Pulling fraud out of the shadows

2018 Global Economic Crime and Fraud Survey
Canadian Insights

www.pwc.com/ca/crimesurvey
Economic crime: the biggest competitor you didn’t know you had

Economic crime is an industry with tentacles in every country, sector, and function. It's tech-enabled, opportunistic, and pervasive.

Organizations used to see fraud as a nuisance, the cost of doing business to be dealt with using ad-hoc or stopgap measures. But our 2018 Global Economic Crime and Fraud Survey found that economic crime is on the rise. 55% of Canadian respondents indicated they were victims of an economic crime in the last 24 months. This is up from 37% in our 2016 report.

It’s not hard to see how we got here. Technology has advanced in leaps and bounds; fraudsters are more strategic in their goals, more sophisticated in their methods; and regulatory regimes, although becoming more robust, are fighting to catch up. In the face of well-publicized corruption and other scandals, public expectations for transparency and accountability around the world are converging toward a common standard of conduct. There is a growing recognition that corruption and economic fraud have become too costly, that they impede organizations’ ability to compete on the world stage.

Our 2018 Global Economic Crime and Fraud Survey found that while economic crime is up, the defence measures necessary to detect and prevent it can — and should — be improved and strengthened across Canadian organizations.

Looking at the data, it’s clear that fighting fraud today requires a shift from macro to micro measures. Companies can no longer rely solely on the loss prevention department or IT reports to detect fraud — they need sophisticated, targeted controls that can be continuously monitored for their effectiveness at all possible touch points, across functional teams, from the back office to the front lines of their business.
Based on the survey responses and the experience of our global network of forensics practitioners, we've identified four critical areas where companies should focus their efforts to minimize the impact of economic crime.

The important question to ask is no longer “Is your organization a victim of economic crime?” but rather, “Are you aware of how crime is impacting your organization? And are you fighting it blindfolded, or with eyes wide open?”

Beware of your blind spots

- 55% of Canadian respondents reported experiencing economic crime in the last 24 months. Many respondents indicated there was no impact of the crime or that they do not know how economic crime is affecting their organization.
- Canadian companies are lagging in the use of disruptive technologies — our survey indicates that only 12% of respondents are currently using or have plans to use artificial intelligence (AI) in the next 12 months to help combat fraud and economic crime.
- Companies need to continue investing in training for their people to help tackle crime from the inside, out. While a majority of Canadian organizations (69%) have a formal business ethics and compliance program in place, only 30% make verifying and promoting their employees’ ethical decision-making a top priority.

Exhibit 1: The most common risk assessment conducted by Canadian respondents in the last two years is for cyber-attack vulnerability.

Q. In the last 24 months, has your organization performed a risk assessment on any of the following areas?
Source: PwC's 2018 Global Economic Crime and Fraud Survey. Canadian responses unless otherwise indicated. Respondents were asked to select all that apply.

Q. What prompted your organization to perform a risk assessment?
Source: PwC's 2018 Global Economic Crime and Fraud Survey. Canadian responses unless otherwise indicated.
Four steps to fight economic crime and fraud

1. Know what economic crime looks like  
2. Manage fraud dynamically  
3. Harness technology to counter crime  
4. Invest in your people, alongside machines
1. Know what economic crime looks like

Is economic crime on the rise, or just our awareness of it?

This year’s Global Economic Crime and Fraud Survey shows that 55% of Canadian companies experienced economic crime in the last 24 months, a significant increase from 37% in 2016.

Exhibit 2: The reported rate of economic crime is on the rise

Q. Has your organization experienced any fraud and/or economic crime within the last 24 months?
Source: PwC’s 2018 Global Economic Crime and Fraud Survey.
Canadian responses unless otherwise indicated.

This upward trend is worth noting — statistically, instances of fraud tend to rise in times of economic downturn. If the Canadian economy enters turbulent times, chances are that rates of identified economic crime will continue to increase. That’s why it’s critical that companies address their blind spots now, instead of waiting for an incident.
This rise can be explained by a combination of growing global awareness of fraud and greater clarity about what “fraud” actually means. But every organization — no matter how vigilant — is vulnerable to blind spots. And because these blind spots usually only become apparent with hindsight, throwing light onto them as early as possible can vastly enhance fraud-fighting efforts.

