

Deloitte.



Not on my watch

Protect your assets and
preserve your legacy

Under siege

Fraud, theft and employee misconduct have always been an unfortunate business reality. But new economic and competitive pressures have changed the landscape, introducing new risks and putting your reputation on the line.

Outsourcing partnerships, mobile employees, off-shore operations and new technologies have blurred organizational boundaries and complicated the job of protecting business assets. As a result, there are countless opportunities to exploit the weaknesses that go hand in hand with progress. Even people with the best intentions can inadvertently set off a chain reaction due to errors and omissions.

So businesses face a fundamental paradox. Large-scale information sharing has become a competitive

necessity. At the same time, protecting intellectual property, business assets and confidential information is critical to an organization's survival.

With the right plan in place, you can mitigate these risks. The first step is to assess and understand your current vulnerability to information loss and theft, fraud, misconduct, regulatory failure and other risks.

We wrote this perspective to help you get a head start on protecting your organization – and your legacy – in the ever changing environment of risk.

Headline headaches

In our experience, there are four main reasons that organizations and businesses end up making news for the wrong reasons:

- 1 Fraud, theft and misconduct
- 2 Regulatory and compliance issues
- 3 Problems with information security, contracts and large technology projects
- 4 Accounting and reporting irregularities

Today, it's easy to feel like you're under siege. There are plenty of people who would do your organization harm given the opportunity.

Don't let it happen on your watch. It's not just your organization's reputation on the line – yours is, too.

Commissioner Cavoukian investigating online privacy breach...

Information and Privacy Commissioner/Ontario, July 28, 2009

The reasons fraud spikes in a recession

time.com, May 20, 2009

Canadian researchers find cyberspace spy network

Canwest, March 30, 2009

UN warns the next world war will be online

gss.co.uk, October 7, 2009

New approach needed to fight securities fraud...

The Globe and Mail, April 03, 2009

Tax agency probes restaurants that hide cash sales

Canadian Press, November 8, 2009

What you don't know can hurt you

Loss or theft of corporate information. Accounting misstatements. Breaches of procurement rules. A lost laptop filled with confidential information and intellectual property. Product recalls. Misappropriation of assets. Regulatory investigations. Any one of these could cause your company to make headlines – for all the wrong reasons.

The key is knowing where you're at risk, and taking the right steps to guard against the unthinkable. That requires an accurate and up-to-date accounting of your current operating environment and the marketplace – everything from where your most valuable information lies, to what processes and controls your organization have in place, where your industry is exposed, what regulations you need to comply with, and a lot more.

If you're uncertain about your assets, controls, or where you're most exposed to risk, you're flying blind. And in this environment, what you don't know can hurt you.

“More than two-thirds of Canadian companies are victims of fraud”

CA Magazine, April 2009

When things get personal

When executives are concerned about events involving fraud, security breaches, systems outages, failed projects, accounting irregularities and other similar scenarios, the financial impact can be the most worrisome issue.

These events can also take a toll on other aspects of your business. Consider the impact a few negative stories can have on your organization's hard-earned reputation and brand. It doesn't take a PR expert to know that it can take years to recover from the devastating impact a security breach or theft can have on your brand once it hits the press. Some organizations never recover.

For C-suite executives and the board of directors, there's one more element of risk: **your own legacy and reputation**. If your organization generates the wrong type of headlines, you can expect it to follow you throughout your career. In some cases, you could even be fined or sued for lack of appropriate oversight.

A company with a profit margin of 5% would need to generate an additional \$4 million in revenues to recover losses from a \$200,000 event.



The weakest link?

No matter where organizations and businesses fail in protecting themselves against harm, they almost always share one common factor. People are the reason that no risk mitigation plan is foolproof.

It's not just about those who intentionally cause harm. Mistakes happen, too. Which means it's important to understand where your organization has significant potential for error – and where those errors can have a disproportionate effect.

Believe it or not, that's the easy part. It's a lot tougher to find out where you're exposed to risk from people with malicious intent who are actively working to cover their tracks.

The best place to start may be the simplest: understand your exposure to different threat scenarios. Then link these scenarios to people – and not just your employees. Customers, suppliers, and contractors – are also in a position to do harm. Then, ensure you have the right set of controls in place to address these scenarios.

While you'll probably never be able to predict the behavior of someone with bad intentions, you need to have the right monitoring controls to detect and address issues quickly.

