

THE POWER OF PREVENTION

How Proactive Penetration Testing Can Strengthen
Your Cybersecurity Posture.

Executive Summary

Despite many organizations understanding the importance of regular penetration testing for cybersecurity preparedness, they continue to face significant operational and financial barriers when it comes to adopting and investing in penetration testing.

95%

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

72%

Nearly three-quarters (72%) 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).

49%

Nearly half of Canadian IT professionals (49%) reported that the shift to a hybrid or remote work model has heightened their organization's security risks and more than one-quarter (26 percent) of Canadian organizations experienced a security breach in the past two years.

Phishing Attacks

53%

Malware Attacks

37%

The most common types of security breaches Canadian organizations experienced in the last two years included phishing attacks (53 percent) and malware attacks (37 percent).

Introduction

The cybersecurity posture of organizations has become increasingly complex amid the evolving business landscape, leaving organizations exposed to new threats with the potential to damage reputation and impact business bottom lines. The ongoing pandemic and rapid shift to a remote and hybrid work model has created global challenges for organizations across sectors and of many sizes.

Cybersecurity is a business imperative, and threats can emerge from unexpected sources at any time. To proactively combat this, it is important for organizations to consistently assess their cybersecurity needs to ensure that the appropriate protective and preventative measures are in place. While some organizations rely on internal IT teams to conduct penetration testing, a trusted third-party IT partner can also be leveraged to test an organization's defences, a critical step to understanding security posture and protecting brand reputation. Partnering with an external IT partner to thoroughly test systems for known vulnerabilities, misconfigurations and mismanagement of devices can help ensure that an organization's data remains secure.

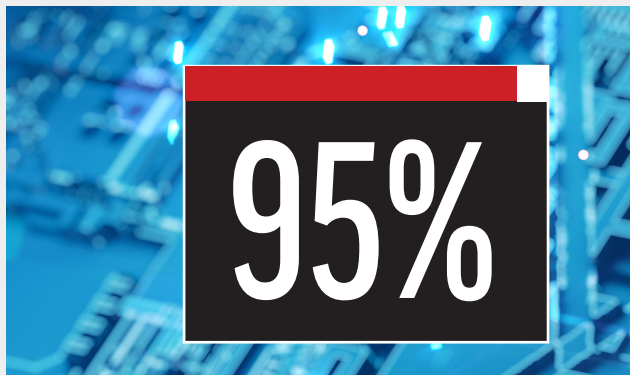
Whether organizations realize it or not, many Canadian companies remain vulnerable to security breaches that often result in detrimental business losses. Penetration testing is an effective way to identify security vulnerabilities within an organization's IT environment prior to a cyberattack, to ultimately help them better understand and protect their security posture. Penetration testing involves a simulated attack against an organization's network, data and personnel which aims to expose their biggest vulnerabilities and threats to data and systems. Investing in penetration testing is one of the most efficient and effective ways to mitigate security breaches and ensure business continuity over both the short and long term.



“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”.

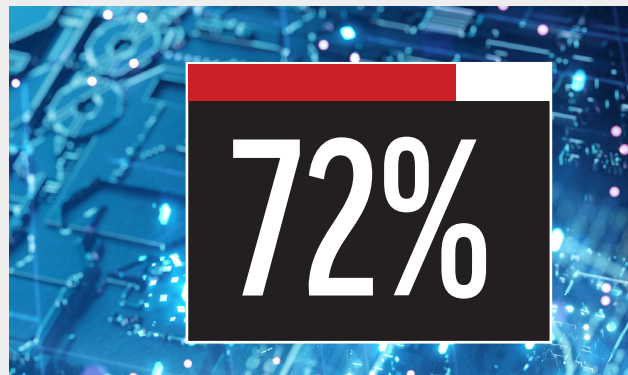


CDW's Key Findings:



