



# ROOTING OUT RISKS

How Canadian Organizations Are Using Penetration Testing to Identify and Thwart Their Biggest Security Threats

## Executive Summary

Serious reputational and operational consequences can occur if cybersecurity preparedness is neglected. As breaches become more recurrent and sophisticated, regular penetration testing can help organizations better evaluate their exploitable vulnerabilities and prioritize actionable steps to identify and defend against security threats.

**95%**

of Canadian IT professionals said their organization takes security and protecting against threats seriously. However, only 60 percent of Canadian organizations perform penetration testing.

**49%**

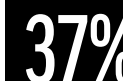
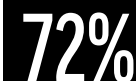
Nearly half (49 percent) of Canadian IT professionals believe that the shift to a hybrid/remote work model has heightened their organization's security risks and over one-quarter (26 percent) of Canadian organizations experienced a security breach over the last two years.

The most common types of security breaches Canadian organizations experienced in the last two years included:

Phishing Attacks

**53%**

Malware Attacks

**37%****72%**

Nearly three-quarters (72 percent) of Canadian IT professionals have concerns regarding their organization's penetration testing capabilities.

The ongoing pandemic has created new challenges for businesses across all sectors and sizes, as many were forced to rapidly adapt their operations to hybrid and remote work. As a result, malicious actors have been looking to take advantage of the changing business landscape, resulting in a global rise in security breaches.

## Introduction

The widespread adoption of remote and hybrid work models throughout the pandemic has made it increasingly difficult for organizations to maintain security and business continuity. Organizations were also challenged by more sophisticated and frequent attacks over the last two years. When cybersecurity preparedness is not an organizational priority, businesses are at a heightened risk for breaches resulting in detrimental impacts on business operations and reputation. Data security is dependent on an organization's latest defence techniques, so it is imperative that organizations objectively test for vulnerabilities within their security strategy to identify which areas are most at risk.

Recently, CDW Canada commissioned a survey with Angus Reid to examine the sentiment of Canadian IT professionals regarding the cybersecurity posture at their organizations. The survey looked at organizations of all sizes and sectors across Canada and the various ways they have been implementing penetration testing before and during the pandemic, as well as their thoughts on the value of having an external IT security services partner.

Penetration testing is defined as the performance of "ethical hacking" and is a simulated attack against an organization's network, data and personnel which aims to identify the biggest vulnerabilities and threats to data and systems. Through penetration testing, an organization can better evaluate and understand weaknesses within their systems and prioritize actionable steps to defend against evolving threats.



**“While most Canadian organizations take security and defending against threats seriously, many are still not conducting – or financially investing in – penetration testing to manage risk.”**

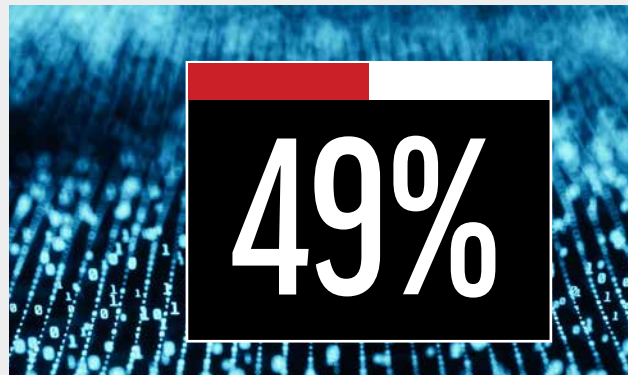


## CDW's Key Findings:



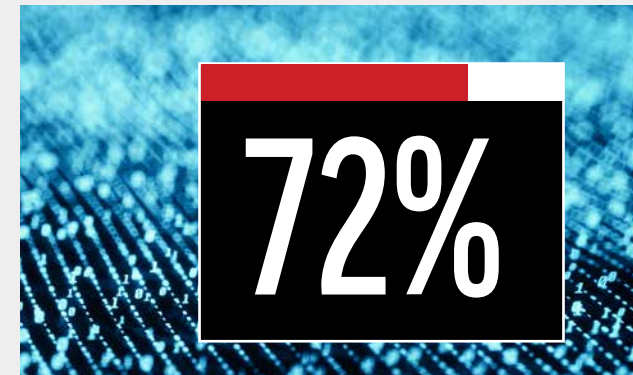
Nearly all (95 percent) Canadian IT professionals said their organization takes security and protecting against threats seriously. However, only 60 percent of Canadian organizations perform penetration testing.

