"IF ONLY YOU HAD COME TO US SOONER" STRATEGIES FOR AVOIDING INSOLVENCY

We know this publication is about dispute resolution, but what we really want to talk about in this article is avoiding insolvency and bankruptcy disputes.

"If Only You Had Come to Us Sooner"

As insolvency lawyers, we deal with business failures. That is to say (not to put too fine a point on it), businesses that go bust or are about to do so. We sometimes make the mistake of assuming that the boards of directors and management of companies are aware of the alternatives available in the event of a cash crunch or a downturn in business income or cash flow. However, over and over again we see situations in which management comes to us when it is really too late to effect any kind of meaningful repairs. Those cases become more of a salvage operation than a true restructuring.

Clients who come to speak to us are almost invariably reluctant to do so (which is only human nature). There is usually no way the CEO wants to reveal that the company is heading into the tank. Nor does the CFO, no matter how vigilant and astute, want to break the news to management and the board that the company is in dire straits.

It is one of those situations, which we are sure you can all visualize, where the professionals say "If only you had come to us sooner…" ("But Doctor, how bad is it?") This is something of an ugly parallel, since medical issues can result in very severe and final consequences. However, business troubles can often be reversed. We can say from experience that, with our help, many businesses have come back from the brink to a flourishing new life.

Duties of Directors and Officers

All directors and officers of corporations, whether large or small, should understand that it is part of their duties to know the financial state of the

IN THIS ISSUE

business they are managing, and to identify the early stages of financial trouble, so that alternatives and solutions can be identified and addressed. This is also a key function of in-house counsel. In other words, you always have to be on alert to spot the financial situations that may be coming down the road.

No matter how competent your CFO may be, we have seen situations where they are reluctant to give the bad financial news to management and the board. It is important that there be an open dialogue among those who are directly in touch with the financial situation of a business. They must be free, without any negative consequences, to give to management and the board a clear and honest report on its financial state. Bottom line: the CFO has to give management and the board the bad news, and they have to listen to it (think for a moment about Conrad Black and Garth Drabinsky).

Talk to Your Banker

There are not many businesses these days that do not face some sort of financial crisis, at one time or another, whether from the inability to borrow or the failure to raise funds through equity financing. These circumstances may put a company into a cash crunch that could force serious decisions to be made very quickly on downsizing the work force or restructuring the overall capital structure. One of the reasons we stay busy is that management often tries to avoid making these decisions, until they end up being made for them (by the banks, trade creditors and so on).

"suppliers often support a restructuring plan..."

The first and best restructuring option is a "soft" or informal restructuring, often completed with the input (not always welcome, but not always avoidable) of the bank. An ounce of this kind of prevention can be worth many pounds of cure. If there is financial trouble on the horizon (or at the doorstep), one of the worst things you can do is "stonewall" your banker or other lender by not returning their phone calls or emails. Bankers (and we know, because we act for almost all of them from time to time) hate to be kept in the dark. It's a far better strategy to keep your banker informed of whatever issues your business is facing.

There was a time (20 or more years ago) when bankers were much more aggressive, and would simply send in a receiver at the first sign of trouble. These days, bankers realize that helping their borrowers through difficult financial times is a smart thing to do. Assisting with a restructuring often improves their chances of getting their loan repaid. It is pretty well accepted these days that almost every business has more value as a going concern than it does in a shutdown or liquidation.

There Are Options

If a "soft" restructuring isn't possible, what then? Avoiding bankruptcy or some other form of insolvency, like receivership, is generally preferable. This is what creditor protection legislation is designed to do. In Canada, there are two statutory regimes for restructuring a troubled business (whereas in the United States, there is only one, i.e. "Chapter 11"). There is ample opportunity for businesses in Canada in financial difficulty to restructure and, more importantly, to settle with their creditors at less than 100 cents on the dollar.

Both the Bankruptcy and Insolvency Act and the Companies' Creditors Arrangement Act give a company the opportunity to obtain a "stay" of legal proceedings by creditors. While a business is under the protection of a stay, none of its creditors can pursue it, and other people that it does business with cannot usually stop doing so. The business gets some "breathing room" to formulate a plan to present to its creditors that will provide for them a better result than if it were simply to go bankrupt (in which case they would usually get nothing).

