


Crises and threats



When it comes to managing threats, taking action is key. Sooner is better than later.

“There cannot be a crisis next week.
My schedule is already full.”

Henry Kissinger

Six critical threats. A thousand critical details.

No one wants to spend time dealing with crises, which makes it all the more surprising that so many Canadian companies fail to prepare for them. That's what this guide is about—getting prepared for critical threats your company might encounter so they're less likely to turn into crises that destroy value.

The major critical threats facing companies today are familiar to most business executives. They fall into six broad areas, each of which brings a unique set of risks.

- intellectual property theft
- corporate fraud
- money laundering
- foreign corruption
- disputes
- corporate restructuring

Staying ahead of critical threats requires a kind of preparedness many companies don't want to spend time on. With so much to manage today, it's easy to put off thinking ahead about things that might become crises tomorrow. Sometimes that kind of procrastination makes sense—and sometimes it doesn't.

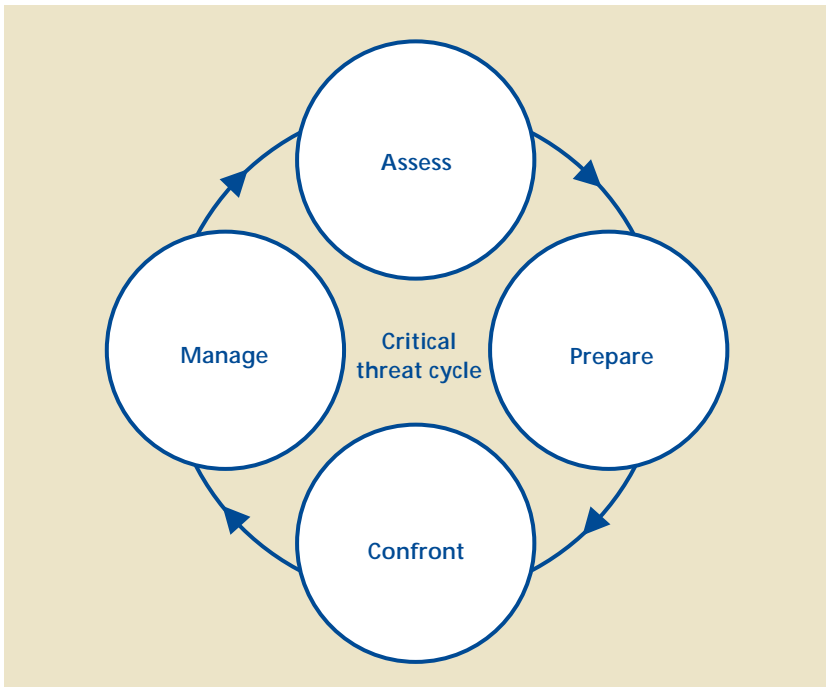
This guide outlines the major areas of critical threats and initial steps to consider for mitigating them. It also includes checklists you can use when you find yourself confronting a crisis. Companies concerned about the potential damage of these kinds of threats will want to take action now.

Risk	Major areas of exposure	First things
Intellectual property theft	<ul style="list-style-type: none"> • License to operate • Rights and licenses • Royalties 	<ul style="list-style-type: none"> • Inventory • Value assessment • Risk review
Corporate fraud	<ul style="list-style-type: none"> • Embezzlement • Conflicts of interest and other corporate policy violations • Fraudulent financial reporting • Procurement and purchasing fraud • Insurance fraud 	<ul style="list-style-type: none"> • Implement anti-fraud programs and controls • Preservation of evidence • Secure information at risk • Secure assets at risk
Money laundering	<ul style="list-style-type: none"> • Terrorist financing • Proceeds of crime 	<ul style="list-style-type: none"> • Risk assessment • Compliance programs • Integrity due diligence • Training & accountability
Foreign corruption	<ul style="list-style-type: none"> • Bribes and kickbacks • Economic extortion • Facilitation payments 	<ul style="list-style-type: none"> • Implement anti-corruption programs and controls • Vendor and partner due diligence
Disputes	<ul style="list-style-type: none"> • Management distraction • Quality of settlement offers • Conflicts of interest on the part of experts • Calculating losses 	<ul style="list-style-type: none"> • Develop a strategy with your legal team • Engage an independent and objective expert • Have resources in place that can move quickly
Corporate restructuring	<ul style="list-style-type: none"> • Cash flow challenges • Redundant assets • Shrinking profits • Shareholder pressures • Missing the red flags of financial distress • Not understanding a company's options 	<ul style="list-style-type: none"> • Stabilize • Strategize • Sustain

