Securing Your Hybrid Work Environment

A guide to understanding and managing emerging cybersecurity risks of hybrid and work-from-anywhere models.

Gallagher

Insurance | Risk Management | Consulting

The Cyber Risk Management Program is currently not available in Quebec.
Le service de gestion des cyberrisques n'est pas disponible actuellement au Québec.

Contents

Headlines **3**

Executive summary 3

Section 1: Risk landscape **4**

Risk #1: Growing vulnerabilities of data and network risks 4

Risk #2: User authentication and password breach 4

Risk #3: One of the greatest vulnerabilities in security — human error 5

Risk #4: Risks associated with international remote working or work-from-anywhere 7

Risk #5: Critical cybersecurity threats amidst a challenging economy in Canada 7

Section 2: Risk analysis **8**

Risk #1: An uptick in data destruction and sensitive information revelation 8

Risk #2: Supply chain vulnerability 8

Risk #3: Tasks conducted online leave traces for cybercriminals compromising information technology 8

Section 3: The future for flexible work in a rapidly evolving cybercrime landscape **9**

Headlines

ESCALATING CYBERTHREATS IN A HYBRID WORK MODEL

- The quick transition to hybrid or remote work model post-pandemic created a rapid surge in dependence on technology. This flexible arrangement has led to the uprising of cybersecurity vulnerabilities in organizations such as data breaches, ransomware attacks, intellectual property theft and other cyberthreats.
- In Canada, cyber dangers are still the No. 1 cyberthreat activity. The 2020 Cyberthreat Defense Report[2] (CDR) states that 78% of Canadian organizations experienced at least one cyber attack within a 12-month period. In 2021, this figure rose to 85.7%[3] of Canadian companies.
- With a transition to a permanent hybrid work environment, cyberthreat actors are taking advantage of organizations' remote accessibility, attempting to compromise corporate networks via remote connections.
- Cybercriminals exploited organizational vulnerabilities during the pandemic. According to a report by EY and ACFE Mumbai,[4] there was a 53% rise in ransomware attacks, and 40% of organizations experienced cyber intrusions due to unsecure Wi-Fi networks, software vulnerabilities and limited cyber awareness among employees in their remote work environments.
- Ransomware is almost certainly the most disruptive form of cybercrime facing Canadians. According to the Canadian Anti-Fraud Centre,[5] there have been over 18,000 reports of fraud in Canada with over $133 million stolen as of March 2023.
- Phishing emails are a major threat facing remote workers. There has been a 600% increase in reported phishing emails since the end of February 2021.[6]

[1] 62% of Canadian employers using hybrid working model: survey
[2] 2020 Cyberthreat Defense Report
[3] 2021 Cyberthreat Defense Report
[4] How can digital transformation of compliance energize integrity frameworks?
[5] Canadian Anti-Fraud Centre
[6] #COVID19 Drives Phishing Emails Up 667% in Under a Month

EXECUTIVE SUMMARY

The rising volume of cyber attacks covering data breaches, ransomware attacks and intellectual property theft in Canada have become a pressing concern for corporate organizations and business operators. According to a 2023 survey conducted by Benefits Canada,[1] 62% of Canadian employers are now using a hybrid working model with some hot-desking or working remotely across multiple offices, locations and countries.

The confluence of technology, connectivity and a scattered workforce presents a range of risks and operational challenges for individuals and companies in the hybrid and work-from-anywhere work model.

For individuals:

- Reliance on personal devices, public Wi-Fi and cloud technologies create opportunities for hackers to obtain sensitive data.
- Phishing and malware pose hazards to personal and professional data for remote workers.
- Blurred personal and professional environments on shared devices are susceptible to online dangers.

For organizations and business operators:

- Flexible and remote work arrangements increase the exposure to cyber danger.
- Using personal devices and a decentralized workforce create new entry points for cyberthreats.
- Relying on personal network usage and not securing remote access endangers cybersecurity.

Cybersecurity risks have been elevated further by mobile working practices. As employees flip between home/office/on-demand workspaces, data breaches, interception of private information and unauthorized network access increases the vulnerability to multiple cyber attack vectors.