It is the duty of management and the board to examine all options available to a corporation in distress. There is nothing shameful about a company

having financial problems (look, for example, at General Motors and Chrysler). In our view, it is one of the fundamental duties of officers and directors to examine, in appropriate circumstances, the options available under this legislation. We often tell clients that it is better to have a Plan "B" that you hope never to use, than to face the possibility of Plan "A" evaporating in circumstances where there is no time to make a Plan "B"

The legislation permits a business to make a "deal" with its creditors which will allow the business to carry on, clean-up the balance sheet and address unmanageable debt. We have seen numerous situations in which creditors (remarkably) accept only a small percentage of their claims against the debtor company in satisfaction of their entire claims, because the obvious alternative is bankruptcy, in which case they would typically receive (as the saying goes) "boom-all". Suppliers often support a restructuring plan that gives them only a small percentage recovery, because they have already written off the bad debts and a successful plan will ensure the survival of a significant customer (although they are unlikely to supply goods or services on credit going forward!). It is often a real challenge for us to get a company to believe that a restructuring plan will not be seen as a big deal by many of its trade creditors. But that is exactly how most trade creditors react in most situations.

Another significant benefit of insolvency legislation is that it permits businesses to deal with all of their creditors at once, which is obviously faster and cheaper than a one-off negotiation with each creditor in a "soft" restructuring, where any one can be the bad apple that causes the whole plan to come crashing down. The key to restructuring legislation is that it allows the majority of creditors to "cram down" on the minority, i.e. approve a plan that is binding on all creditors, even those who vote against it.

In our experience, in an insolvency scenario management always overestimates its ability to work out a consensual deal with all of their creditors separately. In reality, most of the time there are just too many moving parts to be able to get that done. In a formal restructuring creditors faced with a "cram down" are much more likely to be reasonable.

Formal restructuring proceedings have other benefits. For example, officers and directors can be personally liable for certain obligations of the company, like unremitted employee withholdings and unpaid wages and holiday pay.

Most of this personal liability can be dealt with in a formal restructuring. This is a legislative policy decision designed to encourage officers and directors not to jump ship at the first sign of trouble.

So, we are talking here not about dispute resolution but dispute avoidance – which is perhaps the best way to resolve a dispute! In the case of a business in financial difficulty, it is absolutely fundamental to seek a resolution that will not result in months or years of litigation and bitter disputes over who gets what and who has to pay whom.

Clive S. Bird
Tel: (604) 640-4103
cbird@blgcanada.com

Magnus C. Verbrugge
Tel: (604) 640-4198
mverbrugge@blgcanada.com

PRIVACY LEGISLATION: What You Need to Know

Introduction

Private sector organizations throughout Canada are subject to personal information protection legislation when they collect, use or disclose personal information – either the federal Personal Information Protection and Electronic Documents Act ("PIPEDA") , the British Columbia Personal Information Protection Act ("PIPA"), the Alberta Personal Information Protection Act or the Quebec Act Respecting the Protection of Personal Information in the Private Sector. Other statutes deal specifically with the collection, use and disclosure of personal health information. This article focuses on PIPEDA and PIPA.

The core concepts underlying PIPEDA and PIPA are straightforward – the requirement of informed consent to the collection, use and disclosure of personal information; the need to develop policies and procedures to address an organization's privacy practices, including facilitating individuals' access

to, and correction of, their personal information; and the need to develop appropriate safeguards to preserve the security and integrity of personal information within an organization's control. The complexities lie in translating these general principles into concrete action, which are addressed by the checklist at the end of this article.

Which Act Applies to Your Organization?

PIPEDA applies to federal works, undertakings and businesses (such as chartered banks and airlines) engaged in commercial activities, and to other organizations that transfer personal information across provincial borders for consideration. It also applies to all provincial organizations which collect, use and disclose personal information within a province in the course of commercial activities, unless their province has enacted legislation that is "substantially similar" to PIPEDA, as assessed by the federal cabinet.