As more aspects of business and commerce have gone digital, economic crime has followed suit. In the past two years, cybercrime has become the most reported crime in Canada (46%), followed by asset misappropriation (38%), and fraud committed by the consumer (36%). As the world becomes more digital, theft of assets is shifting to new channels and perpetrators, resulting in a permeation between online and physical environments, as well as the types of economic crime. In this report, we focus on how companies can equip themselves now with the mindsets and processes necessary to protect themselves from evolving risks. This begins with recognizing blind spots within organizations and structuring departments to best tackle potential vulnerabilities.

Exhibit 3: Cybercrime, asset misappropriation and consumer fraud were the most frequently reported crimes

Q. What type of fraud and/or economic crime has your organization experienced in your country within the last 24 months?

Source: PwC’s 2018 Global Economic Crime and Fraud Survey.
Canadian responses unless otherwise indicated.
Cybercrime

Around the world, organizations are racing to implement new technologies, using data to innovate and provide value in an increasingly interconnected world. This hyper-connectivity increases cyber risks — and therefore organizations must be vigilant about not only their own security, but that of third party service providers, clients, and even governmental authorities.

Companies who fail to protect themselves from cyber risks may face significant recourse, including intensified regulatory scrutiny, lawsuits, and reputational damage — ultimately undermining the public’s trust in organizations’ ability to thrive in a digital, data-driven world.

Exhibit 4: Cyber-attack techniques used against organizations

Q. In the last 24 months, has your organization been targeted by cyber-attacks using any of the following techniques?

Source: PwC’s 2018 Global Economic Crime and Fraud Survey.
Canadian responses unless otherwise indicated. Respondents were asked to select all that apply.
According to our survey results, 46% of Canadian respondents have experienced cybercrime, compared to 31% of global respondents. Unsurprisingly, 40% of external crime perpetrators in Canada were hackers. Looking forward, nearly half (48%) of Canadian respondents predicted that cybercrime will be the most disruptive force to their organization in the next two years.

In the last two years, Canadian respondents who were victims of a cyber breach were primarily affected by asset misappropriation (32%), disruption of business processes (29%), and extortion (23%). These breaches were typically conducted through phishing (58%), malware (45%), and network scanning (20%).
While more companies are becoming aware of the frequency, sophistication, and severity of such cyber breaches, there is still a potential blind spot: knowing when the cyber breach begins and ends. Organizations tend to focus on the “smashed door” (how the culprit got in), as opposed to what happens after the breach (what the culprit does once it’s in). Focusing on the latter will lead to better controls that detect malicious activities rapidly and protect the organization’s most critical assets.

The risk of delayed detection

Cybercrime is particularly insidious as its impact is not always immediately clear. It is often the case that organizations may not be alerted to a breach until the hacker sells or exposes the data, or until the organization performs a routine compromise assessment. In other cases, companies may never directly feel the impact at all.

Companies are also often late to report cyber breaches, in part due to their fears around public reaction and reputational damage. There is also a patchwork of regulatory requirements for cyber breach disclosures, which can be confusing to organizations that operate in multiple jurisdictions. Since the impact of a cybercrime is likely to spill outside of the victim organization over time and affect other organizations and individuals, it’s important that these instances are dealt with immediately — even if businesses want to downplay the event to their clients and the public. Regulators locally and globally are also increasing the requirements for timely disclosure of cyber breaches.

A surge in cyber response plans

Canadian businesses have recently improved when it comes to cyber response plans, in part due to the growing awareness of the impact an incident could have on an organization. Canada was lagging compared to global averages in 2016, however there has been a rapid implementation of cybercrime response plans in the last two years: 64% of respondents now have a fully operational response plan in place, compared to 31% in 2016.

While on the surface this looks promising, PwC’s 2018 Global State of Information Security Survey identified that only half of the respondents run drills at least annually to rehearse their cyber response plans. Failure to prepare is preparing to fail. Of the Canadian companies with a cyber security program, 40% of these have a designated Chief Information Security Officer (CISO). However, a closer look at the data shows a worrying trend: only 43% of CISOs report to the Board of Directors — lagging behind global companies, which sit at 61%. As more and more threats continue to manifest through technology, it is important that CISOs have a broader mandate and visibility within the organization.

The increasing sophistication of cybercriminals has called for businesses to mature all aspects of their cyber security — from prevention and detection through to response. Cybercriminals are using a combination of human, physical and technical methods to achieve their malicious objectives. If organizations are going to truly tackle cybercrime head-on, employees cannot work in silos.