Section 1: Risk landscape

Context

The interconnectedness of the digital workplace has raised concerns about cyber risk exposure for both individuals and corporate organizations in Canada. With the broad-scale adoption of cloud-based services and the rise of hybrid and remote work environments, the cyber risk perimeter extends further. With organizations in varying states of preparedness to respond (ideally defend) a targeted cyber attack, human error is viewed by many as the primary threat from a technology integration perspective.

RISK #1: GROWING VULNERABILITIES OF DATA AND NETWORK RISKS

In a hybrid cloud setup, IT teams typically use an open internet to set up private and public clouds resulting in data transfer and leakage. Moreover, a lack of safeguarding information privacy while moving data to the cloud may lead to inappropriate visibility of commercially sensitive data and man-in-the-middle (MitM) attacks. Encryption and robust cybersecurity measures are essential to deliver a secure of flow data across the network.

Additionally, if the VPN isn't adequately encrypted, remote workers may still be vulnerable to hackers. A VPN without effective end-to-end encryption greatly raises the risk of a cyber attack by having the potential to reveal user IP addresses, login information and other private data. The Colonial Pipeline attack is one example of how stolen VPN credentials enabled a lateral cyber attack.

RISK #2: USER AUTHENTICATION AND PASSWORD BREACH

An employee working remotely is not covered by the security umbrella of the company, hence the increase in the number of personal devices, various online platforms and unsecured networks lead to authentications and password breaches.

Unauthorized access and potential data breaches might result from weak or compromised authentication procedures. Where BYOD (bring your own device) is permitted, enabling employees to use both personal and workplace devices opens up the opportunity for a malware-infected device to laterally infect other network devices and access data.

Common security errors include the use of weak passwords, password reuse across multiple platforms and the use of common passwords (e.g., password123, qwerty). Cybercriminals take advantage of these flaws by using various strategies, such as brute-force attacks or phishing operations, to gain unauthorized access to accounts and networks.

"Prior to COVID, most of the IT team would walk around the business and pick up a laptop to make a change. They wouldn't have a different local administration password to administer that PC.

So what you had was this massive compound and effect. Externally you could get in through a firewall without multifactor authentication (MFA). You could then get onto a device that had the same local admin password as everything else. They could scan the rest of the network that were just loading ransomware into every PC that had that username and password.

It got to a point where most of the backup servers also had the same username and password as the PC. So it was very easy for an attacker to just dial in. Not to be caught, not to be found. Spread ransomware and get the backups as well.

This was a prime position for deploying ransomware."

Johnty Mongan, Global Head of Cyber Risk Management — Gallagher

RISK #3: ONE OF THE GREATEST VULNERABILITIES IN SECURITY — HUMAN ERROR

The human factor is a significant and often overlooked aspect of cybersecurity. Human behavior, actions and decisions play a crucial role in determining the overall security posture of an organization. Here are some key points to elaborate on the human risk factor in cybersecurity.

- **Phishing and social engineering:** Phishing attacks, which involve tricking individuals into revealing sensitive information or performing malicious actions, heavily rely on human vulnerability.
- **Insider threats:** Insider threats refer to individuals within an organization who misuse their access privileges or intentionally compromise security due to malicious intent or financial gain.
- **Personal negligence:** Accidental errors by employees like misplacing sensitive documents, sending confidential information to the wrong recipients or failing to follow security protocols due to a lack of cognizance or distractions.
- **Lack of security awareness and training:** Without proper security awareness, training programs and cybersecurity practices, employees may not be equipped to recognize and respond to potential cyberthreats.
- **Shadow IT:** Shadow IT refers to the use of unauthorized software, applications or cloud services by employees without the knowledge or approval of the IT department, adding more security threats.

5 MAIN TYPES OF CYBERCRIME GROUPS

TO LAUNCH MORE SUCCESSFUL CYBER ATTACKS, MALICIOUS ACTORS WITH DIFFERENT SPECIALIZED SKILLS HAVE CONGLOMERATED TO FORM CYBERCRIME AS A SERVICE (CAAS) GROUPS.

Access as a Service (AaaS)

A service offering in the undergrounds whereby malicious actors sell access into business networks. The price for network access can range quite a bit. The highest price was $95,000[7] for an Asian telecommunications service provider.