PIPA and its counterparts in Alberta and Quebec (as well as certain personal health information statutes) have been designated as being substantially similar to PIPEDA and apply to the collection, use and disclosure of personal information by most organizations within those provincial boundaries. The other provinces are under the PIPEDA regime. PIPA applies to a much wider array of organizations than PIPEDA, including trusts and non-profit organizations. PIPA also applies to the use or disclosure of personal information collected before it came into force.

Canadian privacy commissioners have indicated a willingness to enforce privacy obligations against domestic organizations even in connection with personal information that is transferred abroad for processing or other reasons.

Similarly, organizations based in foreign jurisdictions may find themselves subject to Canadian personal information protection legislation to the extent they have a real and substantial connection to Canada and possess the personal information of Canadians.

What is "Personal Information"?

"Personal information" is, stated simply, information about an identifiable individual. This definition is very broad, and includes an array of information that, taken together or in combination with other information, may allow someone to identify an individual. This may include residential address,

"...an organization may only collect, use or disclose personal information for a purpose that a reasonable person would consider appropriate in the circumstances."

likeness, financial status, investment activity, marital status and employment status PIPA excludes from the scope of activities to which it applies "contact information" and "work product information". Contact information is information which enables an individual to be contacted at a place of business. Work product information is the information produced by people at work.

Development of Policies and Procedures and Appointment of a Privacy Officer

Both PIPA and PIPEDA require organizations to develop the policies and procedures necessary to comply with the rules relating to the collection, use and disclosure of personal information, including developing a process for responding to individual complaints and requests for access to personal information. Information regarding these policies and procedures must be made available to individuals on request, together with the contact information for the privacy officer designated by the organization.

Consent

The fundamental principle underlying PIPEDA and PIPA is the concept of consent. Subject to certain prescribed exceptions, the legislation requires an organization to disclose to individuals the purposes for which their personal information will be collected, used or disclosed before those activities occur, and obtain their consent to that.

Although express informed consent is ideal (and may be required depending upon the sensitivity of the information in issue), PIPA provides that an individual may be taken to have consented to the collection, use and disclosure of their personal information for a purpose that would, at the time of the activity, have appeared "obvious to a reasonable person", if they provided the information voluntarily.

Given the administrative, technical and practical difficulties associated with obtaining express consent, an "opt-out" mechanism – in which consent is assumed unless the individual notifies the organization that they do not consent – is often more efficient in many circumstances. PIPA expressly permits "opt-out" mechanisms if four conditions are met: (a) the organization provides a notice of the purposes for which it intends to collect, use or disclose the information; (b) the individual is given a reasonable opportunity to decline to consent; (c) the individual doesn't decline within the specified

time; and (d) the collection, use and disclosure of the information is reasonable, having regard to its sensitivity. Although PIPEDA also permits "opt-out" mechanisms, it is not as specific about the circumstances justifying them. PIPA allows individuals to withdraw their consent to the collection, use and disclosure of their personal information by giving reasonable notice., subject to certain limitations.

PIPEDA and PIPA recognize that it is sometimes impractical to obtain informed consent. They permit information to be collected, used and disclosed without consent if, among other things, doing so is clearly in the interests of the individual and consent cannot be obtained in a timely way.

There are many statutory exceptions to the requirement that personal information only be collected, used or disclosed with consent. For example, under PIPEDA and PIPA: information may be collected, used and disclosed without consent if it is reasonable to expect that obtaining consent would compromise the accuracy of the information, the collection, use and disclosure of the information is reasonable for an "investigation" and it is reasonable to believe that an offence may occur or has occurred. An organization is also generally relieved of the need to obtain consent if the collection, use and disclosure is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or of a province. Under PIPEDA, Informed consent is not required if the organization's collection, use or disclosure of the information is required by law. PIPA also provides an exception if the collection, use or disclosure of the information is only "authorized" by law.

