Fraud, cyber & compliance: A triple threat for Canadian organizations

The case for an interconnected defense strategy

March 2022

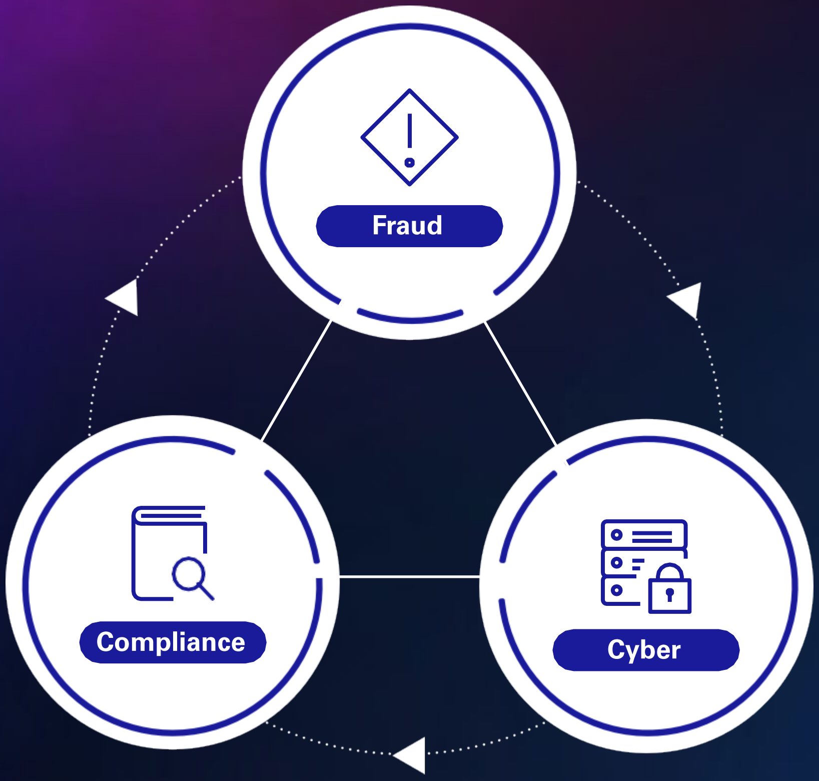
home.kpmg/ca

Introduction

Canadian organizations are faced with mitigating a 'threat loop' comprised of fraud, compliance risk and a growing array of cybersecurity threats. But defending against this threat loop will require a collective, interconnected effort, rather than dealing with the risks they pose in isolation.

A KPMG[1] survey of more than 600 North and South American executives across multiple industries confirms anecdotal evidence about the effects of the pandemic on these three interconnected threats. Based on the results of this survey, we're sharing our perspective on what these findings mean for Canada.

Are Canadian companies managing to fend off this triple threat? Our view of the landscape suggests that many have limited defences in place, and the shift to remote or hybrid work is making existing controls less effective — requiring a new approach to close this threat loop.



Key takeaways

Fraud, non-compliance and cyber breaches are the costly norm

The majority of companies across North America reported that they've suffered losses from fraud, compliance breaches and/or cyberattacks. Larger companies are more likely to experience losses from either internal fraud (which originates with an employee, manager, officer or owner) or external fraud (which originates with a third party, such as a customer or vendor).

Businesses expect fraud, compliance risk and cyberattacks to intensify in the yearahead

Two-thirds of respondents expect either external or internal fraud to increase in the next year, and even more (77%) expect that cyber risks will grow. Nearly every respondent expects to see more regulatory or compliance requirements related to data privacy, labour relations and the environment in the next fiveyears.

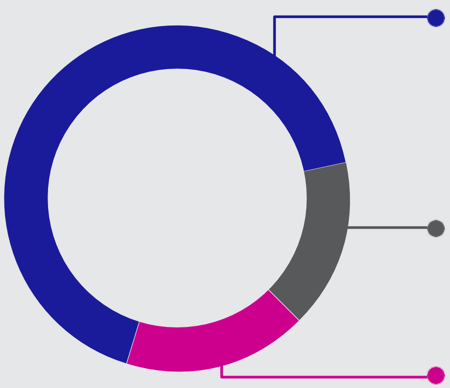
Not enough companies are completely on top of fraud controls, compliance and cybersecurity

Looking specifically at how respondents say their companies perform across a series of measures relating to cybersecurity, fraud control and compliance, KPMG found that only a small proportion report strong controls across at least half of the relevant measures.