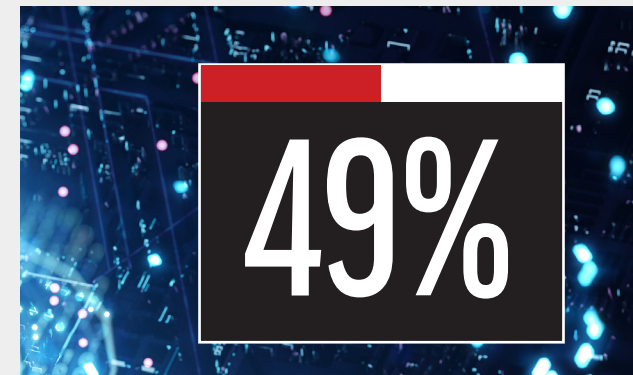
Nearly all (95 percent) Canadian IT professionals said their organization takes security and protecting against threats seriously. However, only 60 percent of Canadian organizations perform penetration testing.

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 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 and could benefit from working with a trusted third-party partner to help assess and strengthen their organization's cybersecurity posture.



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.



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



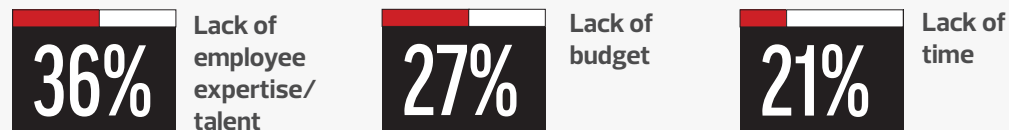
Of the 26 percent of Canadian organizations that have experienced a security breach over the last two years, 29 percent experienced between two and five security breaches. The most common types of security breaches Canadian organizations experienced in the last two years included phishing attacks (53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

Many Canadian Organizations Lack the Internal Expertise to Adequately Perform Penetration Testing

With the increased frequency and impact of cyberattacks, organizations understand the importance of penetration testing. Penetration testing allows organizations to proactively detect and bridge security gaps before they are exploited, which ultimately helps mitigate their biggest threats to data and ensures their reputation and bottom line remain secure. However, the ability to take on a proactive security approach depends on several factors, and many organizations face significant operational and financial barriers when it comes to utilizing and investing in penetration testing.

Although nearly all (95 percent) Canadian IT professionals report that their organization takes security and protecting against threats seriously, only 60 percent of Canadian organizations perform penetration testing. In addition, nearly three-quarters (72 percent) of Canadian IT professionals are concerned about their organization's penetration testing capabilities. The top concerns cited include:



The lack of employee expertise and talent is of particular concern, as 65 percent of organizations said penetration testing is performed by internal employees. This suggests that while internal IT teams understand the benefits of penetration testing, many lack the skills and expertise to conduct this type of testing. In addition, while IT talent can be difficult to recruit and retain, large organizations rely more heavily on internal employees to perform security protocols than any other organization size. This is likely because smaller organizations may not have the resources for internal IT talent with expertise in security. Of the organizations that did perform penetration testing, the majority (87 percent) of large organizations used internal employees to perform them. This is concerning given the lack of internal expertise cited previously. Overall, no matter the size of an organization, engaging a trusted third-party partner to help perform penetration testing can help bridge the skills gap and ensure compliant and vigilant testing is performed.



“Nearly three quarters (72 percent) of IT experts expressed concerns regarding their organization’s penetration testing capabilities, citing lack of employee expertise and talent as a top concern.”


Investments in Penetration Testing are More Important Than Ever

Despite over half (64 percent) of Canadian IT professionals reporting that their organization values penetration testing, only 40 percent of Canadian organizations are investing in this. Threat actors will continue to take advantage of the uncertain circumstances caused by the pandemic, and it is critical that organizations take a proactive approach to ensure their information and assets remain protected at all times. Over half (56 percent) of organizations have reported that the value of their external IT security services partner has increased since the onset of the pandemic.