With this in mind — and given that 38% of respondents neglected to perform a risk assessment for cyberattack vulnerability in the last two years — Canadian organizations still need to seize opportunities to protect and strengthen their digital assets. They’re facing disruption from new market entrants, emerging technology and an ever-changing threat landscape. In order to stay competitive and innovate in the digital world, Canadian organizations need to revisit their cybercrime program to balance risk and opportunity.
Consumer fraud

Consumer fraud is defined in our survey as fraud against a company through illegitimate use of, or deceptive practices associated with, its products or services by customers or others. It encompasses many common kinds of fraud — from credit card fraud to insurance fraud to mortgage fraud — and affects all of society. With the advent of new technologies, consumer fraud has become even more prevalent; deceptive and unlawful scams frequently occur online from phishing via email, to online extortion through ransomware.

The rise of mortgage fraud

One subset of consumer fraud, mortgage fraud, is on the rise, particularly in Ontario and British Columbia¹ where home prices are at a high. The pressure to commit mortgage fraud will likely increase in light of the Office of the Superintendent of Financial Institutions’ revised guideline on residential mortgage underwriting, which imposes new, more stringent stress tests that consumers applying for uninsured mortgages will need to meet. In a competitive housing market, individuals may be compelled to embellish on their mortgage applications in hopes of buying the home of their dreams. This may lead to greater exposure to operational and credit losses for companies, as more individuals fail to make payments and go into mortgage default.

Counterfeiting gone digital

Counterfeiting has also grown to unprecedented levels. Counterfeit sellers are taking advantage of the huge growth in online shopping; as the internet provides more direct lines between vendors and consumers, fraudsters are able to sell unregulated goods through communication platforms and online market places. This poses risks to the global economy. Counterfeiting steals revenue and jobs from businesses that manufacture and sell legitimate products, governments lose tax revenue from products manufactured or sold on the black market, and consumers’ health and safety are put at risk from substandard products. A 2016 report commissioned by the International Chamber of Commerce (ICC) estimated that the negative impacts of counterfeiting and piracy are projected to drain US$4.2 trillion from the global economy and put 5.4 million legitimate jobs at risk by 2022². Moreover, according to Interpol, a clear link has been established between counterfeit goods and transnational organized crime due to the lucrative profits realized on a global scale. These profits are often used to fund other criminal activities such as drug trafficking, human smuggling and sophisticated cyber schemes³.


External actors: Be careful who you do business with

One of a company's biggest blind spots — and biggest threats — are the people it has invited to do business with, including customers, vendors, and service providers. The survey shows that external actors were responsible for 58% of respondents’ most disruptive incidents. These are third parties with whom companies could have regular, profitable relationships and a certain degree of mutual trust, but who may actually be stealing from the company.

Addressing this blind spot is especially important when it comes to acquisitions and transactions, where organizations can risk buying and inheriting successor liability, reputational issues, and ineffective or non-existent controls. Fraud and regulatory risk assessments are therefore a crucial part of pre-deal due diligence. Organizations must investigate who the companies they’re acquiring are working with, who their clients are, and any past history of nefarious business practices. Enhanced due diligence around fraud, cybercrime, anti-corruption, and anti-money laundering (AML) practices will help identify risks.
and determine how they can either be carved out of a deal or remediated post-deal. It’s common for businesses to focus on financial, operational or tax due diligence, but Canadian companies need to expand their due diligence process to other areas, such as anti-bribery and anti-trust, where they’re still lagging behind global organizations.

Gathering intelligence on potential counterparties can help organizations gain a better understanding of who they’re dealing with. Before making any key strategic decisions, companies should use the tools available to them — sophisticated intelligence tools can yield useful publicly available information on target investments. This helps uncover potential risks, such as allegations of corruption and reputational risks associated with joint ventures in foreign markets.

### Regulatory risk is growing

Canadian companies are not safe from exposure to foreign laws. Canadian companies that are registered in the U.S. are subject to the Foreign Corrupt Practices Act (FCPA) and are susceptible to the significant fines and penalties that are being imposed by the Securities and Exchange Commission (SEC) and the U.S. Department of Justice. If an organization purchases a business that was subject to the FCPA prior to the acquisition, they could be a victim of successor liability unless adequate measures are taken to address the matter.