Our findings show that many larger Canadian organizations have an *intent* to improve cyber resilience, fraud detection and compliance—but not the *urgency* to do so. Unfortunately, awareness of the threat loop frequently comes after they experience a cyberattack, fraud incident or regulatory breach. Being proactive, however, can help to mitigate risk and lessen the impact when an incident occurs—because it's a matter of when, not if.

Fraud

To your knowledge, has your North American company experienced either of the following types of fraud in the past 12 months?



66.9%

External fraud (credit card fraud, identity theft perpetrated by individuals outside the company)

15.8%

Not aware of any fraud

17.3%

Internal fraud (procurement fraud, misappropriation of company funds perpetrated by individuals inside the company)

We hear a lot about external fraud, but the impact of internal fraud is just as concerning. There's also a 'collusion' aspect of fraud that combines external and internal, such as a threat actor bribing a disgruntled employee to provide access to sensitive data. A significant 31% of respondents say their companies have suffered from fraud perpetrated by an insider in the past year.

The top two types of internal fraud that North American companies have experienced in the past 12 months are false expense claims or other misappropriation of company funds **(47.8%)** and procurement fraud **(45.7%)**.

With more people working from home, controls that were put in place before the pandemic are no longer sufficient. During the abrupt shift to remote work at the start of the pandemic, many companies rushed to put processes and technologies in place, without the proper due diligence (and they may not have revisited those processes and technologies since). This also opened up organizations to new risks: For example, if a remote employee exfiltrates personal data from the company using his or her personal email address, the company won't be able to flag it on the corporate server.

Yet, it's more difficult to set the 'tone at the top' when employees are working remotely. And you need to have the right controls in place; this involves doing a fraud risk assessment and mapping your major risks. If you did this before the pandemic, you should do it again, because you're facing different risks now than pre-pandemic. These challenges are unlikely to recede due to the proliferation of the hybrid work model.

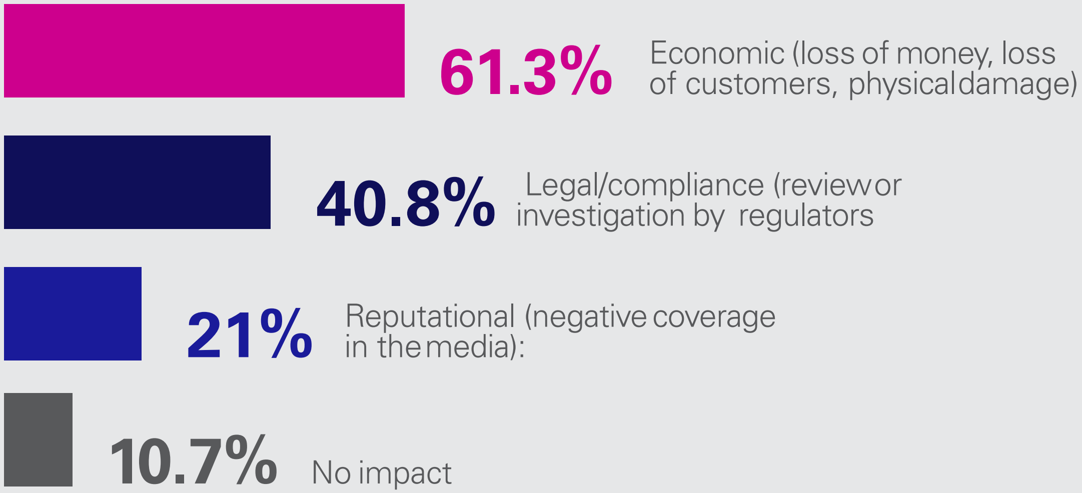
One way to combat fraud is through the use of data analytics in the forensics process. This allows you to create rules and generate exception reports to find red flags. Typically, you'll reduce the cost of fraud—and the time it takes to discover it.