It is easy to become lost in the maze of exceptions and sub-exceptions to the general rules of informed consent in PIPEDA and PIPA. It is therefore always important to return to the over-arching principle of both statutes: an organization may only collect, use or disclose personal information for a purpose that a reasonable person would consider appropriate in the circumstances.

Outsourcing

PIPA expressly permits organizations to use third-parties to process information without obtaining the consent of the individuals to whom the information relates, and the federal privacy commissioner has concluded a similar right exists under PIPEDA. The third party must use the information

only for the purposes originally authorized by the individual and to assist the first organization, and the third party remains responsible for the information while it is in its custody. Appropriate agreements must be in place to govern such relationships.

Business Transactions

Subject to certain exceptions, PIPA expressly allows personal information regarding employees, customers, directors, officers and shareholders to be disclosed in the course of due diligence activities undertaken in connection with transactions. The information must be necessary to determine whether to proceed with the transaction, and there must be a non-disclosure agreement limiting the purposes to which the receiving organization can put the information.

If the transaction does not proceed, the recipient of the information must destroy it or return it to the disclosing organization. If the transaction does close, personal information relevant to the part of the organization affected by the transaction may be disclosed, but the affected individuals must be informed that the transaction has occurred and that their personal information has been disclosed.

Employee Personal Information

The general provisions of PIPEDA apply to information about employees that is collected, used and disclosed only in connection with the operation of a federal work, undertaking or business. Where PIPEDA applies in a province, it does not affect the collection, use and disclosure of information regarding employees of provincially-regulated organizations. However, PIPA contains specific provisions governing municipally regulated organizations' collection, use and disclosure of "employees personal information". PIPA defines employee personal information as "personal information about an individual that is collected, used or disclosed solely for the purposes reasonably required to establish, manage or terminate an employment relationship between the organization and that individual", but excluding "work product information".

Apart from the many general exceptions to the consent requirement, PIPA allows an employer to collect, use and disclose employee personal information without the individual's consent if: (a) that is reasonable for the purposes of establishing, managing or terminating an employment relationship with the individual; and (b) the organization notifies the individual that it will be doing so for those purposes. Note that consent is not required – it is only necessary to inform the

employee (unless an exception to the consent requirement applies).

Access and Correction

One of the most potentially onerous aspects of PIPEDA and PIPA is the requirement that individuals be given reasonable access to their personal information and the ability to correct it. Typically, an organization is required to respond to such requests within 30 days.

In addition to the personal information itself, PIPA requires an organization to disclose, in response to an access request, information regarding how the information is being used and has been used, and the names of the individuals or organizations to which it has been disclosed.

Under PIPA, access may be refused if disclosing the information would reveal confidential commercial information that could reasonably be expected to harm the competitive position of the organization, if an investigation has not yet been completed or if the information is covered by lawyer-client privilege. Access must be refused if disclosure would reveal the personal information of another individual, but attempts must be made to sever that information and provide the balance.

Retention of Personal Information

PIPEDA and PIPA also address document-destruction practices. Subject to other legislation that imposes specific time limitations, personal information used to make a decision directly affecting an individual must be retained for at least one year. Otherwise, subject to specific statutory or regulatory directions to the contrary, information should be "anonomyzed" or destroyed as soon as it is reasonable to assume that it is no longer required for the purpose for which it was collected, if there are no other legal or business reasons for maintaining it.

Security

Perhaps the most significant exposure to legal claims (and the greatest likelihood of statutory claims, as discussed below) arises from "identity theft" and "data spills" in the form of the inadvertent public disclosure of personal information.

Both PIPEDA and PIPA impose obligations to preserve the security and integrity of personal information. PIPEDA requires organizations to implement security safeguards "appropriate to the sensitivity of the information". Better safeguards are required for more sensitive information. PIPEDA goes on to provide that the safeguards should include: "(a) physical measures, for example, locked filing cabinets and restricted access to offices; (b) organizational measures, for example, security clearances and limiting access on a 'need-to know' basis; and (c) technological measures, for example, the use of passwords and encryption".

PIPA contains a more general requirement that an organization "protect personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks".