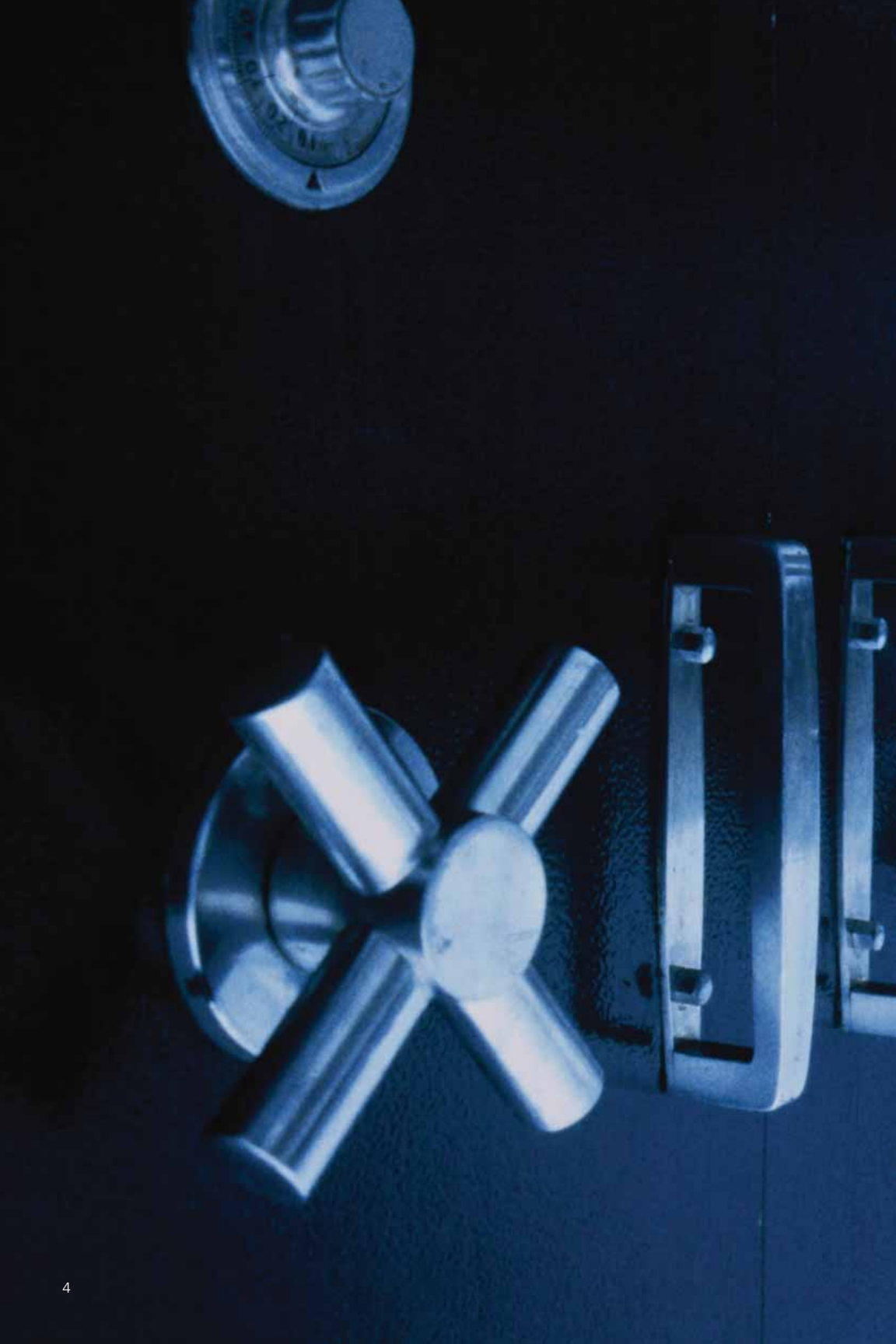
Crises and threats

Business is filled with risks that can destroy value in a heartbeat. We call them critical threats. An accounting error. A problem with stock options. A missing laptop. Even small things can snowball, and the next thing you know, it's front page news, your stock is taking a beating—and your phone is ringing off the hook.

