CIBC

CIBC PRIVATE WEALTH

Preserving family wealth

Fulfill the promise of your ambitions

What's your vision for success? We've learned that success often means achieving a sense of satisfaction and joy about the use of your wealth for yourself, your family and causes you hold dear.

It also means having peace of mind about your financial affairs, trusting that your wealth advisor is managing the complexities of wealth ownership. Additionally, for some, it means that plans are in place to realize your vision for broader community impact and a lasting family legacy.

CIBC Private Wealth can be your partner for all of your investment, wealth planning and private banking needs. Our professionals are dedicated to delivering exceptional performance and service with an unwavering focus on you and your best interests.

We hope the information on the following pages will inspire you to articulate your own vision for your wealth. It would be our privilege to help you bring your ambitions to life.

Contents

CIBC

CIBC PRIVATE WEALTH

Preserving family wealth

Introduction

Preserving family wealth

Whether you created your wealth or inherited it, preserving wealth for yourself and for future generations requires sound investment management and a thoughtful strategy to address the risks you may face, not only to your assets but also to your reputation, your online security, your household and your family's personal safety. All of these have value, and all are part of your overall wealth. This booklet presents tactics for addressing all the risks to family wealth.

Asset protection

Asset protection follows the continuum of life's events, reflecting the changes that individuals, families, careers, businesses and wealth undergo. Sometimes wealth "events" occur suddenly (an earlier-than-expected inheritance, for example), and some wealth accumulates over time (such as a business that grows and prospers). Both can result in significant wealth and potentially significant exposure to risk. Within the wealth spectrum, a simple way of thinking about asset protection strategies is from lower-risk and simpler tactics to higher-risk and more complex and sophisticated tactics. This approach will cover everything from how assets are owned and titled, to how they're insured and protected, to how they can be held for efficient asset management. Not every tactic will be right for every family, but each deserves careful consideration and a discussion with your advisor about how to use them effectively to protect your family's wealth.

"An ideal time to address the ways you can protect your assets is when you are creating or revising an estate plan," says Amanda Regnier, senior wealth strategist at CIBC Private Wealth. "This is the time when most people realize how important it is to take the steps to ensure they're doing the right thing for their families. Another good time is when major life events occur, such as the birth of children or grandchildren or the founding of a business."

Here are some of the important asset protection steps you can take.

Asset ownership

Proper titling of assets is a basic element of asset protection and one of the simplest ways to minimize risk. If you practice in a profession characterized by frequent litigation—a physician or a contractor, for example—you can consider putting the bulk of your assets in your spouse's name or holding them as "tenants by the entirety," which can provide protection from a creditor of one spouse. An asset held this way often cannot be claimed by the creditor of one spouse since it is effectively owned by both. Only the couple's joint creditors can access assets held as tenants by the entirety. There are two important exceptions to the rules on tenancy by the entirety. No matter how the property is titled, it can be seized to pay federal taxes. In addition, in community property states, creditors generally can reach all the assets of a married couple to satisfy the debts of either spouse, regardless of how the assets are titled. You should also ask your advisor about your state's homestead laws, which can protect your personal residence.

Insurance

Various types of insurance also serve as basic asset protection measures. Life insurance is one insurance option because the death benefit generally is exempt from both taxes and from the claims of creditors. A life insurance policy can also fund a buy-sell agreement in the event of the death of a business owner or partner. While most people are familiar with the need for life insurance, even the wealthy sometimes overlook the need for adequate property and liability insurance.

A significant liability umbrella policy can help protect you from many types of risk: a lawsuit from a disgruntled employee if you own a business; legal negligence, if your lake house neighbors borrow your jet skis and have an accident; host

liability, if an underage drinker leaves your home and has an accident. "You may know that you need to insure for the replacement cost for your home, but you may not think enough about what you could be sued for," says Regnier. "Lawsuits against wealthy people pose a very significant risk. If you employ household help, you should consider an employment practices liability insurance (EPLI) policy—often available as an add-on to an umbrella policy. And if you serve on the board of a private company or nonprofit group, you should consider directors and officers (D&O) liability insurance."