Loss of personal information by an organization requires a quick and informed response. Privacy commissioners have created detailed guidelines for assessing the severity of a breach and determining what steps should be taken, and there have been consultations recently regarding entrenching similar rules in the statutes themselves. Depending on the nature of the information, an organization should consider implementing a breach response procedure that engages appropriate levels of management, IT personnel and legal counsel, immediately and as required. In addition, the guidelines require notification of the commissioners and the affected individuals in appropriate circumstances.

Consequences of Non-Compliance

The federal privacy commissioner is responsible for administering PIPEDA (but cannot herself make legally binding orders). Under PIPEDA, an individual may apply to the Federal Court for orders compelling an organization to comply with its privacy obligations and for an award of damages "including damages for any humiliation that the complainant may have suffered". Other compliance orders are also available.

The enforcement regime under PIPA is different. The Information and Privacy Commissioner for British Columbia has been assigned responsibility for administering and enforcing PIPA, including the conduct of inquiries and the making of orders. It is an offence to violate an order of the Commissioner. The penalties include fines of up to $10,000 for individuals and $100,000 for corporations. If an organization fails to comply with a final order of the Commissioner, an individual affected by the Commissioner's

order can sue the organization for damages for "actual harm that the individual has suffered as a result of the breach by the organization" of its PIPA obligations. A similar right to sue exists if an organization has been convicted of an offence under PIPA and there is no further right of appeal.

Compliance Check-Up

This is a list of some of the issues organizations must address when assessing their level of privacy compliance. How does your organization rate?

Internal Administrative Issues

1. Designate a privacy officer.

    (a) Grant them the appropriate authority, resources and support.

    (b) Publicize their designation and contact details internally and externally.

    (c) Ensure they are adequately trained to:

        (i) be responsible for all personal information in custody or control of the organization, including information given to third parties for processing;

        (ii) implement procedures to protect personal information, receive and respond to complaints, access requests, challenges to accuracy and inquiries conducted by the privacy commissioners (within the stipulated time periods);

        (iii) supervise staff training and communicate to staff information about the policies and procedures, and develop explanatory literature; and

        (iv) investigate all complaints and rectify non-compliant practices.

2. If appropriate, establish a privacy working group under the leadership of the privacy officer to analyze and document the organization's current privacy practices. Membership should include:

    (a) all relevant departments and divisions (personnel, customer service,

public relations, security, legal, IT, records management, accounting/audit); and

(b) outside advisors, if necessary.

3. Develop and implement appropriate policies:

(a) privacy policy;

(b) document retention policy;

(c) communication systems policy; and

(d) security policy.

4. Develop and implement information security standards:

(a) physical measures;

(b) technological tools;

(c) organizational controls.

(d) mobile devices require particular attention. Not only is it necessary to establish specific technical security protocols dealing with such devices, but is it essential to ensure that employees properly safeguard these devices when carrying them outside the office.

5. Ensure that IT safeguards are reviewed at regular intervals to ensure that they are reasonable, current and up to date.

6. Consider the privacy implications of transferring personal information to associated legal entities, including subsidiaries and affiliates.

General Business Issues and Practices

1. Identify the specific purposes for which personal information is collected, used and disclosed and ask whether those purposes are reasonable and appropriate.

2. Ensure appropriate consent is obtained.

3. Review and ensure validity of standard documents and practices:

    (a) client agreements, including appropriate provisions confirming consent to the collection, use and disclosure of personal information;

    (b) "upstream" and "downstream" information-sharing contracts;
    (c) other commercial agreements, including outsourcing agreements;

    (d) advertising agreements and practices, including contests;

    (e) the use of social networking tools, which have also recently caught the interest of privacy commissioners.

4. Consider standard contractual terms in light of privacy concerns:

    (a) representations and warranties regarding the lawful collection, use and disclosure of information being received by the organization, or disclosed by the organization;

    (b) indemnification provisions for third parties' breaches of personal information laws;

    (c) choice of law; and

    (d) exclusive choice of jurisdiction.