Instead of worrying about critical threats, take steps to mitigate and manage them. Start with a thorough assessment of your exposure in each area and work your way around the critical threat cycle to make sure you're covered.



Managing critical threats requires two things. Getting prepared, and responding when things go wrong. Many of the actions you should take to prepare for threats are the very same actions that make them less likely.



Safeguarding value. Reducing risk.

Intellectual property is like hard currency in many industries, and protecting it is critical. Yet many companies lack a clear understanding of exactly what their intellectual property is—and more to the point, what it's worth.

That inattention creates risks of theft, loss and sacrificed revenue—as well as the potential for costly legal actions. Simply put, when intellectual property is compromised, whether by theft or carelessness, your business can lose value instantly.

Avoiding this risk requires knowing what your intellectual property is, where it is and what it's worth. Only then can you start developing controls to protect it—and keep crises from happening.

Many companies feel their intellectual property is sufficiently managed when their lawyers register patents, trademarks and the like. But the truth is, that's only a small piece of the intellectual property puzzle. A disciplined program of monitoring and controls is necessary to maximize the value and minimize the risks of theft and loss.

First things

- Inventory your intellectual property across the enterprise and by line of business. Define it, catalogue it and keep your inventory current.
- Assess the value of your intellectual property, starting at the top in terms of value. Document your valuations completely.
- Don't go overboard protecting everything. Some intellectual property is not worth the cost of tight control—while other intellectual property can make or break your company. You have to know which is which.

Essential capabilities

Managing the threat of intellectual property loss requires a 360-degree view by a forward-looking team—with competencies in several specialized areas. Between your in-house resources and your outside advisors, make sure you have each of these capabilities covered:

- Intellectual property licensing
- Strategic alliance structuring
- Counterfeit and grey market tracking
- Due diligence
- Patents, copyrights, trademarks and trade secrets
- Intellectual property valuation
- Royalty and revenue recovery

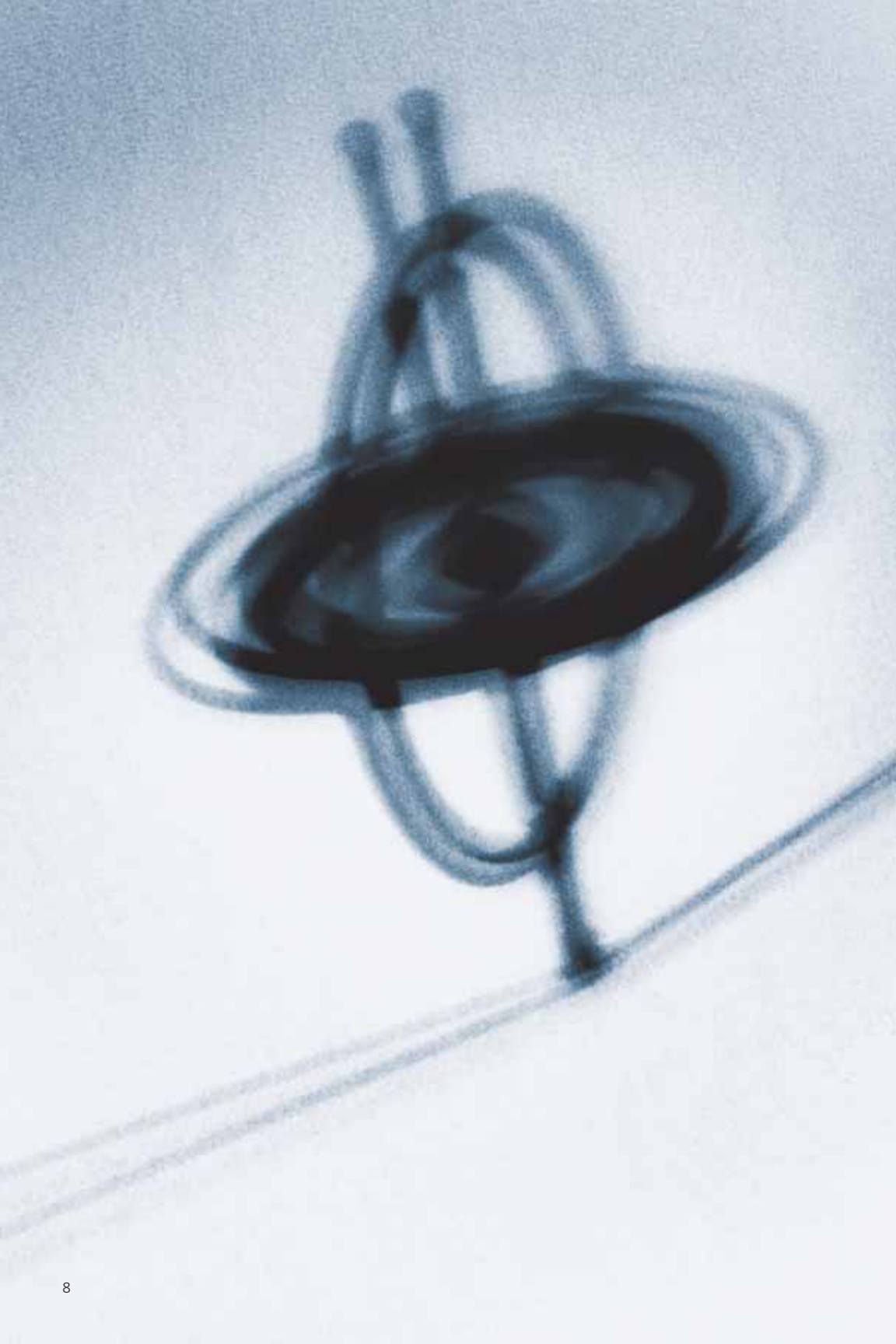
Intellectual property is like real property— just harder to track