This indicates that while most Canadian organizations take security and defending against threats seriously, many are not conducting regular penetration testing to manage risk.



Nearly half (49 percent) of Canadian IT professionals believe the shift to a hybrid/remote work model has heightened their organization's security risks. Before the pandemic, nearly half (45 percent) of respondents said they performed penetration testing on a quarterly basis.

This number increased to 56 percent during the pandemic. This reveals that some organizations have increased their frequency of penetration testing during the pandemic due to heightened security risks.



Nearly three-quarters (72 percent) of Canadian IT professionals have concerns regarding their organization's penetration testing capabilities. The top concerns cited include lack of employee expertise/talent (36 percent), lack of budget (27 percent) and lack of time (21 percent).

This suggests that many IT professionals lack confidence in their organization's penetration testing capabilities.



## CDW's Key Findings:



More than one-quarter (26 percent) of Canadian organizations experienced a security breach in the last two years. Loss of productivity (58 percent), loss of data (37 percent) and financial loss (25 percent) were the top-cited impacts security breaches had on Canadian organizations in the last two years.

This demonstrates that investing in penetration testing should be a priority for Canadian organizations to mitigate security breaches and ensure business continuity.



Of the 26 percent of Canadian organizations that have experienced a security breach over the last two years, 29 percent experienced between two and five security breaches. The most common types of security breaches Canadian organizations experienced in the last two years included phishing attacks (53 percent), malware attacks (37 percent), ransomware attacks (35 percent) and business email compromises (35 percent).

This indicates that Canadian organizations are facing a heightened and wide range of security risks.

# The State of Penetration Testing in Canada

With the rise of security breaches throughout the pandemic, many Canadian organizations are witnessing the value of penetration testing firsthand and some are adopting it as the first line of defence against potential cyberattacks. While nearly all (95 percent) respondents said their organization takes security and protecting against threats seriously, only 60 percent of Canadian organizations perform penetration testing. Interestingly, just under a quarter (22 percent) said they were unsure if their organization performs penetration testing, and 18 percent said their organizations do not perform penetration testing. Furthermore, while over half of Canadian IT professionals said their organization values penetration testing, only 40 percent indicated their organizations are investing in it.

If building an organization's security defence capabilities and implementing a regular penetration testing program is key to keeping businesses protected against threats, why are some organizations not investing in penetration testing? Some of the top barriers cited by respondents included:

- Penetration testing is not a company priority (57 percent)
- Lack of employee expertise/talent (34 percent)
- Lack of budget (33 percent)

This reveals that while organizations need a deep understanding of emergent threats and their own security posture to stay safe, many lack the time, talent or resources for regular penetration testing.



When it comes to protecting an organization against potential threats, adopting an “attacker” mindset is vital to exposing weaknesses. This means comprehensive and thorough testing is key to detecting exposed critical assets ahead of malicious actors. Many Canadian organizations are leveraging various types of penetration testing to identify and address gaps in their cybersecurity posture, including:

43%

- **Partial-Knowledge Testing** – With this type of testing, no detailed, underlying technical information (such as application source code) is provided. Other information, including web application or host user credentials, partial network diagrams, application walkthroughs and any other relevant information for testing may be provided.

34%

- **Full-Knowledge Testing** – All relevant technical implementation is provided with this type of testing, including full network architecture and application source code. In addition, access to application development teams or network architects may also be provided.