In Canada, public companies, citizens and Canadian-based private companies are subject to the Corruption of Foreign Public Officials Act (CFPOA). Effective October 31, 2017, the Canadian Government aligned more closely with global anti-bribery and anti-corruption regulations in most countries (excluding the U.S.) by repealing the long existing exception for facilitation payments. Facilitation payments to foreign public officials (also known as

---

**Exhibit 8: Canadian respondents reported fewer incidents where their organizations were asked to pay a bribe than Global respondents**

<table>
<thead>
<tr>
<th></th>
<th>Yes, in the country we primarily work in</th>
<th>Yes, globally</th>
<th>No</th>
<th>Don’t know</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Canada</strong></td>
<td>4%</td>
<td>71%</td>
<td>21%</td>
<td>4%</td>
</tr>
<tr>
<td><strong>Global</strong></td>
<td>4%</td>
<td>50%</td>
<td>27%</td>
<td>8%</td>
</tr>
</tbody>
</table>

Q. In the last 24 months, has your organization been asked to pay a bribe?

Source: PwC’s 2018 Global Economic Crime and Fraud Survey.
Canadian responses unless otherwise indicated. Percentages are rounded to the nearest whole number. Respondents were asked to select all that apply.
“grease payments”) now constitute a crime under CFPOA, and could lead to criminal prosecution, conviction of individuals for up to 14 years in prison, and substantial fines for corporate entities.

As a result, public companies in Canada without policies in place to prohibit facilitation payments may face increased regulatory, financial, and reputational risks. Companies should consider re-evaluating contracts, developing new procurement and payment processes, and strengthening their compliance and training programs.

In a recent development, the Canadian Government announced it was expanding the tools it has to deal with bribery and corruption issues to include drafting new legislation on Deferred Prosecution Agreements (DPAs). With DPAs, proceedings may be suspended, the accused will agree to certain penalties, including conducting robust remediation, in order to reduce the risk of corruption reoccurring. In exchange, the prosecutor could drop all charges—if the accused fulfills all required agreed upon commitments. This marks a significant shift in Canadian bribery and corruption legislative and enforcement policy, one that Canadians and Canadian companies will benefit from as the DPA scheme should encourage compliance with the CFPOA by providing prosecutors a tool to negotiate with the accused under judicial supervision — and avoid long, costly trials.

Canada is also receiving pressure from the global community to strengthen its AML regime. In September 2016, the Financial Action Task Force (FATF) issued a report on Canada that among other things called for increased AML regulatory supervision of the real estate sector and precious metal dealers. FATF also expressed serious concerns that AML laws and regulations have been rendered inoperative for Canadian lawyers due to constitutional reasons. Canada’s response to FATF’s findings will likely result in increased regulatory activity in sectors that have not had this attention in the past. The Department of Finance is currently considering expanding Canada’s AML regime to high-risk sectors, including but not limited to: white label ATMs; non-federally regulated mortgage lenders; finance, lease and factoring companies; and high-value goods dealers.

Exhibit 9: The majority of Canadian respondents are subject to AML regulations

Q. Is your business subject to AML regulations?
Source: PwC’s 2018 Global Economic Crime and Fraud Survey, Canadian responses unless otherwise indicated.
2. Manage fraud dynamically

The times are changing

Not only is public sensitivity about corporate misconduct at an all-time high, in some cases, corporations and leaders are also being held responsible for past behaviour, when the “unspoken rules” of doing business might have been more lax.

The perceived impacts of economic crime in Canada

There’s a disconnect between where fraud measures are focused (“the devil you know”) and where fraud actually affects companies (“the devil you don’t”). Despite more reported instances of economic crime in Canada, respondents feel they have experienced less impact on brand reputation, employee morale, and business relations, and significantly less impact from regulators and on share price compared to global respondents.

Exhibit 10: Fraud and economic crime impact all elements of a business, but Canadian respondents indicated that economic crime had a lower impact to their organizations than global respondents (%).

<table>
<thead>
<tr>
<th>Aspect</th>
<th>Canada</th>
<th>Global</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee morale</td>
<td>48</td>
<td>29</td>
</tr>
<tr>
<td>Business relations</td>
<td>29</td>
<td>36</td>
</tr>
<tr>
<td>Reputation/brand strength</td>
<td>26</td>
<td>37</td>
</tr>
<tr>
<td>Relations with regulators</td>
<td>21</td>
<td>30</td>
</tr>
<tr>
<td>Share price</td>
<td>11</td>
<td>39</td>
</tr>
<tr>
<td>Total</td>
<td>118</td>
<td>168</td>
</tr>
</tbody>
</table>

Q. What was the level of impact of the most disruptive fraud/economic crime experienced on the following aspects of your business operations?

Source: PwC’s 2018 Global Economic Crime and Fraud Survey.

Canadian responses unless otherwise indicated. Percentages are rounded to the nearest whole number.
Although direct losses associated with economic crime may be construed as having a low material impact on an organization, there are other consequential impacts that could materialize as a result of direct losses, such as increased regulatory scrutiny. 41% of Canadian respondents indicated they expect an increase in enforcement of regulations in their organization in the next 24 months, suggesting their increased awareness of the need to meet regulation standards (or else erode consumer and shareholder confidence in the long term). The failure to appropriately respond to or report on the impacts of economic crime can ultimately cause more lasting damage than the fraudulent activity itself.