> "You need to have strong processes related to KnowYour Client, and all third parties should be monitored to help minimize your risk—because fraud could be coming from various third parties such as vendors, suppliers, clients, partners and employees."

Myriam Duguay
Partner, Forensics,
National Leader, Investigation and Fraud Risk Management
KPMG in Canada

Cybersecurity

Which of the following impacts did your North American business experience as a result of a cyberattack in the past 12 months?



Digital transformation is one of the key driving factors of cyber breaches and attacks—but the pandemic has made things much worse. Last year, large-scale cyberattacks made headlines and in some cases forced nation states to take action against ransomware threat actors. As a result, attack groups are splintering off into smaller groups and targeting small and mid-sized organizations and/or non-traditional industries so they can fly under the radar.

> **One in two** North American respondents expect their cybersecurity risk to increase somewhat over the next 12 months, while **34.6%** expect it to increase greatly. **Zero per cent** of respondents expect it will decrease greatly.

Companies surveyed for the report indicated rises in the frequency of attacks, including phishing (44%), scamming (33%), malware (22%) and ransomware (20%). Threat actors have also become more aggressive in exploiting zero-day vulnerabilities. With disruptions in the supply chain, third- and fourth-party risks are also increasing cyber risk, according to the findings from our report, *From Awareness to Action: Elevating Third-Party Risk*. If your suppliers have suffered a breach, it's possible your data has also been breached and/or you can't provide your products/services.

At the same time, the survey found that only a small proportion of respondents are able to identify and contain a cyberattack in real time or even within 24 hours. It takes, on average, two weeks to identify a cyberattack and another two and a half weeks to contain it. And yet, respondents aren't sufficiently concerned, with 87.9% of North American respondents somewhat or completely satisfied with how long it takes their company to recognize an IT attack.

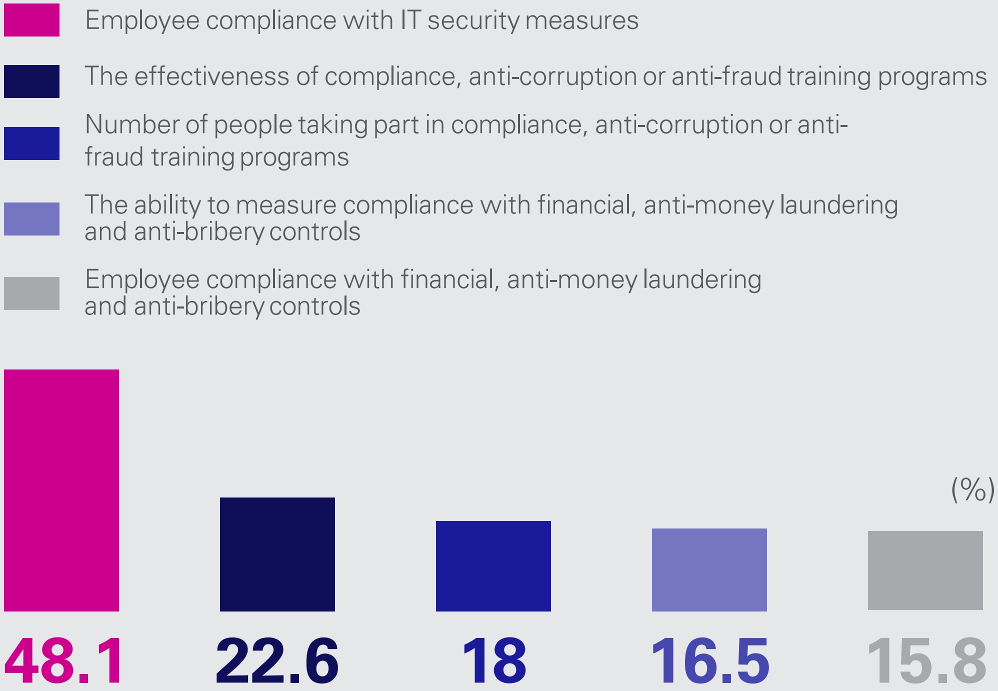
Organizations need strong preventative processes and controls as well as regular vulnerability assessments to reduce the likelihood of cyber events—but they also need crisis management, disaster recovery and cyber insurance to reduce the impact when something does go wrong.