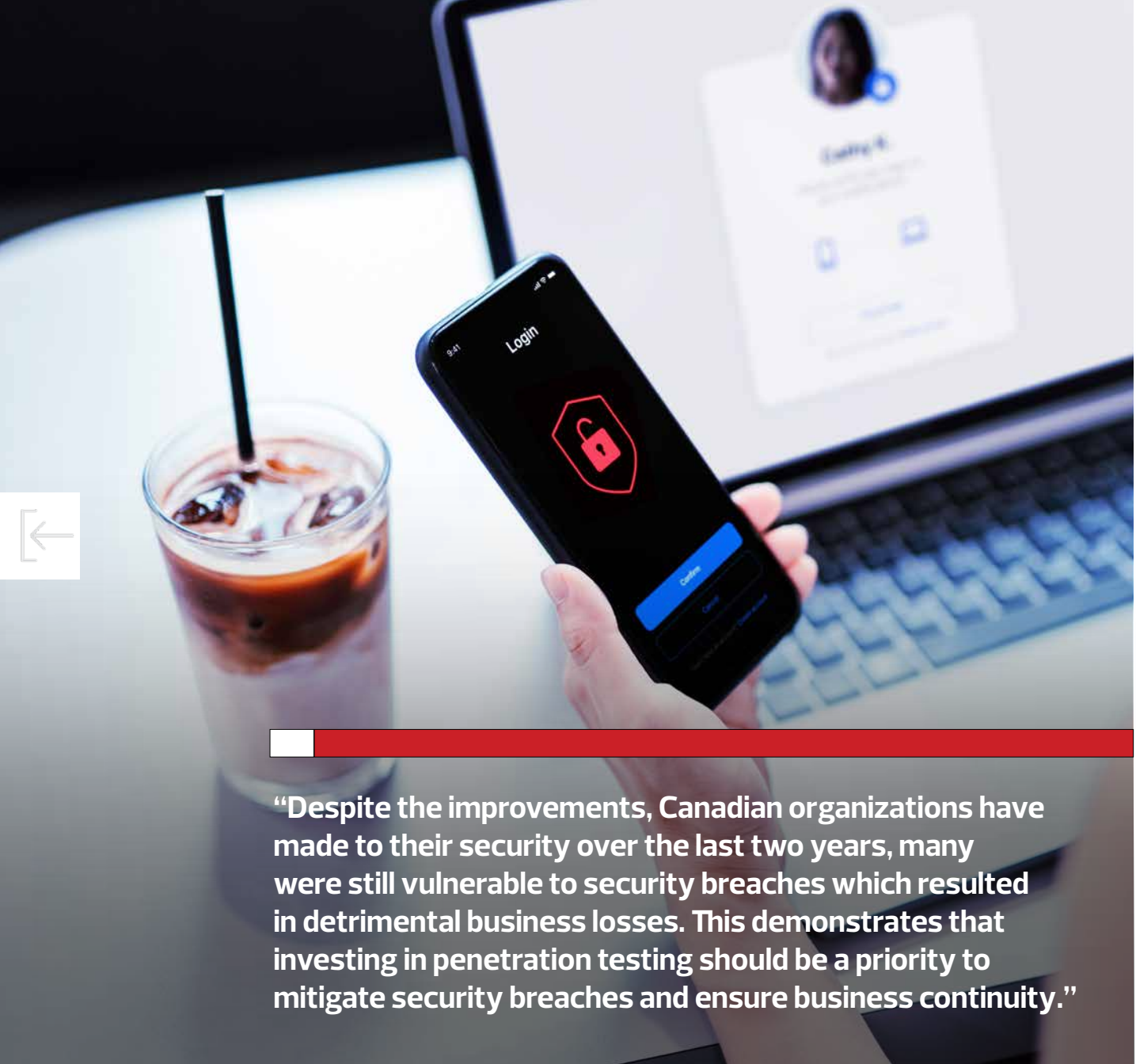
29%

- **Zero-Knowledge Testing** – No previous information about the organization's network or web applications is provided, other than the target IP addresses and/or URLs.

The top three domains used by Canadian organizations to conduct penetration testing included networks (70 percent), web applications (62 percent) and user security awareness (62 percent).