Ransomware as a Service (RaaS)

Credited as one of the reasons ransomware attacks continue to increase, RaaS has enabled less-skilled hackers to launch costly attacks on large organizations — like SolarWinds — by providing the necessary tools and techniques. This newfound accessibility has led to a dramatic 63.2% increase[8] in RaaS extortion groups in the first quarter of 2022.

Bulletproof Hosting

Bulletproof hosting services are essentially leased hideouts where malicious actors can store files or even the malware necessary for their attack campaigns. The threats are enabled by advanced persistent threat (APT) groups because they supply a stable infrastructure.

Active since 2006, Void Griffon is one such malicious actor group whose service has been used for multiple years by some of today's top-tier APT groups and malware distributors.

Crowdsourcing

Cybercriminals have turned to crowdsourcing their offensive research and development processes to find new attack methods. This relatively new type of cybercrime has increased since 2021. There is an uptick observed in malware actors holding public contests in the criminal underground to find new creative attack methods.

Phishing as a Service

Like RaaS or AaaS, this attack technique allows virtually anyone with even an entry-level knowledge of the cybersecurity landscape to benefit from a phishing attack—often monetarily and often via email-based entry. A 2022 report from Proofpoint[9] states that more than three-quarters (78%) of global organizations saw email-based ransomware attacks in 2021. Not only is phishing common, but it's costly — the email-based attack cost large enterprises almost $15 million USD annually.[10]

[7] Access-as-a-Service Rising in Popularity
[8] Lockbit, Conti, and Blackcat Lead Pack Amid Rise in Active RaaS and Extortion Groups
[9] Proofpoint's 2022 State of the Phish Report Reveals Email-Based Attacks Dominated the Threat Landscape in 2021
[10] The Ponemon 2021 Cost of Phishing Study

RISK #4: RISKS ASSOCIATED WITH INTERNATIONAL REMOTE WORKING OR WORK-FROM-ANYWHERE

The risk of fine and flow-on reputational damage can occur where data privacy regulations such as the European Union's General Data Protection Regulation (GDPR) are not adhered to GDPR regulations impose strict requirements on the processing and transfer of personal data, and place a duty of care on both the organization and the employee/worker to store and manage data in a secure manner.

Given the range and complexity of cyber risks including phishing, social engineering and network security breach, one noteworthy risk involved is the use of third-party tools and services, such as cloud storage providers, collaboration platforms or communication tools. The absence of robust cyber education, security practices and compliance standards regarding the use of third-party tools including public Wi-Fi may provide cyber attackers with an open door to access commercial sensitive data and personal information.

RISK #5: CRITICAL CYBERSECURITY THREATS AMIDST A CHALLENGING ECONOMY IN CANADA

The dynamic field of cybersecurity is creating vulnerabilities for organizations responding to changing workforce expectations. According to the 2023 Global Digital Trust Insights Survey,[11] fewer than 40% of Canadian senior executives responded that they've fully mitigated their risk exposure following a move to flexible working patterns in 2020, including enabling hybrid and remote work, accelerated cloud adoption and increased use of internet of things technologies.

The survey also found that only 38% of the Canadian C-suite claim to have considered their organization's high-priority vital systems and processes. Almost half (46%) of respondents claim they occasionally utilize client data without explicit agreement. Furthermore, 49% might not always thoroughly investigate each partner or third party with which they disclose customer data.

[11] A C-suite united on cyber-ready futures

Section 2: Risk analysis

The pivot to remote working brought with it an exponential increase in cybersecurity threats. A 2020 data breach crisis reported that there were more data breaches[12] in the last 12 months than in the last 15 years combined.

RISK #1: AN UPTICK IN DATA DESTRUCTION AND SENSITIVE INFORMATION REVELATION

A persistent threat to Canadian organizations, ransomware is the most disruptive form of cybercrime facing Canadians. Aside from the financial cost of the ransom itself, ransomware can stop the operation of important systems, damage or destroy an organization's data, and reveal sensitive information.

In Canada, a ransomware attack resulted in a loss of essential services at an Ontario hospital in June 2021[13]. In October 2021, due to some of their servers being encrypted and locked, a municipal transit service was unable to share route and scheduling information. Cybersecurity reporting indicates that even after paying ransom, there is no guarantee that the data will be restored. One survey of Canadian businesses found that only 42% of organizations[14] that paid the ransom had their data completely restored.