> “An interconnected approach between cyber, fraud and compliance helps to not only reduce the likelihood of an event happening, but also reduces the impact if—and when—something does happen.”

Alexander Rau
Partner,
Cybersecurity
KPMG in Canada

Compliance

Which of the following have been negatively impacted by an increase in employees working from home in the last 12 months?



Digital transformation creates additional risk for companies since they're changing systems and processes—and they may not be aware of the interdependencies of datasets and systems leading to compliance risk exposures. The pandemic has made this even harder, since compliance is harder to manage with remote or hybrid workforces.

55% of respondents acknowledge that their business has paid regulatory fines or suffered financially due to compliance violations in the past year—but undiscovered instances of non-compliance mean these numbers are likely to be even larger.

The risks of non-compliance go beyond regulatory fines. Compliance is also a reputational issue, and oftentimes reputational considerations cause leaders to pay attention to compliance more than fines and enforcement. Where many Canadian organizations are failing with compliance is in not proactively identifying all of their compliance requirements—including legislative, regulatory, contractual and internal—and only taking action after it's too late.

A strong compliance program means you can demonstrate sufficient due diligence to prevent and protect your clients' data and/or your own data assets. This is even more important with upcoming regulatory changes and the broadening of the compliance function, specifically around the focus on environmental, social and governance (ESG) factors.

A preliminary inventory of compliance requirements followed by a compliance risk assessment exercise helps you know your risks and know your exposures. If you're going to invest time, effort and money on better controls, you need to know **where** to invest it.

> "An organization may be exposed to additional risk if they're not thinking about internal controls and compliance as a key element of any large transformation initiative."

Pedro Medeiros
Partner,
Governance, Risk & Compliance Services
KPMG in Canada

Are you prepared for the triple threat?

The pandemic has made things worse: Nearly nine in ten respondents say that working from home has negatively affected the effectiveness of their companies' fraud prevention measures, compliance risk mitigation or cybersecurity.

Few respondents say their companies reflect international best practices in their anti-corruption compliance (18%), environmental compliance (21%), anti-money-laundering compliance (22%), anti-fraud controls (23%) and data privacy controls (27%).

At the same time, most respondents expect fraud, compliance risk and cyber threats to intensify in the year ahead. And while most companies have some defences in place, a comprehensive approach is rare in Canada, with the exception of some tier-one financial institutions.

Looking ahead, KPMG in Canada recommends organizations take the following four steps to defend against the triple threat:

1

Develop an interconnected defense strategy where compliance, fraud andcyber efforts work together.

2

Coordinate or integrate the cyber, fraud and compliance functions into one role, with the mandate to manage these risks via a unified approach.

3

Conduct risk assessments across these areas at least once every twoyears—and more often if there's a major change in the organization (such as an acquisition or merger) or a major event (such as a global pandemic).

4

Ensure your risk assessments take into account a range of exposures, including those related to technology, people, processes and/or behaviour.

How KPMG can help

KPMG can provide a comprehensive threat loop assessment where we combine our Cyber Maturity Assessment, Fraud Risk Assessment and Compliance Program Assessment to help you understand the impacts of the threat loop on your organization. Other KPMG in Canada service offerings in the areas of fraud, cyber and compliance include, but are not limited to:

Fraud

- Fraud risk assessment and antifraud programs
- Forensic investigations
- Forensic data analytics
- Forensic regulatory and compliance services
- Forensic technology services
- Financial crimes services