**“While most Canadian organizations take security and defending against threats seriously, many are still not conducting – or financially investing in – penetration testing to manage risk.”**



**“Despite the improvements, Canadian organizations have made to their security over the last two years, many were still vulnerable to security breaches which resulted in detrimental business losses. This demonstrates that investing in penetration testing should be a priority to mitigate security breaches and ensure business continuity.”**

## Cybersecurity is a Business Imperative, and Threats Are Everywhere

It is critical that organizations protect themselves from security risks, as over one quarter (26 percent) of respondents reported their organizations experienced a security breach in the last two years. The most common types of security breaches Canadian organizations experienced included phishing attacks (53 percent), malware attacks (37 percent), ransomware attacks (35 percent) and business email compromises (35 percent).

The business impacts of a security breach can be detrimental and have been attributed to major business shortcomings, including loss of productivity (58 percent), loss of data (37 percent), financial loss (25 percent), loss of reputation (25 percent) and loss of business (13 percent).

The majority (81 percent) of organizations that experienced a security breach said the source was external, originating from outside their organization's infrastructure, while nearly one-quarter (22 percent) said the source of the security breach was internal, originating from inside their organization's infrastructure. This reveals that external sources pose the most heightened risk to organizations, creating a serious need for enhanced defence mechanisms to keep external threats out.

# External IT Security Services Partners are More Important Than Ever

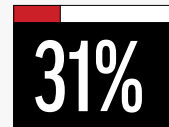
With the increased threat of security breaches, the importance of third-party penetration testing remains paramount.



of Canadian IT professionals surveyed said the value of their external IT security services partner has increased since the onset of the pandemic.



of respondents reported that their organization has an external IT security services partner.



of respondents do not have an external IT security service partner.

These results showcase the importance of having a trusted partner by your side to detect and bridge security gaps before they are exploited.

With decades of experience, CDW has experts who specialize in reducing security risks by helping organizations prepare for – and defend against – security threats. As a trusted security partner, we develop customized solutions to best align strategies with an organization's unique risks and conduct penetration tests to identify and catalogue vulnerabilities in your existing defence systems. Our risk assessment consultants conduct in-depth research to inform the testing, such as reviewing documented policies and procedures and interviewing key stakeholders to uncover the greatest security risks. During penetration tests, CDW is often successful in accessing mission-critical database servers and identifying financial data, intellectual property and human resources information that can lead to harmful consequences if exploited.

An external IT solutions partner has an objective novel view and is uniquely positioned to identify gaps in security systems that have not been previously explored. Collaborating with security and penetration testing experts provides a valuable external outlook into how different threat actors may approach an attack, bringing in fresh and diverse perspectives from internal testers. These experts are dedicated to ethical hacking and stay up to date on the latest attacks and trends. Partnering with a trusted partner will better position your organization to ensure that compliant and vigilant penetration testing is performed in an effective and cost-efficient way.

**“Security risks have heightened as organizations continue to navigate hybrid and remote work models. Working with external IT security service partners can help organizations visualize their cybersecurity posture with comprehensive assessments that identify the biggest risks to their assets.”**

# What We Are Seeing in Different Industries



## Business/Professional Services

Over half (56 percent) of business/professional services organizations reported that penetration testing was not a company priority, despite regularly experiencing security breaches (29 percent) and over one-third (31 percent) said their organizations are not investing in penetration testing. In fact, the business/professional services industry was the industry most likely to report more than 10 security breaches in one year (13 percent). In addition, nearly half (44 percent) of business/professional services organizations reported that the shift to a hybrid/remote work model heightened their organization's security risk. This indicates that a lack of penetration testing can dramatically increase your organization's vulnerability to security risks.

However, the remaining 60 percent of business/professional services respondents whose organizations did conduct penetration testing took it very seriously and remained vigilant about their data security throughout the pandemic.

- IT professionals in business/professional services were the most likely of all industries to conduct penetration testing at least quarterly (65 percent) during the pandemic.





## Government

Government organizations reported significant risk during the pandemic and were more than twice as likely to experience a security breach in the last two years compared to those in financial services. While this risk was heightened by the shift to hybrid/remote work models in the last two years, government organizations were the least likely to report investing in penetration testing during the pandemic. Government respondents also reported low rates of confidence in their ability to respond to security vulnerabilities, showing a low level of preparedness to face a high level of risk.