**Break down silos**

Organizations are typically structured with business units like Human Resources, Finance, Operations, and IT. When thinking about risk mitigation, business units have usually prepared their own plans but often they are not sharing with one another. This means that crimes that happen on the front lines of a business may not be shared with the back office, and vice versa. This is still a major blind spot. In addition, when asked about the level of impact the most disruptive crimes had on their business operations, a significant number of respondents simply didn’t know, or indicated that there wasn’t an impact. The instances of “don’t know” responses in our survey shows that there’s a lack of knowledge-sharing across business units.

There are many benefits to adopting a centralized response to fraud detection. In addition to gathering information from many sources across an organization — from digital alerts, to whistle-blowers, to formal investigations, and so on — a centralized approach offers a broader view of how one localized instance of fraud can affect other internal and external stakeholders. With only 59% of respondents conducting a general fraud risk assessment and 15% of respondents neglecting to perform an annual assessment at all, Canadian businesses need to seize opportunities to establish cross-functional processes to tackle economic crime.

---

**Exhibit 11: Half of the most disruptive instances of fraud were detected by corporate controls**

| Source | PwC’s 2018 Global Economic Crime and Fraud Survey. | Canadian responses unless otherwise indicated. | Percentages are rounded to the nearest whole number. |
Bad news travels fast

In an era of radical transparency, companies often don’t get to decide when an issue becomes a crisis. The jury of public opinion does. Society’s rules change faster than regulators’, and there is little tolerance for those who don’t follow them. This year, we introduced a new category of fraud: business misconduct. This refers to the deceptive practices associated with the manufacturing, sales, marketing, or delivery of a company’s products or services to its clients, consumers, or the general public. The significant percentage of respondents who reported suffering from business misconduct (21%) suggests that this problem is far more widespread than the numerous high-profile business frauds splashed across the headlines.

Survey respondents ranked reputational harm as one of economic crime’s biggest impacts. This is not, of course, to minimize regulatory compliance, which, if anything, is more critical than ever. But consider that regulators, by definition, operate within limited jurisdictions and under well-defined processes. A company’s brand reputation, on the other hand, is subject to no fixed jurisdiction, law, or due process.

The C-Suite and board are accountable

Chief executives are increasingly seen as ambassadors of their organization, and are expected to have their fingers on the pulse of every facet of their company’s culture and operations at all times. So when ethical or compliance breakdowns happen, they’re often held responsible — both in the court of public opinion, and increasingly by regulators. Whether merited or not, one thing is clear: C-Suite and board members cannot claim ignorance as an excuse.
Our Canadian survey shows that 9 out of 10 times (91%), the most serious incidents of fraud are brought to the attention of senior management or the board. Furthermore, of the 69% of respondents who indicated their organization has a formal business ethics and compliance program, 18% said the Chief Compliance Officer had primary responsibility for it, 17% said the CEO, and another 17% said the General Counsel. Although these results are fairly split, they’re promising, applying a sharp spotlight on how senior management is responsible for managing crises — and the extent to which they are (or are not) adjusting their risk profiles accordingly.

CEOs are held accountable for how they handle a fraud or other crisis. Are you ready for this responsibility?

- Do you have a crisis response plan?
- Have you defined when a crisis response is necessary?
- Have you shared the plan to all the appropriate stakeholders?
- Have you designated a crisis response team?
- Are you confident in your ability to react in a timely fashion when a crisis hits?
3. Harness technology to counter crime

Implement the right technology today

When it comes to fraud, technology can be a double-edged sword. On the one hand, we live in a time of exciting innovation: artificial intelligence (AI), big data, and blockchain are just some of the pivotal technological advances we’ve witnessed. Many of these technologies can be leveraged to combat fraud, and act as additional lines of defence for organizations.