A survey of 945 individuals who were laid off, fired or quit their jobs in the past 12 months shows that 59% admitted to stealing company data and 67% used their former company's confidential information to leverage a new job.

Ponemon Institute, Feb 2009

A question of balance

It's one thing to have the right capabilities in place to investigate wrongdoing once you know it has occurred. You also need to balance your reactive risk management capabilities with your ability to be proactive.

Because it's just as important to fight these risks before they strike. That's much more difficult – because it can be like grappling with an invisible foe.

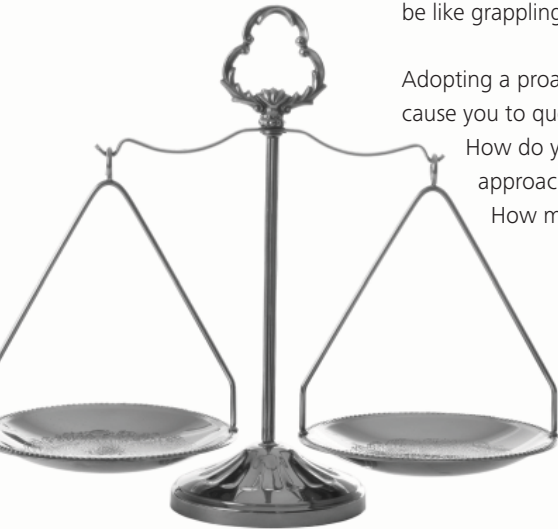
Adopting a proactive approach may cause you to question your efforts.

How do you know if your approach is working?

How much is too much?

Fortunately, there is a method to the madness. Start by connecting your investment in controls with your organization's tolerance for risk and the value of assets you are protecting. Then attach dollar figures to which risks you're able to live with – and which are unacceptable. Get granular about which specific threats matter most – and whether the prevention methods required to mitigate them make sense for your organization.

A measured, logical approach like this can help you balance your proactive and reactive risk management investments.



Getting started

To identify where you are at risk, it's important to ask the right questions first. Here are some that we've found to be most useful in helping our clients get started.

- ✓ **Are your controls adequate** to detect and prevent wrongdoing in enough time to make a difference?
- ✓ **Are you being proactive** enough in detecting fraud, waste and abuse?
- ✓ **Have either downsizing** or economic pressures reduced the effectiveness of your controls?
- ✓ **Are your policies** being followed? How do you know?
- ✓ **How many incidents** are you experiencing compared to your competitors? What accounts for the difference?
- ✓ **Do your auditors,** regulators, or compliance teams report repeat weaknesses?
- ✓ **Are your employees** following the rules when it comes to reporting expenses, awarding contracts, and checking quality?
- ✓ **Is your employee** turnover rate high compared to industry benchmarks?
- ✓ **Do you know** who you're doing business with? Are current due diligence processes adequate?
- ✓ **Is your intellectual** property protected? How?
- ✓ **Does your organization** have a culture of security, integrity and trust? How do you maintain it?

We can help

Like many companies, you may be relying on specialized expertise to address concerns in each of these areas. Increasingly, the lines are blurred between these different areas. There's a lot of overlap, and the best approach is to tackle them as a highly interconnected set of challenges using world-class expertise.

Kennedy Information recently named Deloitte the global leader in both forensic investigations and risk management consulting, stating that Deloitte "operates the world's largest and most robust risk consulting practice" with "offerings that stretch across every segment of the market."

That means we have the ability to examine the risks you're facing today from every angle. And when it's time to execute, we're ready – no matter where the problems lie, or what skills are required.

If you're looking for advisors who can give you the whole picture when it comes to managing risk, call us.

Adel Melek

National Co-Leader

Partner

416-601-6524

amelek@deloitte.ca

Gary Moulton

National Co-Leader

Partner

416-601-5737

gmoulton@deloitte.ca

For more information visit www.deloitte.ca

1858 150 2008
Deloitte celebrates
150 years of professional service



www.deloitte.ca

Deloitte, one of Canada's leading professional services firms, provides audit, tax, consulting, and financial advisory services through more than 7,700 people in 57 offices. Deloitte operates in Québec as Samson Bélair/Deloitte & Touche s.e.n.c.r.l. Deloitte & Touche LLP, an Ontario Limited Liability Partnership, is the Canadian member firm of Deloitte Touche Tohmatsu.

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu and its member firms.

© Deloitte & Touche LLP and affiliated entities.

Designed and produced by National Design Studio, Canada 09-1887