Intellectual property is an intangible product that has commercial value. The value of intellectual property is the amount of money someone would spend to create what he could steal from you instead. In some industries, that value is measured in billions of dollars.

Examples of intellectual property include:

- Customer lists
- Industrial designs
- Permits, mineral rights, licenses
- Environmental studies
- Agreements and contracts
- Patents, know-how, trade secrets
- Trademarks and brands
- Business processes
- Product pricing models

Many companies focus only on the threat of their own intellectual property being stolen. But that cuts both ways. For example, sometimes companies accidentally find themselves in possession of intellectual property that belongs to others—knowledge and trade secrets of competitors that come into your business with new personnel. When you're thinking about risks related to intellectual property, don't overlook your exposure because of this kind of infiltration.



No wiggle room

Sarbanes-Oxley and its global reverberations have made financial statement integrity an iron maiden of corporate accountability. There's not an inch of wiggle room—and errors can be fatal.

But fraud does happen—despite your best intentions—and it must be found. The risks are simply too high. Even the hint of irregularity can wipe out value in an instant. Whether it's the cost of litigation or the cost of losing investor confidence, the threats are real and serious.

Preparedness in the area of financial statements starts with an effective fraud risk assessment—and ends with disciplined controls. It also includes a detailed plan for managing crises in the event they cannot be forestalled. The plan should provide specific guidance for securing evidence and for internal and external communications.

First things

- Assess the ‘tone at the top’ to make sure your leadership sets the standard for integrity.
- Evaluate your exposure for major fraud scenarios, including external, internal and collusive fraud.
- Assess fraud risks against current controls. Determine the level of exposure arising from each category of risk.
- Document audit committee oversight. Pay special attention to the risk of management overriding controls.
- Update your crisis communications plan.
- Identify go-to resources for support on short notice.

Essential capabilities

Assessing financial statement integrity goes far beyond number crunching. Sometimes it even comes down to detective work—sifting through email archives—or asking the tough questions that no one really wants to answer. Make sure your team is fully prepared to deal with strategic and technical issues in each of these areas:

- Diagnostics for assessing fraud risk exposure
- Advanced technology for detecting financial statement anomalies
- Data mining
- Loss quantification
- Fraud awareness training
- Forensic accounting

Keeping needles out of haystacks

Fraud costs Canadian businesses and their stakeholders millions of dollars every year, but finding it can sometimes seem like an impossible task. With evidence well-hidden among billions of discrete transactions spread out around the world, it's a lot like finding a needle in a haystack. That's why it makes so much sense to try to deter fraud from happening in the first place.

An anti-fraud program has five elements: a formal fraud risk assessment process, a comprehensive control environment, specified anti-fraud control activities, a fraud-focused information and communication program, and thorough monitoring activities. Each of these elements must be addressed at the highest level of your organization. In fact, the proposed Canadian Securities Administrators (CSA) rules specifically place responsibility for anti-fraud activities with senior management.