Protection through trusts

Trusts are an excellent way to keep money in the family, especially as children grow up and embark on lives—and enter relationships—of their own. Parents and grandparents often use trusts for a specified period; for example, until beneficiaries reach a certain age or maturity, or are in stable marriages. You can specify ages at which the trust should make payouts of income or principal, or leave the choice entirely up to the discretion of trustees. Another option is to take a hybrid approach: The trust instrument calls for payouts at specific ages, but the trustee can postpone distributions if the beneficiary is a spendthrift or has creditor problems, for example. Trusts offer a lot of flexibility and should be created with that overriding goal in mind. You can give trustees the power to move the situs, or location, of the trust in response to new state laws that achieve better creditor protection. In some states, trustees can amend the trust under certain circumstances or even decant the trust—pour funds from one trust to another—which may help them attain continued creditor protection.

While it's human nature for people to think of divorce as a "low-risk" potential event in their families, it does happen. An irrevocable trust can be a good choice for assets vulnerable to being lost in a divorce, especially if there's family sentiment surrounding the assets. A trust can usually withstand legal challenges to a prenuptial agreement. (Please see "Loving Union, Legal Contract" later in this booklet.)

A special type of trust known as a **self-settled asset protection trust** is another option for protection through trusts and is available through CIBC Delaware Trust Company. Delaware's laws (and those of some other states) provide that a grantor using this type of trust may protect the assets in the trust from the claims of his or her own creditors. A self-settled asset protection trust may guard against risks to which certain people are exposed: professionals who may be sued for malpractice, corporate officers and directors who may be named in shareholder-related litigation and investigations, and business owners who would like to shield personal assets from future creditor claims and business reverses. Keep in mind that certain "super creditors"—the Internal Revenue Service (IRS), the Securities and Exchange Commission and minor children seeking child support—can still make a claim on assets held in an asset protection trust.

Family entities

Family limited partnerships (FLPs) and **limited liability companies (LLCs)** are entities created by a group of individuals, generally for efficient management of the underlying assets. These entities can also provide asset protection, particularly if the client is not the sole member, partner or manager of the entity. A chief attraction of FLPs and LLCs is that creditors generally cannot satisfy a claim with assets in the entity or force a liquidation. The creditor must obtain a "charging order" that attaches distributions made from the entity and generally only has a right to the debtor's distributions up to the amount of the debt. The manager or general partner of the entity controls the distributions.

Assets can be insulated with two layers if an LLC (or FLP) interest is transferred to a trust by a sale or gift. The first layer is the protection that the LLC provides with respect to the underlying assets. The trust does not own the underlying assets; rather, it owns an interest in an LLC. Further, the trust is not the manager of the LLC. Neither the trust nor a creditor can force a distribution of the asset from the LLC. The second layer is provided by the trust, which gives the trustee control over distributions and prevents the beneficiaries and their creditors from making claims on the assets. When considering this, or any other, type of asset protection vehicle, be sure to discuss the provisions of the relevant documents with your legal advisor.

Special protection for retirement accounts

It's important to remember that assets in retirement plans covered by the Employee Retirement Income Security Act (ERISA), such as those in an individual's 401(k), enjoy full protection under these federal laws. "Retirement assets are never subject to a creditor's claim or a lawsuit's judgment," says Regnier, "with one exception: An individual retirement account (IRA) isn't covered by ERISA, even though it's a special type of retirement account with special tax status under federal laws. While bankruptcy laws protect an individual's IRAs, they may be vulnerable to creditors' claims depending on your state's laws."

CIBC

CIBC PRIVATE WEALTH

Preserving family wealth

Protecting who you are: Reputation risk

Protecting who you are

Here today, gone tomorrow. That could describe your reputation. Indeed, Warren Buffett once said, "A reputation can be built over decades, but it can also be lost in just five minutes."

Sometimes, the worst reputation implosions by businesses are self-inflicted wounds. But given the online world in which we live today, not all damage to a business's or individual's reputation is self-inflicted. Consider the story of Lisa-Michelle Kucharz, a professor and anti-cyberbullying advocate. For two years, a total stranger—who was interested in a man Ms. Kucharz had previously had a relationship with—used the internet to accuse her of being a pedophile, having an affair, engaging in sex for money, and having mental health challenges. The defamer also contacted Ms. Kucharz's employer via Facebook, wrote blogs, and shared hundreds of posts on social media. Not only did it hurt her emotionally and professionally, but it also cost her tens of thousands of dollars in fees for private investigators, cyber investigators and attorneys.[1]

Some of the negative content is still available in Ms. Kucharz's Google search results. Think of it this way: You are who Google says you are. A search could produce a public record of a minor regulatory fine (making you a "lawbreaker"), or a court case in which you were sued for late child support many years ago (meaning you obviously "don't care about your family").