Exhibit 14: Canadian respondents lag in their use of disruptive technology to help combat economic crime and fraud compared to their global counterparts

<table>
<thead>
<tr>
<th>Technology</th>
<th>Canada</th>
<th>Global</th>
</tr>
</thead>
<tbody>
<tr>
<td>Periodic analysis</td>
<td>42%</td>
<td>56%</td>
</tr>
<tr>
<td>Continuous monitoring</td>
<td>51%</td>
<td>58%</td>
</tr>
<tr>
<td>Proactive detection</td>
<td>40%</td>
<td>49%</td>
</tr>
<tr>
<td>Transaction testing</td>
<td>47%</td>
<td>50%</td>
</tr>
<tr>
<td>E-mail monitoring</td>
<td>48%</td>
<td>56%</td>
</tr>
<tr>
<td>Contract or other unstructured data review</td>
<td>32%</td>
<td>43%</td>
</tr>
<tr>
<td>Leveraging big data</td>
<td>21%</td>
<td>39%</td>
</tr>
<tr>
<td>Data visualization/dashboards</td>
<td>42%</td>
<td>56%</td>
</tr>
<tr>
<td>Communications monitoring</td>
<td>51%</td>
<td>58%</td>
</tr>
<tr>
<td>GRC solutions</td>
<td>40%</td>
<td>49%</td>
</tr>
<tr>
<td>Pattern recognition</td>
<td>47%</td>
<td>50%</td>
</tr>
<tr>
<td>Transaction testing</td>
<td>48%</td>
<td>56%</td>
</tr>
<tr>
<td>E-mail monitoring</td>
<td>32%</td>
<td>43%</td>
</tr>
<tr>
<td>Contract or other unstructured data review</td>
<td>21%</td>
<td>39%</td>
</tr>
<tr>
<td>Leveraging big data</td>
<td>42%</td>
<td>56%</td>
</tr>
</tbody>
</table>

Canada ■ Currently using or planning to implement in the next 12 months
Global ■ Currently using or planning to implement in the next 12 months

Q. To what degree is your organization using or considering the following alternative/disruptive technologies and techniques in your control environment to help combat fraud and/or economic crime?

Source: PwC’s 2018 Global Economic Crime and Fraud Survey.
Canadian responses unless otherwise indicated.
12% of respondents are currently using or have plans to implement artificial intelligence (AI) in the next 12 months to help combat fraud and economic crime.

But the flip side is that the technology has become so ubiquitous it offers more opportunities for fraudsters to target organizations across different levels of business operations and act with anonymity. Companies need to be cautious when implementing new technologies to also safeguard these platforms or products against risks, and to educate the entire company on best practices to stay vigilant and prepared against threats.

When it comes to using technology to combat economic fraud, it’s clear that Canadian organizations are not using it to its full extent — or worse, not using it at all. Our Canadian survey indicates that only 12% of respondents are currently using or have plans to implement artificial intelligence (AI) in the next 12 months to help combat fraud and economic crime.

Exhibit 15: Most Canadian respondents have no plans to use AI or advanced analytics

Q. To what degree is your organization leveraging Artificial Intelligence or Advanced Analytics to combat/monitor for fraud and other economic crimes? (% of respondents who said their organization uses and derives value)

Source: PwC’s 2018 Global Economic Crime and Fraud Survey. Canadian responses unless otherwise indicated.
There are a number of reasons why companies may be slow to adopt these technologies, including clunky legacy systems and costs. Technology is expensive to buy and adopt across large organizations — prohibitively so, for some. And the decision about what to purchase, and when, is a delicate one. Some invest in emerging or disruptive technologies that they don't use optimally, for instance. Others adopt technology too late and find themselves behind the curve. However, these barriers are becoming less significant: as these technologies mature, they are becoming increasingly affordable.

Looking at the global results, a larger share of global respondents use technology for detection of economic crime in areas that are heavily scrutinized by laws and regulations, such as anti-money laundering, sanctions, export controls, and anti-trust. Though Canadians are finding value in the continuous monitoring, testing, and proactive detection of economic crime, cost barriers remain a deterrent, and adopting disruptive technologies is still not a priority for many Canadian companies.

Canadian companies need to shift their mentality towards using emerging technologies for economic crime mitigation, or else remain vulnerable to a number of risks. This will mean investing not only in the necessary tools, but also in the team to manage the technology and make sense of the data.

Blockchain technology — a race between criminals, businesses, and law enforcement

While at first glance blockchain technology and its product, the cryptocurrencies, have the right ingredients for successful money laundering (portable; transferable between borders; relatively low transaction fees; reasonably safe from confiscation; and seemingly anonymous), solid evidence of large-scale criminal activity using blockchain as the tool to facilitate economic crime has not yet materialized.

This is likely because certain features of cryptocurrencies have prevented them from becoming the ideal money laundering instrument. Cryptocurrencies are not truly anonymous, as blockchain technology digitally records transactions in a universally shared and unchangeable ledger. This means law enforcement can track down customer information from cryptocurrency exchanges if needed.