Beyond protecting the business from the cost of fraud and addressing regulatory requirements, many organisations regard this as an opportunity to communicate to stakeholders that they are doing everything possible to protect against the risk of fraud. An effective anti-fraud program can preserve your assets and reputation, while demonstrating due diligence to regulators. In the event of a regulatory action, an effective compliance program will also go a long way in reducing potential fines and showing that management did all it could to avoid problems.



It all comes out in the wash

The government of Canada has passed new legislation (Proceeds of Crime [Money Laundering] and Terrorist Financing C-25) in 2007, which calls upon an ever-increasing spectrum of participants to take an active role in the prevention of money laundering. Like it or not, that's the world we're operating in—and companies involved in financial services, insurance, real estate, accountancy, brokerage, gaming and precious metals have to take these new requirements seriously. The personal and corporate risks are simply too high to ignore.

No business, cash-intensive or not, is immune from becoming the unwitting accomplice of money launderers. These challenges are compounded for global companies with multiple legal and regulatory requirements, languages, systems and business cultures.

As the international community moves toward tighter regulations and more aggressive enforcement, companies operating in global markets face new responsibilities to identify, report and prevent money laundering activities, no matter where in the world they do business.

First things

- Establish, test and monitor enterprise-wide policies and procedures.
- Maintain a strong control culture.
- Designate a Chief Anti-Money Laundering Officer.
- Identify who you'll depend on for external counsel in each jurisdiction.
- Provide education and training in crisis management for key individuals.
- Build in continuous improvement to reflect changing legislation.
- Identify resources for conducting electronic transaction look-backs.
- Stress-test your capabilities to detect risk.
- Develop a comprehensive incident management plan.
- Test your detection framework to make sure it actually works.

Essential capabilities

As money launderers have become increasingly sophisticated, so too must the management of this critical threat. Conducting effective forensic investigations and evaluation of compliance frameworks involving electronic data, in particular, requires advanced technology, deep experience and these specialized capabilities:

- Risk assessments at the enterprise and business unit level
- Protocols for responding to regulatory orders
- Drafting and enhancing policies and procedures
- Training, compliance assessments, forensic analysis
- Advanced data mining technology
- Chain of custody controls
- Investigations

No room for error

While all the critical threats covered in this book are significant, the threat of money laundering is uniquely troublesome. Perhaps it's the association with illegal drugs or terrorism, perhaps it's the implication of organized crime. Whatever the reason, suspicion of money laundering can destroy personal and corporate reputations faster than almost any other threat. Even the hint of involvement can send your stock price into a tailspin. When a money-laundering crisis begins to emerge, there is no room for error. That means you have to be prepared well in advance. Know exactly who your team will be and how everyone will respond.

Most important of all, recognize the fact that regulations related to money laundering are becoming more and more complex. International businesses need to be aware of laws that can reach over borders and financial systems causing unexpected impacts and publicity.

In today's zero tolerance corporate climate, taking responsibility to safeguard your organization, its employees, directors and shareholders from the fallout of possible criminal and civil fines and penalties is essential.



The world is watching

Canadian companies that do business with foreign governments are at risk for problems associated with corrupt practices regulations. The only question is whether you're taking the threats seriously enough to prevent them from becoming crises.

The stories are legendary—bribery, possession, money laundering and more. In some countries, these practices are business as usual. Which is all the more reason to take this issue seriously.

A new salesperson for a business unit in Africa greases the wheels to get a deal done. A production manager in Indonesia bribes officials to get materials delivered on time. It's an age-old practice with many names—and it's a surefire way to destroy the value and reputation of any Canadian company.

Some argue that the chances of getting caught are slim. That doesn't matter, because the consequences of getting caught are enormous. Your company can be liable for punitive damages, your officers and directors face personal and criminal risk, governments can impose sanctions and your company can be prohibited from getting future contracts.

First things

- Know your agents in foreign countries. Understand what you're paying them—and why.
- Scrutinize all foreign payments, especially those made through local bank transactions.
- Monitor all documentation related to payments and transactions.
- If something seems unusual, don't hesitate to investigate. If something seems too good to be true, it probably is.
- Insist on including right to audit clauses in all contracts.