5. Ensure appropriate insurance coverage.

6. Monitor and control personal information in due diligence activities, and enter into appropriate non-disclosure agreements. Ensure that closing and post-closing procedures comply with applicable privacy legislation.

7. Review Internet presence.

    (a) ensure the website contains a statement of the organization's privacy policy, including a convenient method of contacting the privacy officer;

(b) consider how and why personal information is collected through the website; and

(c) ensure that appropriate consents are obtained from website users.

8. Develop policies regarding employee and customer surveillance, and ensure that they are consistent with the evolving guidance provided by Canadian privacy commissioners.

Labour and Employment Issues

1. Review and ensure validity of standard documents:

(a) employment agreements;

(b) collective agreements;

(c) independent contractor agreements; and

(d) employee and workplace manuals.

2. Review and consider reasonableness of existing information collection, use and disclosure practices, and ensure appropriate notices are provided in advance:

(a) interview questions;

(b) application forms;

(c) aptitude testing;

(d) background checks, criminal record checks, personal references, educational records;

(e) medical and psychological examinations;

(f) video and other electronic surveillance;

(g) physical searches;

(h) workplace inspections;

(i) email, including back-up archives of user-deleted messages;

(j) monitoring key strokes, photocopier use, browser use, Internet downloads;

(k) monitoring login/logout;

(l) security access card-tracking;

(m) monitoring voicemail or telephone use; and

(n) disclosure to outside service-providers and partners (including charities, marketing organizations, etc.).

Conclusion

Private sector personal information protection legislation has been in place for several years. However, the standards continue to evolve and Canadian privacy commissioners continue to offer guidance targeted to specific issues. It is essential to be attuned to the practical implications of these statutes, take an active role in ensuring your organization's compliance with them, and ensure that you keep pace with current expectations.

Robert J. Deane
(604) 640-4250
rdeane@blgcanada.com

BE SUCCESSFUL IN SUCCESSION: Handing Over the Reins of a Family Business Takes Preparation

Family businesses, and other closely held private companies, make up a significant proportion of the enterprises driving the world's economies. Companies owned and operated by families are everywhere we look, from small corner groceries to global business empires.

"With a commitment to...customized planning, the likelihood of leaving a thriving legacy for future generations...is dramatically improved."

But these types of business face a unique challenge which, if not addressed, can (and often does) lead to the downfall of a lifetime of work. How can the founder of a family business ensure successful succession, competent management and prosperity, and at the same time maintain family harmony?

The answer can be found, in part, through communicating and building consensus among the key stakeholders in the business. Remember, the family business affects not only those family members who are actively involved, but also those who are non-participating owners and potential future owners or participants.

It is essential for the founder to do some preliminary soul searching before opening these lines of communication and beginning a meaningful family discussion. Here are some general guidelines to improve the chances of successfully transitioning your family business to the next generation.

The key stakeholders need to conduct a succession readiness check-up. This is the first step in developing your family business succession action plan. You have to start by asking yourself some tough questions. Some of the important things to consider are when you want to retire (and whether you would be financially secure if you did so), how much the business is worth, whether you have a potential successor, whether you have developed an equalization strategy for children active in the business and not, and whether you have a shareholders' agreement. Additional questions to ask are set out in the checklist at the end of this article.

In planning for succession, it is essential to be aware of the objectives of all key stakeholders. Each of them should conduct a personal assessment of their short- and long-term objectives, professional and personal goals, and management and ownership interests. A succession plan will not likely succeed if it is developed in a vacuum.

The success of this planning is dependent on the members of the family being able to communicate, discuss and collaborate on their issues and objectives. Consider appointing a professional advisor or outsider to customize, facilitate and moderate this process. A set of operating principles or code of conduct may also be useful, to set the ground rules.

With the individual assessments complete and a communication process in place, the next step is to address the critical business issues. Identify and prioritize key issues facing the family business. Ask the question: "How important is discussing and resolving this issue to the survival of our business?"

Part of the strategic planning for any business (whether or not succession is on the horizon) is to have vision and mission statements. Mark the common family goals for the business by developing agreed statements. These statements will form the guiding principles for the other succession planning work to be done.