What is reputation risk, really?

Reputation is defined as the estimation in which a person or thing is held, especially by the community or the public generally. Reputation risk, common in the business world, is a type of risk related to trustworthiness, standing and esteem, and can be applied to individuals as well. Most importantly, it is a "retained risk," says Ray Monteith, senior vice president and organizational resilience practice leader with HUB International's risk services division—you can't transfer this risk to anybody else.

"Numerous insurance options are available for the transfer of other types of risk," says Monteith. "If you suffer a loss because your home or business burns, or your house is burglarized and valuable art or jewelry is stolen, insurance provides you remedy and recovery. Reputation risk is a risk that you as an individual, or a business owner, retain and must manage yourself. And you can't always easily undo the damage. Let's say you feel you've been publicly libeled, and you decide to sue the person you think is responsible. The damage is still out there, and the libel suit may just bring more attention to it."

Filing a lawsuit can trigger what's called "the Streisand effect," a term coined by a reporter in 2005 after Barbra Streisand went to court to make a photographer remove a photo of her home from his website. Before Streisand filed the lawsuit, the photo had only been downloaded a handful of times. As a result of the publicity surrounding the case, the image gained nearly a half million views.[1]

Losing control of the narrative

When your reputation is damaged, you've lost control of your own narrative. And when others define who you are, they can paint whatever picture they want. Reputation risk is an extremely important strategic focus within organizations and for senior business leaders. The same should be true for a prominent affluent individual or family. But can you put a true "value" on your personal reputation?

[1] "How to deal with online defamation," reputationdefender.com, 06.17.2019.

"Your reputation is exactly as valuable as the purpose for which you want to use it," says Brian Schnese, senior risk consultant in the organizational resilience practice with HUB International's risk services division. "If you don't intend to use your reputation to further your personal or business goals, then it may not have a lot of value. So the first exercise you should undertake is explicitly defining your purpose in managing your reputation. Today, we hear a lot about 'personal brand,' a term we weren't using 10 years ago. If your identity is your brand, and vice versa, protecting your personal brand is extremely important. Think, for example, in terms of controlling your brand to enhance your family foundation's philanthropic agenda and to create and preserve the family legacy."

There are numerous threat vectors today, but few are as pernicious as social media. In many cases, says Schnese, it's enough for a person to simply make an assertion about another for a reputation to be damaged. "Unfortunately, people seeing the assertion tend to leap to judgment very quickly and often won't invest in fact-finding. Assertions or accusations tend to really 'stick.' The most important point to keep in mind is to have a discussion and a plan for how you will—or will not—respond if this happens."

Schnese offers a cautionary tale for the response to an accusation that can severely damage a reputation. The late Ravi Zacharias, a world-famous Christian apologist leader who established Ravi Zacharias International Ministries (RZIM), was accused of sexually abusing women and improperly using funds from RZIM to pay for their silence. RZIM's initial response was to deny the accusation flatly; RZIM even attempted to discredit the accusers, many of them vulnerable women in parts of Southeast Asia. As allegations continued to come out, even after his death in 2020, the organization was forced to revise its message, offering sympathy for the victims, and saying that RZIM was seeking the truth, taking investigative steps and committing to transparency.

"It isn't always the case that an accusation is false," says Schnese. "Sometimes the narrative is true and will eventually be substantiated. In that case, the initial response to dig in and deny can be as big a black eye as the accusation itself. Then you must back away from your initial denial. RZIM had to go through a multistage recovery—from their initial stance to the truth of the accusations. This is a textbook example of how not to respond."