Following a zero-trust approach to network security, composed of Zero Trust Network Access (ZTNA), Secure Web Gateway (SWG) and Cloud Access Security Broker (CASB) capabilities, strengthens protection and control across the attack surface. Moreover, establishing strong patch management strategy, like making a zero-day exploit plan, communicating with vendors and utilizing virtual patching, limits the scope of ransom exploit.

RISK #2: SUPPLY CHAIN VULNERABILITY

As the world becomes more interconnected, organizations increasingly rely on multiplatform digital supply chains to optimize performance, facilitate payment, make data-informed decisions and quickly respond to changing operating conditions.

Supply chain cyber risks can have far-reaching consequences impacting not only individual organizations but also the entire ecosystem of suppliers, partners and customers. Sensitive information, including customer information, product designs, manufacturing techniques and intellectual property, is exchanged throughout supply chains. Therefore, it is possible to suffer financial loss and reputational harm as a result of a data breach or unauthorized access to this information.

The KPMG 2021 CEO Outlook[15] highlights some positive indicators from senior executives to aid supply chain risks.

- Forty-eight percent of respondents say they will focus on the security and resilience of their supply chains/supplier ecosystems to build digital resilience.
- Forty percent say they will invest to develop secure and resilient cloud-based technology infrastructure.
- Seventy-nine percent say that protecting their partner ecosystem and supply chain is just as important as building their organization's cyber defences.

RISK #3: TASKS CONDUCTED ONLINE LEAVE TRACES FOR CYBERCRIMINALS COMPROMISING INFORMATION TECHNOLOGY

The shift to using new teleworking infrastructure and processes may lead to undetected exploitation of vulnerabilities in existing remote work technologies. Security agencies in both the United States and the United Kingdom have warned that a growing number of cybercriminals are targeting individuals and organizations with malware.[16]

Remote working operations of interconnected vendors and customers further amplify organizational risk. Compliance with regular and comprehensive penetration testing maintains a strong security posture and identifies vulnerabilities in hybrid work environments.

[12] Cybersecurity investment 2020
[13] Toronto's Humber River Hospital under code grey after ransomware attack
[14] TELUS Canadian Ransomware Study
[15] KPMG 2021 CEO Outlook
[16] UK and US Security Agencies Issue COVID-19 Cyber Threat Update

Section 3: The future for flexible work in a rapidly evolving cybercrime landscape

Whether it is artificial intelligence, 5G wireless technology, AI or cloud computing, the road to digitization has become more complex and layered as new cyber attack vectors emerge and become more sophisticated.

Implementing zero trust and MFA along with robust password strategies, the growing application of browser isolation technologies are helping eliminate the risk of data loss and network compromise.

Given that the majority of businesses rely on data to function, grow and deliver their strategic objectives, any permanent adoption of hybrid working models requires careful consideration and an effective mix of cybersecurity expertise and data security protocols. As time progresses, there is a growing expectation that flexible working patterns and mobile (including international) work-from-anywhere will become part of the fabric of the 21st century workplace. While this enables organizations to adapt to shifting worker expectations, the dependency on technology investment and increased cybersecurity bench strength will challenge decision-makers to ensure they are consistently one step ahead of the cyber actor and attack vectors.

"While porting services to the cloud removes a lot of security maintenance concerns, such as patching and password policies, it has pushed attackers to target the most vulnerable element of a network—the human component—through both social engineering and targeted attacks, to access internal services and systems.

Penetration testing simulates an attacker's mindset when approaching a target. It now involves a phased approach to testing all the separate components of the network infrastructure and determining how each component can directly or indirectly pose problems for each other.

Before working as penetration tester in the commercial sector, I carried out cyber and digital investigations in the police force, and later covert tracking and hacking of digital devices and computer-based forensics. The landscape always was and always will be evolving, but penetration testing as a service will still follow the same testing methodology to look for vulnerabilities in authentication and active services—with the same end goal to help clients close these vulnerability gaps and strengthen their defences."

Jay Lucas, Principal Consultant, Cyber Risk Management Practice, Gallagher

Connect With Us

To find out more about any of our services, please get in touch with:

Cyber Practice
CyberRM@ajg.com

Gallagher

Insurance | Risk Management | Consulting

AJG.com/ca **The Gallagher Way.** Since 1927.