Some criminals have benefited from “zero-knowledge proof” technology, which removes any identifying information such as sender, recipient, and the value of a transaction from a blockchain’s ledger. While this loophole presents some risks, businesses and law enforcement are also using blockchain technology to their advantage. For example, because a blockchain is essentially a distributed ledger consisting of many “building blocks”, there needs to be numerous points of failure for hackers to access meaningful information. This renders cyberattacks less effective. Blockchain also has the potential to eliminate intermediaries and administrative costs related to compliance with know-your-customer (KYC) regulations by allowing organizations to access client verifications performed by other organizations.
Customers aren’t just one consideration of your business — they are your business

Your customers are the lifeblood of your business — and many are getting exposed to fraud for the first time.

The business case for investment in economic crime technology goes well beyond protecting against reputational, regulatory, or financial damage. It also includes enabling an organization to safely build and sell new products and services on a digital platform and protecting customers from unforeseen risks. As business models continue to evolve through the digital revolution, organizations will need to be aware of the challenges of today’s digital fraud.

Industry lines are blurring

In the digital economy we are witnessing a crossing over of some non-financial services companies into payment systems. Whereas financial services traditionally have the most advanced anti-fraud measures and the legacy knowledge of fraud and money-laundering risk, some of these relative newcomers to the payment space lack this experience and know-how — making them, and their third-party ecosystem, susceptible to both fraud and regulatory risk.

New digital products are creating new attack surfaces

To bring products to market, companies once followed an established business to business (B2B) process involving resellers, distributors, and retailers. On today’s innovative business to consumer (B2C) digital platforms, there is a much wider attack surface — and much more room for fraud to break through.

The technical sophistication of external fraudsters continues to grow

Digital fraud attacks are becoming more and more sophisticated, thorough and devastating. Single ransomware attacks can cripple organizations and fraudsters manage to move billions of dollars between bank accounts every day.

You can change your credit card number, but you can’t change your date of birth

The knowledge-based authentication tools long used to control fraud are outdated, but most companies haven’t replaced them yet. When a national entity suffers a massive breach, what’s stolen isn’t a replaceable asset such as cash — but unique, deeply personal identity markers such as birthdates and social insurance numbers. Unfortunately, many companies have not yet adopted the new techniques — such as digital device ID and voice biometrics — that are now necessary to protect their customers’ assets.
4. Invest in your people alongside machines

A small investment in culture can pay huge dividends

While some instances of economic crime can be contravened by machines, most require human judgement and interference to avoid. That’s because the most critical factor — the “last mile” to a bad decision — is human choice. Focusing on human behaviour ultimately offers the best opportunity to reduce or prevent economic crime.

While many employers place trust in their employees, a staggering percentage of economic crime (35%) is committed by internal actors. This has been matched by increased regulation: pressure to meet sales targets has become a major source of concern from regulators in the wake of big bank scandals. The Financial Consumer Agency of Canada is reviewing business practices among Canada’s leading banks after the media reported some employees felt pressured to upsell, trick, or even lie to customers to meet sales targets. Similar accusations have recently been made in the media about Canadian telecommunications giants.

Exhibit 16: Fewer companies report having ethics and compliance programs

Q. Do you have a formal business ethics and compliance program in your organization?
Source: PwC’s 2018 Global Economic Crime and Fraud Survey.
Canadian responses unless otherwise indicated.
Percentages are rounded to the nearest whole number.
A majority of Canadian organizations (69%) have a formal business ethics and compliance program in place. However, only 30% make rewarding their employees’ ethical decision-making a priority. This requires buy-in from the top. If the C-Suite starts encouraging and promoting ethics and compliance in the workplace, then employees will likely follow suit.

**Controls and culture: The fraud triangle**

An excellent way to frame the problem of internal fraud is to use a construct called the fraud triangle.

The beginning of a fraudulent act often follows a similar trajectory. It starts with incentive (such as pressure to perform from within the organization). Then, if an opportunity presents itself, the person will usually wrestle with it emotionally. The last piece of the puzzle, which enables them to move from thought to action, is rationalization.

It’s easy for companies to see the pressures of the job as the main cause of internal crime, but our survey suggests otherwise: 64% of Canadian respondents ranked opportunity as the number one factor that contributed to fraudulent activity.