Essential capabilities

If your leadership behaves in accordance with ethical, legal and moral guidelines, that will go a long way toward instilling integrity throughout the organization. Beyond that, be sure you have your fingers on the pulse of all potential risks around corrupt practices, especially related to M&A. Don't cut corners on any of these capabilities:

- Risk assessment related to corporate structures
- Analysis of existing contracts and relationships
- Investigations of reputation and integrity of principals
- Corporate culture assessment
- Assessment of internal controls and compliance programs
- Evidence preservation

The long arm of the law

Canada's Corruption of Foreign Public Officials Act (CFPOA) came into force in 1999. Violations can result in imprisonment and/or fines for companies and their individual officers, directors, employees and agents.

The CFPOA is the counterpart to the U.S. Foreign Corrupt Practices Act, which deals with bribery and accounting. Its bribery provisions apply to U.S. public and private companies, and U.S. and foreign companies registered with the SEC, including Canadian companies. Accounting provisions apply to U.S. and foreign companies registered with the SEC, as well as foreign subsidiaries and affiliates of issuers.

High-stakes conflicts

Corporations in Canada and around the world face ever-increasing threats of litigation and related business disputes. Competitors, customers, shareholders, regulators and even employees pose risks ranging from class action suits to contract enforcement and more. When these kinds of disputes flare up, speed, discipline and clear-eyed professionalism become the essential ingredients for effective resolution.

Companies today may encounter disputes in many areas, but five categories of disputes are especially complex: business interruption insurance, buy-sell disputes, class action settlements, construction disputes and intellectual property disputes. Each of these brings with it a host of technical issues that require involvement by specialized counsel and experts.

But the challenges go beyond complexity: disputes can become emotional roller coasters, too. This combination of complexity and passion can lead to high drama that may cloud decision making and effective action. That's one reason companies engage balanced teams of advisors for dispute management. Legal experts. Damage quantification experts. Forensic investigators. Expert witnesses. Economists. Whoever and whatever it takes to make the case—that's what your team should bring to the table. By engaging a diverse group of professionals, you can be more confident that every angle is being covered and minimize the hazards of "group think."

Major areas of high-stakes conflicts	
Critical threats and opportunities	
Business interruption insurance	<ul style="list-style-type: none"> • Design risk management for new facilities • Loss accounting • Establishing the “as was” replacement cost • Negotiating with insurers
Buy-sell disputes	<ul style="list-style-type: none"> • Early issues identification • Arbitrator selection • Documentation of positions
Class action settlements	<ul style="list-style-type: none"> • Appeals process support • Benefit calculation and distribution • Claim population identification and notification • Searches for difficult-to-locate class members • Status and tax reporting
Construction disputes	<ul style="list-style-type: none"> • Ensuring maximum recoverable damages • Accelerating claims and payments • Mitigating risk • Identifying fraudulent activity
Intellectual property disputes	<ul style="list-style-type: none"> • Discovery • Deposition preparation • Settlement strategies • Trial preparation

First things

- Establish a methodology for tracking early indicators of potential disputes.
- Build a team of advisors who can hit the ground running on short notice.
- Create a dispute resolution plan that includes evidence preservation and documentation.
- Line up experts early.

Essential capabilities

Expert management of disputes requires experience in areas as diverse as tax, information technology, insolvency, corporate finance, mergers and acquisitions, compensation, accounting and auditing, computer forensics and corporate governance. Other specialized capabilities include:

- Arbitration
- Expert testimony
- Assessing risk and damage exposure
- Business and asset valuations
- Forensic investigations
- Business insurance analysis
- Royalty recovery
- Construction disputes
- Securities litigation support
- Class action litigation support

You need the truth

In the pressure-cooker environment surrounding high-stakes disputes, it's easy to start believing your own press. But if you get too caught up in winning, you may find yourself pushing for all-or-nothing solutions that can increase risks. Especially when people driving the process are entrenched with personal agendas that might conflict with the corporate goals.

Sometimes disputes are not about winning or losing at all. Sometimes they're about settling to minimize risk and damage. And sometimes they're simply about avoiding protracted litigation that can distract your leadership team from staying focused on the business. To balance all these potential conflicts, the first thing you'll need is a clear view of the truth.

Getting that view requires the right investigative and analytical tools in the hands of experienced advisors who won't sugarcoat the facts. So when you finally come face to face with the big questions, you'll have complete confidence in the answers.



