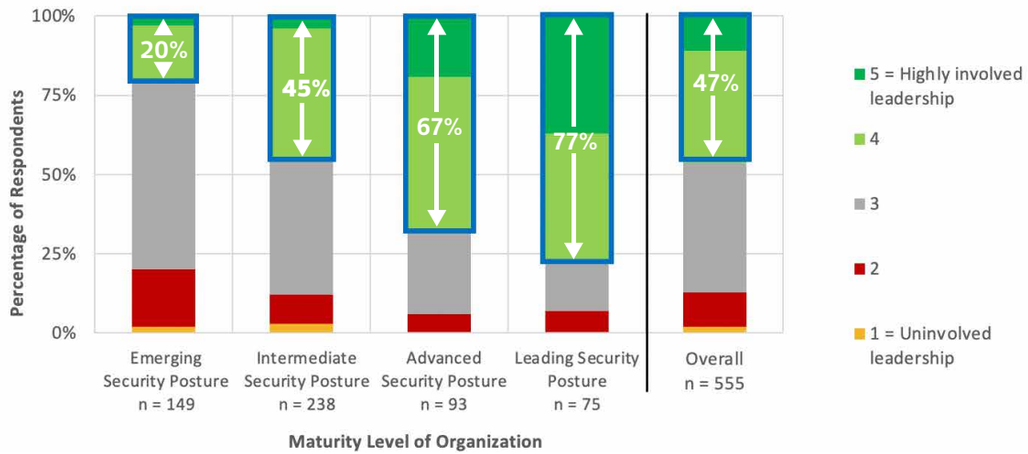
Train quarterly.

- Organizations that do quarterly security awareness training (SAT) experienced fewer incidents or successful attacks than organizations with any other training frequency; even monthly SAT did not result in fewer incidents.
- 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.

Adopt DevSecOps.

- Secure Development Lifecycle (SDL) is foundational to a sustainable DevOps culture. DevSecOps embeds security into rapid-release development cycles.
- 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 over half of even the least-mature organizations employ it.

LEADERSHIP CREATING A CULTURE OF SECURITY BEST PRACTICES



Source: CDW Security Survey 2022 (n = 555)

Recommendations and Calls 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. This assessment must include people, process and technology to accurately reflect your current state, set a vision of your future state and define a roadmap to guide you.

II. Rethink security with zero-trust.
Digital transformation is disrupting traditional security. Canadian organizations need to adapt their approach to security to ensure they have the required resilience as their business evolves. Rethink security through the zero-trust model to focus on protecting enterprise infrastructure, applications and data based on identity and trust of both users and devices.

III. Embrace cloud for cybersecurity.
Cloud is a key infrastructure element your security program protects. Security solutions and services are primed for digital transformation; organizations need to embrace cloud-enabled security platforms. Security that is architected and built to leverage cloud technologies allows organizations to meet the needs of their digital workforce and customers.

IV. Restore trust in your backups.
The frequency and severity of the security incidents that organizations experience make trusting your backups more critical than ever. Organizations need to prioritize securing their backups to guarantee integrity and availability. This is vital to ensure they can recover to a trusted state as required by their recovery point objectives (RPOs) and recovery time objectives (RTOs).

V. Create a culture of security ownership.
Organizations need to make the protection of enterprise systems and data everyone's responsibility. This can be achieved by making it part of an organizational culture that values security as a differentiator. Communicate security- and privacy-related key performance indicators to leadership and to the broader organization to drive ownership and awareness within the organization.

For detailed findings and CDW's recommendations to IT and business leaders, check out the full report.

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

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