More recently, the online brokerage Robinhood, whose brand is built around "power to the little people," badly mishandled its response to the GameStop trading frenzy, says Schnese. "It's a complex story, but they blocked customers from buying GameStop and even created 'sell' orders on behalf of some customers. While they later explained their actions as a compliance issue, the company's initial response was to explain nothing—and the public narrative became total outrage. Subsequently, they doubled down on their message about compliance, but the damage had been done."

Both Monteith and Schnese advise that a first consideration about your potential response is: Consider the source. Maybe you don't care if somebody posts a photo on Facebook of you walking down the beach looking very nonexecutive or sloppily dressed. But maybe you really care if somebody posts a doctored photo of your daughter engaging in unflattering behavior. This should be part of what you identify as all your "risk vectors"—a complete understanding of how you feel vulnerable. In some cases, altered photos are used to extort people. Schnese, a former FBI Special Agent, knows some of these cases all too well: Hackers stole compromising photos of actress Scarlett Johansson and used them in an extortion plot. "It isn't that you may be engaging in risky behaviors," says Schnese. "But in the hands of the wrong people, what you might consider something ordinary suddenly isn't. And it's a terrible invasion of privacy."

Today, "deepfakes" generated by artificial intelligence (AI)—the 21st century's answer to Photoshop—are becoming more common. Many deepfake videos are pornographic: The AI firm Deeptrace found 15,000 deepfake videos online in September 2019, and a staggering 96% were pornographic, with 99% of those mapping faces from female celebrities onto porn stars. AI can create convincing but entirely fictional photos from scratch, as well as profiles on LinkedIn and Twitter.[2]

[2] "What are deepfakes – and how can you spot them?" Theguardian.com, 01.13.2020.

On the internet forever: Is there a remedy?

A critical part of managing reputation risk is understanding an ugly truth, says Monteith: "What's on the internet is not only there forever, it's there to be harvested."

Even if you're not a high-profile business leader or a very wealthy family, your online presence could affect your ability to get a job. Almost every organization today explores the online profile of job candidates in depth. A casual Google searcher might stop at the top results on a person or company, but companies with reputations to protect, and whose employees reflect their reputation, go way down "below the fold."

Experts that specialize in reputation can be hired to flood search results with positive information, pushing the negative far down in results. But let's assume you have a business and you feel its reputation (and yours by extension) has been harmed. If you want to have negative information removed, you first have to consider several questions: Has your business been affected by the content? Has there been any actual harm to your business that you can prove? Have you lost customers or received inquiries that likely stemmed from the negative content? Depending on your answer, you may be able to convince the webhost/ISP/website to redact some or all of the content, particularly if it violates any of the site's terms or is particularly objectionable. Depending on the laws of your jurisdiction and the specific facts of your situation, there may also be potential claims that your counsel could threaten—and prosecute—against the individual, such as intentional interference with prospective business relations, tortious interference with contract, and so on.[3]

It's important to know the definition of "defamation" if you decide to act on information you believe has damaged your or your business's reputation: Defamation is a knowingly false statement of fact that is damaging and can be either spoken (slander) or written (libel). The newly coined term "Twibel" includes any libelous statement that appears on the internet in any forum, including X, formerly known as Twitter.

"Your first option to consider should be simply reaching out to the person or group that you believe has damaged you," says Schnese. Unfortunately, if it's online, you often can't determine that. Remember that some social media platforms (X and Instagram, specifically) don't require real names—the anonymous blogger posting negative content about you or your business could be known as @fishingman or @concernedcitizen. "If you can identify the offender, you probably won't get a reply," says Schnese. "In that case, consider the step of engaging an internet data removal service that can get at the ultimate source."

In today's world, an online presence can also be hacked and used for garden-variety identity theft, but also for new opportunities: criminals filing unemployment claims in your name or claiming pandemic relief funding. (Please see "A safer online life" for more on online protection.) Data breaches keep coming, and they keep getting bigger. "We shouldn't like it or get comfortable with it, but think of it like putting a bike helmet on your child. Make sure you have all the tools in place to keep yourself safe online," says Monteith.

Wealthy families, such as clients of CIBC Private Wealth, often have annual family meetings. If you do, consider including a frank discussion among family members about recent activity that might show up online. Do some intelligence-gathering to determine any new risk exposures. It can be a very proactive approach and can serve as your own incident or crisis response plan—just in case.