When all else fails

Among all the critical threats facing companies today, the risk of a business loss and/or insolvency is one of the most feared. Its impact on management, employees, shareholders, customers, suppliers, and even communities is real and potentially catastrophic. In the face of such risks, it is still possible for forward-thinking companies to preserve value and protect valued employees by taking decisive action. As soon as there's even the hint that a company may have trouble sustaining itself, these steps should be taken.

- **Stabilize.** At the first sign of trouble, a company must determine what's going wrong and understand its options for action. This requires answering tough questions and preparing for even tougher decisions that can include revisions of financial forecasts, reductions in workforce, sale of redundant assets, and difficult contract renegotiations.
- **Strategize.** Once operations are stabilized, restructuring opportunities or other forms of operational turnarounds can emerge. Experienced advisors who understand your options are critical.
- **Sustain.** A successful restructuring requires a plan for keeping the company going. That may involve new management, cash flow realignment, improved financial controls, or a focus on continuous operational improvement.

If your business is underperforming, you need to take action before it's too late. The risks associated with doing nothing – or doing the wrong thing – can be catastrophic. Regardless of the root of the problem, stakeholders need to see that the organization is implementing the right strategic actions quickly and effectively. When a liquidity crisis is looming, engaging experienced specialists to conduct a thorough situational and financial analysis is the surest path to cost-effective and timely results.

First things

Develop a tactical plan so you can:

- Implement cash flow management tools.
- Accelerate cash receipts.
- Prioritize cash disbursements.
- Challenge management assumptions.
- Create credible communication channels.

Essential capabilities

By initiating remedial action in the face of liquidity risks, you'll inspire stakeholder confidence and gain the time you need to achieve the best possible outcomes. Specific capabilities your team must have include:

- Turnaround capabilities
- Cost structure analysis
- Debt structuring and refinancing
- Liquidity management
- Asset disposition
- Cash management and creditor communication
- Management or liquidation of loan portfolios

When what you need most is time

In today's overheated business environment, underperforming companies face a real challenge. Often the management team goes through drifting and denial stages, which can threaten ongoing viability. Companies need to take action before it's too late.

A plan of arrangement under the *Companies' Creditors Arrangement Act* (CCAA) provides an underperforming company with debts in excess of \$5 million with the flexibility to devise a plan of compromise with its creditors in the hopes of resolving its financial problems. CCAA offers a distressed company protection from the actions of creditors and other stakeholder parties and allows the company to continue operations while a plan of arrangement is formed.

It is critical that the creditors vote to approve any plan of arrangement. If the plan is accepted by the required majority of creditors, it becomes a legally binding agreement for all. A plan of arrangement can be drafted in a variety of ways and can be tailored to suit your unique circumstances. It can:

- Reduce total debts
- Allow a longer period of time to repay debts
- Stop further interest from being added to unsecured debts
- Stop lawsuits and other debt collection activities

A company can use CCAA protection to effect a financial restructuring while it deals with underlying operational problems. For a plan of arrangement to be successful, the underlying business must be viable and management must be capable of executing a restructuring. Additional time is often required to effect a restructuring, and a plan of arrangement will provide that time.

Ready or not

Every business faces critical threats—and some of them can become crises no matter how well a company prepares. Whether you're working to recover damages in a dispute or preserve your reputation in the face of a government inquiry, sure-footedness and expert knowledge are critical to success.

Fortunately, the same actions that will help your company avoid crises will also help you manage them if things escalate. Those actions require having a clear view of the road ahead, putting an experienced team into place, getting an early start on gathering evidence and documentation, and understanding what you can and cannot do in any particular situation.

When it comes to addressing critical threats, many companies do not have the required expertise in house. That means they must turn to outside advisors who can work together to preserve value and manage threats effectively.

That's where we can help.

About Deloitte

Deloitte, one of Canada's leading professional services firms, provides audit, tax, consulting, and financial advisory services through more than 6,800 people in 51 offices. Deloitte operates in Québec as Samson Bélair/Deloitte & Touche s.e.n.c.r.l. The firm is dedicated to helping its clients and its people excel. Deloitte is the Canadian member firm of Deloitte Touche Tohmatsu.

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firms, and their respective subsidiaries and affiliates. As a Swiss Verein (association), neither Deloitte Touche Tohmatsu nor any of its member firms has any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names "Deloitte," "Deloitte & Touche," "Deloitte Touche Tohmatsu," or other related names. Services are provided by the member firms or their subsidiaries or affiliates and not by the Deloitte Touche Tohmatsu Verein.

www.deloitte.ca