Many companies have over-emphasized the importance of financial incentives when considering what might drive a person to commit fraud. Generally, the motivation here is not money, but rather fear and embarrassment — a fear to admit to making a mistake. With this in mind, organizations need to examine the pressures and incentives coming from the top, beyond the expected financial results. Short-term bespoke controls can monitor whether aggressive sales programs are leading to fraudulent behaviour. A well-publicized open-door or hotline policy can also provide a valuable early warning system of potential problems in an organization.
No matter how committed employees are to a company, it’s important to conduct risk assessments on a regular basis to identify and remediate fraud. Another effective compliance tool is to have employees periodically confirm they understand and have followed company protocols. This exercise can be a powerful deterrent and serve as supporting documentation if needed during the course of an investigation.

The task of detecting and preventing economic crime or fraud is undoubtedly a complex one. It means finding the right blend of technological and people-focused measures, guided by a clear understanding of the motivations behind fraudulent acts and the circumstances in which they occur. Organizations need not resign themselves to the belief that technology is the only solution, or that a certain amount of fraud is simply part of the cost of doing business. Rather, by establishing a culture of honesty and openness from the top down, they can imbue their organizations with a spirit of open accountability, and pull fraud out of the shadows.

How prepared are you? Be sure to ask yourself:

- Have you completed a fraud risk assessment recently? If not, why not?
- Do you know the norms for ethics and compliance in your industry?
- Does your ethics and compliance program explicitly target fraud?
- Are your pressures and incentives compliant with regulations? Are they consistent with doing the right thing for your customers and your people?
- Do you have an open-door policy or hotline that could serve as an early-warning sign of internal fraud?
- Have you probed your internal culture for potential trouble spots?
Conclusion

**Economic crime is not just a problem to solve: it’s also an opportunity to emerge stronger**

We all know the old adage that there are two certainties in life: death and taxes. In fact, there is a third: economic crime. While the perceived impact of economic crime is declining in Canada, organizations can’t afford to “take their fingers off the pulse” with respect to their overall anti-fraud regimes — especially since Canadian respondents are typically reactive in addressing fraud and economic crime.

With a greater understanding of the present threats that face us, we have an even greater opportunity to prepare for events and respond with resilience. By taking a centralized approach to the prevention and detection of fraud and economic crime, and putting the right culture, training, fraud policies, and technology in place, Canadian organizations will be well-positioned to defend themselves against instances of economic crime and emerge even stronger.
Contacts

Want to know more about what you can do in the fight against economic crime?
Contact one of our subject matter specialists:

**Domenic Marino**
National Forensics and Disputes Services Leader
(416) 941 8265
domenic.marino@pwc.com

**Jonathan Allard**
Partner, Forensics Services
(514) 227-6158
allard.jonathan@pwc.com

**Lori-Ann Beausoleil**
Partner, Forensics Services
(416) 687-8617
lori-ann.beausoleil@pwc.com

**Jennie Chan**
Partner, Forensics Services
(416) 815-5057
jennie.m.chan@pwc.com

**Marie-Chantal Dréau**
Partner, Forensics Services
(514) 205-5407
marie-chantal.dreau@pwc.com

**Richard Forand**
Partner, Forensics Services
(514) 227-6159
richard.forand@pwc.com

**Paul Levine**
Partner, Forensics Services
(514) 227-6162
paul.levine@pwc.com

**Steven Malette**
Partner, Forensics Services
(613) 755-5979
steven.m.malette@pwc.com

**Krista Mooney**
Partner, Forensics Services
(403) 509-7336
krista.a.mooney@pwc.com

**Sajith Nair**
Partner, Cybersecurity
(416) 815-5185
s.nair@pwc.com

**James Pomeroy**
Managing Director, Forensics Services
(902) 491-7416
james.a.pomeroy@pwc.com

**William Platt**
Partner, Forensic Technology Services
(416) 814-5710
william.j.platt@pwc.com

Thank you to our Canadian report contributors:

**Domenic Marino**
National Forensics and Disputes Services Leader

**Rob Fischer**
Managing Director, Forensics Services

**Ven Adamov**
Director, Forensics Services

**Steven Malette**
Partner, Forensics Services

**Marie-Chantal Dréau**
Partner, Forensics Services

**Michel Hebert**
Director, Forensics Services

**Simon Gosselin**
Vice President, Forensics Services

**Cyrielle Fischbach**
Manager, Forensics Services

**Peter Hargitai**
Partner, Risk Assurance

**Sajith Nair**
Partner, Cybersecurity
About the survey

PwC's 2018 Global Economic Crime and Fraud Survey was completed by 7,228 respondents from 123 territories. Of the total number of respondents, 52% were senior executives of their respective organizations, 42% represented publicly-listed companies and 55% represented organizations with more than 1,000 employees.