Ownership and management responsibilities do not necessarily go hand in hand. Develop a plan outlining how to transfer them. Separate them if necessary. The options may include family succession, management buy-out or sale to an outsider.

If a family successor has been selected, develop a plan to groom that person for the position. Effectively training and cultivating a successor requires work. Have timelines within which set milestones must be met.

The best-laid succession plans can unravel in the event of the sudden death or disability of an owner or key employee. A contingency plan is vital here.

Once you have the fundamentals of a succession plan in place, you need to take stock of the strategic plan for the business. The plan should align with stakeholder values, the vision and mission statements, and the ownership and management succession plans.

Family governance is the final piece of the succession puzzle. Consider establishing a family charter, advisory board or committee, code of conduct, compensation committee, philanthropy committee, wealth education and responsibility plans, as appropriate.

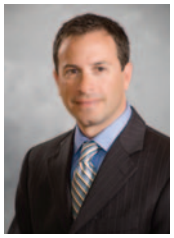
Although there are many common issues facing families and their businesses when planning for succession, each family is unique. With a commitment to

engage in customized planning, the likelihood of leaving a thriving legacy for future generations, rather than a family feud, is dramatically improved. Without it, you are taking a chance on your life's work.

SUCCESSION READINESS CHECKLIST

Transition and succession planning is a process that often gets deferred until it is too late. Operating the business understandably takes precedence, but think about the following questions and the impact your answers will have on your family, your heirs, your clients, your management team and the business itself.

1. Do you know when you want to retire? When?
2. Do you want the next generation to be involved in the business?
3. Have you identified a possible successor for your business and your position? Who?
4. Is your chosen successor willing, able and prepared?
5. Have you developed a distribution or equalization strategy for children active in the business and not?
6. Is the continuity of the business important to you?
7. Do you have an exit strategy from the business?
8. Do you have a shareholders agreement?
9. Is there a buy-sell provision in the shareholders agreement, and is it funded?
10. Are you and your family financially secure, and does this security rely on the continued success of the business?
11. Do you know how much your company is worth? How much?
12. Could your business continue without you if you became ill, disabled or died today?



Noel Z. Golden
(604) 640-4141
ngolden@blgcanada.com

Dispute Resolution is general information, not legal advice. We would be pleased to provide additional details and to discuss the possible effects of these matters in specific situations.

Vancouver Dispute Resolution Department Manager:

P. D. (Don) MacDonald
Direct Tel: (604) 640-4119
E-mail: pdmacdonald@blgcanada.com

Editor:

Stephen Antle
Direct Tel: (604) 640-4101
Email: santle@blgcanada.com

To obtain additional copies of Dispute Resolution, to change your mailing address or to request articles on specific issues, please contact the editor.

Borden Ladner Gervais LLP
Lawyers · Patent & Trade-mark Agents

Calgary
1000 Canterra Tower
400 Third Avenue S.W.
Calgary, Alberta, Canada T2P 4H2
tel: (403) 232-9500 fax: (403) 266-1395

Montréal
1000 de La Gauchetière Street West
Suite 900, Montréal, Québec, Canada H3B 5H4
tel: (514) 879-1212 fax: (514) 954-1905

Ottawa
World Exchange Plaza
100 Queen St., Suite 1100
Ottawa, Ontario, Canada K1P 1J9
tel: (613) 237-5160 1-800-661-4237
legal fax: (613) 230-8842 IP fax: (613) 787-3558

Toronto
Scotia Plaza, 40 King Street West
Toronto, Ontario, Canada M5H 3Y4
tel: (416) 367-6000 fax: (416) 367-6749

Vancouver
1200 Waterfront Centre
200 Burrard Street, P.O. Box 48600
Vancouver, British Columbia, Canada V7X 1T2
tel: (604) 687-5744 fax: (604) 687-1415

Waterloo Region
Waterloo City Centre
100 Regina Street South, Suite 220
Waterloo, Ontario, Canada N2J 4P9
tel: 519 579-5600 fax: 519 579-2725
IP fax: 519 741-9149

www.blgcanada.com