Penetration Testing as a Fundamental Cybersecurity Tool

As organizations continue navigating the evolving hybrid or remote work environments, many organizations are looking to increase their investment in preventative and protective measures such as penetration testing. Over half (56 percent) of respondents said the value of their external IT security services partner has increased since the onset of the pandemic, which underscores the importance of having a trusted partner by your side to detect and bridge security gaps before they are exploited. However, just over half (52 percent) of respondents reported that their organization has an external IT security services partner, while one-third (31 percent) did not.

CDW's team of trusted IT experts specialize in reducing security risk and utilizing penetration testing to uncover security vulnerabilities in an organization's work environment. CDW can help an organization better understand their company's security posture and test its readiness to withstand and respond to real-world cyberattacks. CDW's expert penetration testers can create a testing plan unique to each organization's environment and use industry-recognized and proven methodologies to discover, analyze and exploit vulnerabilities within it to ensure an organization's data and assets remain protected.



“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.”



The Pandemic Has Exacerbated Existing Security Risk Challenges and Concerns

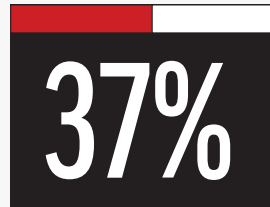
As a result of the pandemic, organizations have accelerated their digital transformations and quickly adopted new tools and technologies to maintain operations. This swift digital transformation opened the doors to novel cybersecurity risks and provided opportunities for existing vulnerabilities to be exploited. Nearly half (49 percent) of Canadian IT professionals reported that the shift to a hybrid or remote work model has heightened their organization's security risks and more than one-quarter (26 percent) of Canadian organizations experienced a security breach in the past two years. Of the 26 percent that experienced a security breach in the past two years:



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



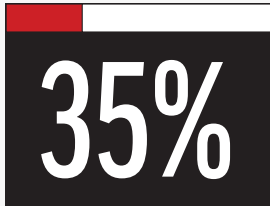
Phishing attacks



Malware attacks



Ransomware attacks



Business email compromises

Security breaches can result in major consequences and losses when it comes to a business's bottom line. Loss of productivity (58 percent), loss of data (37 percent) and financial loss (25 percent) were the top three impacts cited by Canadian organizations in the last two years. With increased risk comes a greater focus on cybersecurity. Nearly half (45 percent) of respondents said they performed penetration testing on a quarterly basis before the pandemic, and this number increased to 56 percent during the pandemic. In addition, over half (56 percent) of organizations cited the value of their external IT security services partner has increased since the onset of the pandemic. This demonstrates that while the focus on prevention – rather than reaction – to cybersecurity incidents is increasing among organizations, there is still work to be done.

“The shift to a hybrid/remote work environment during the pandemic has heightened organizations’ security risks and resulted in increased security breaches such as phishing attacks, malware attacks and ransomware attacks. As a result, some organizations have increased their frequency of penetration testing during the pandemic”.



Where Do We Go From Here?

As Canadian organizations continue navigating the remote and hybrid work environment, it is crucial that organizations take a layered approach to cybersecurity and ensure they have a dedicated team that can perform compliant and vigilant penetration testing. As such, the top takeaways we recommend for organizations include:

- **1. Continue to invest (or consider investing) in penetration testing.**
With the ever-increasing prevalence of security risks and vulnerabilities, it is important for organizations to minimize as many risks of business losses by implementing a robust security strategy and ensuring that compliant and vigilant penetration testing is performed.
- **2. Engage a third-party IT partner to help manage your organization's security.**
External IT partners can leverage various penetration testing techniques, along with specialized tools, to test and strengthen your organization's security posture and ensure business continuity.
- **3. Review your cybersecurity/IT infrastructure investment priorities on a regular basis and ensure that you have a team in place that can proactively mitigate risks.**
Top concerns faced by Canadian organizations related to penetration testing included lack of employee expertise/talent, lack of budget and lack of time. This demonstrates the importance of evaluating your IT employee and investment opportunities to ensure that cybersecurity remains a top priority.

At CDW, **WE GET** penetration testing, so you don't have to. Our highly trained team of IT experts can help you 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).