Cyber

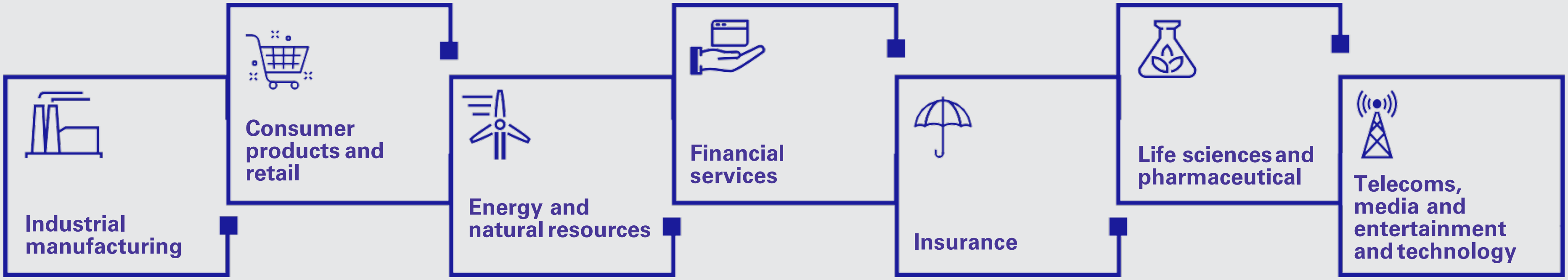
- Cyber maturity assessment, staff training, user verification tools, threat intelligence, and real-time monitoring
- Cyber security function outsourcing, ensuring best of breed cyber controls, coverage and ROI
- Incident response plan creation and testing
- Cyber insurance attainment and maintenance

Compliance

- Regulatory compliance program implementation and enhancement (Inventory of regulations, risk assessment, testing, remediation and reporting)
- Compliance audits, compliance program reviews and maturity assessments
- Transformation assurance, including internal controls & compliance support

About the research

This study was based on a survey of 642 executives almost evenly divided across seven industries:



Industrial manufacturing

Consumer products and retail

Energy and natural resources

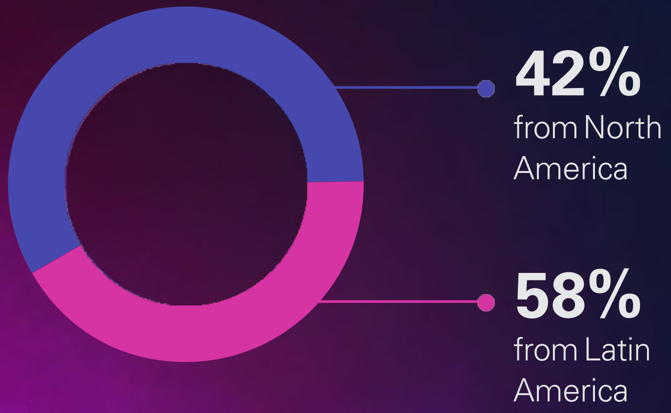
Financial services

Insurance

Life sciences and pharmaceutical

Telecoms, media and entertainment and technology

Geographic distribution of respondents



The sample was predominantly composed of senior leadership: More than half of respondents were board members, members of the C-suite, or heads of departments. This report has focused primarily on the North American response sample.

Contacts

Enzo Carlucci
Partner, National Service
Line Leader, Forensic
KPMG in Canada
416-777-3383
ecarlucci@kpmg.ca

Hartaj Nijjar
Partner, National Service
Line Leader, Cybersecurity
KPMG in Canada
416-228-7007
hnijjar@kpmg.ca

Angela Moch
Partner, National Service
Line Leader, Governance,
Risk & Compliance
KPMG in Canada
416-777-8093
amoch@kpmg.ca

Myriam Duguay
Partner, Forensic,
National Leader, Investigation
and Fraud Risk Management
KPMG in Canada
514-840-2161
myriamduguay@kpmg.ca

Alexander Rau
Partner,
Cybersecurity
KPMG in Canada
416-777-3450
alexanderrau@kpmg.ca

Pedro Medeiros
Partner, Governance,
Risk & Compliance
KPMG in Canada
416-476-2263
pedromedeiros@kpmg.ca

home.kpmg/ca

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.