- Government respondents were more likely to report that the shift to hybrid/remote work models heightened their organization's security risk (59 percent).
- A low eight percent of government respondents reported that their organization invested in penetration testing during the pandemic.
- Government respondents were more than twice as likely to experience a security breach in the last two years (29 percent) compared to those in financial services (14 percent).
- Less than one-quarter (23 percent) of respondents working in government reported feeling "very confident" in their organization's ability to perform remediation activities against identified security vulnerabilities, the lowest of all industries.



## Education

The pandemic had a particularly negative impact on the education industry when it came to its organizational security. Despite security declining over the last two years, education continued to trail behind other industries in data security.

- Nearly half (42 percent) of education respondents said their organization's security had been negatively impacted over the last two years, citing "some" or "significant" difficulties, the highest of all industries.
- A low four percent of respondents reported that their organization's security experienced significant improvements over the last two years, the lowest of all industries.

In addition, the education industry had the most overall concerns (86 percent) related to their organization's penetration testing capabilities. The top-cited concerns amongst education respondents included lack of employee expertise/talent (36 percent) and lack of budget (33 percent).

Beyond lack of resources and financial limitations, over one-quarter (26 percent) of education respondents indicated that penetration testing was not a company priority. As a result, even amongst organizations that did invest in penetration testing, investment was low and infrequent.

- A low five percent of respondents in education indicated that their organization conducts penetration testing more than once per quarter.
- The median penetration testing investment amount was \$29,999 for education respondents, compared to \$74,999 in business/professional services and \$249,999 in government and financial services.

The education industry had a particularly difficult time maintaining its security posture and lags behind other industries in penetration testing, according to IT professionals in the field. This group also cited significant concerns about their ability to perform penetration testing, compared to other industries.





## Financial Services

Throughout the pandemic, the financial services industry has maintained a strong security posture and is a leader when it comes to security assessments and preparedness. In fact, most financial services respondents (84 percent) said their organization takes security and protecting against cyber threats “very seriously”, the highest of all industries.

The financial services industry cited the lowest number (14 percent) of security breaches over the last two years. This is no coincidence, as the financial services industry was the most likely to perform up-to-date cybersecurity procedures. As a result, IT professionals in this industry are confident in their organizations' security.

- 78 percent of financial services organizations perform penetration testing and/or comprehensive security assessments.
- Less than one-fifth (14 percent) of financial services respondents experienced a security breach over the last two years, the lowest rate of security breaches compared to other industries.
- No respondents in financial services said penetration testing was not a company priority.

In addition, over half (56 percent) of financial services employees reported that their organization's security had experienced some or significant improvements over the last two years, the highest of all industries. This shows a direct correlation between investing in penetration testing and comprehensive security assessments to ensure an organization's overall security posture. This correlation is particularly important in an industry that deals directly with citizens' finances and assets.





## Where Do We Go From Here?

As Canadian organizations continue to navigate the current threat landscape, many will continue relying on external IT partners to protect and defend against cyberthreats. As we look to the future, the top takeaways we recommend for organizations are:

- **1. Leverage third-party security experts**  
Engaging a trusted third-party partner to perform penetration testing can help bridge the skills gap and alleviate the internal pressures to ensure compliant and vigilant testing is performed.
- **2. Recognize the link between penetration testing and the strength of your organization's security**  
With the ever-evolving cybersecurity risk landscape, an organization's best method of defence is preparedness. Detecting and bridging security gaps before they are exploited yields incredible savings for organizations including money, time and reputation.
- **3. Commit to investing in penetration testing**  
Frequent penetration testing enables organizations to examine their cybersecurity posture to identify and mitigate the biggest threats to their data, before they lead to detrimental business losses that can be difficult to recover from.

At CDW, **WE GET** penetration testing so you don't have to. Our best-in-class IT experts are available every step of the way.

**To learn more, contact our CDW solutions and services experts at 800.972.3922 or visit [CDW.ca/pentest](https://www.cdw.ca/pentest).**