Other tactics you and your family can take include:

- Embrace the idea that, for better or worse, as a prominent or wealthy person, you're probably on somebody's radar.
- Clearly define what you want your desired brand positioning to be. Discuss with your family how reputation can affect wealth preservation and business or foundation goals.
- Consider hiring an outside consultant to do a comprehensive online audit.

[3] "An Attorney's Advice for Removing Negative, Defamatory and Infringing Material from the Internet," by Christine Rafin, Esq., reputation-communications.com, 12.30.2020.

- Create a Google alert for your name (and for your spouse and children), company, tagline and products.
- Purchase the domain name for your name and the various iterations of it—e.g., Elizabethsmith, Elizabeth-smith, Elizabeth_smith—and buy the domain name for as many extensions as you can: .com, .net, .info, .biz. Remember that anybody can purchase a domain name that's not already taken. Somebody with a grudge or an ax to grind could easily create a negative website with your name as the domain name. And through good wording for maximum search engine optimization, the bogus site could come up first in Google search results. There is no online "accuracy police." Keep in mind that Google is in business to give searchers what it thinks is relevant, not necessarily what is true.
- If you have a family foundation, be aware that foundations have numerous reporting requirements that can reveal personal information about family members. These sites get heavy traffic, which means they show up high in search engine listings. Families should be very thoughtful about how their chosen foundation's reporting requirements could impact privacy.

"We work with large organizations all the time to change their culture and thinking about risk," says Monteith. "Individuals or families can adopt the same strategy. The more time and effort you spend upfront on preparedness, the more rapid your recovery can be. Think of your response plan to negative information that could damage your reputation just like you would a fire and an escape plan in your home. Know the risks that can put you in this situation, but perhaps most importantly, know your way out."

What is defamation?

Defamation is the act of communicating false statements about a person that injure the reputation of that person. According to Merriam-Webster, "Harming someone's reputation in speech with falsehoods is known as slander, and doing the same thing in writing is known as libel (which sometimes includes speech as well). Any ordinary citizen who can claim to have suffered harm as a result of such defamation may sue. So why aren't politicians suing all the time? Because an exception is made for 'public persons' (a category that includes most other celebrities as well), who must also prove that any such statement was made with 'reckless disregard for the truth.' And although, even by that standard, public persons are defamed all the time, most of them have decided that it's better to just grin and bear it."

According to Law.com's Legal Dictionary, damages for slander may be limited to actual (special) damages, unless there is malice. Some statements—such as an accusation of having committed a crime, having a feared disease or being unable to perform one's occupation—are called libel per se or slander per se, and can more easily lead to large money awards in court and even punitive damage recovery by the person harmed. Most states provide for a demand for a printed retraction of defamation and only allow a lawsuit if there is no such admission of error.

CIBC

CIBC PRIVATE WEALTH

Preserving family wealth

Protecting what you have built: Household, liability and online risk

Protecting what you have built

Safeguarding family wealth requires recognizing, acknowledging and preventing exposure to risks—and risks come in all shapes and forms, including people, computers or legal actions. All have the potential to damage your financial security and your family's wealth. And, in large part, all are based on issues of trust.

Affluent families can be very guarded about whom to trust, while at the same time having a feeling of invincibility, according to Teresa Leigh, founder and CEO of Teresa Leigh Home and Family Office. "On the one hand, a family of significant wealth feels 'shielded' by professional advisors such as lawyers," says Leigh. "On the other hand, there is the attitude of, 'If I can build and run a successful business, how can my housekeeper harm me?'"

Leigh says that the most important issues for the affluent are preserving time and financial resources and shortening their "learning curve." "Affluent families are very busy and need to delegate many of the details of their lives to others," she says. "But they also need guidance and assurance on how to do that in a responsible and thorough way. They really want the best expertise they can find, as fast as they can find it."

Household management: You *are* an employer

Consider the following scenario: A family requires staff for their multiple households—house managers, an executive personal assistant, a nanny and housekeepers. The hiring process involves finding a good pool of candidates, interviewing them, administering personality and skill testing to selected candidates, and developing a plan to retain staff. Once hired, the family's responsibilities include staff management, payroll, security procedures and compliance with employment law. Another scenario might involve a multi-generation family's beloved head housekeeper wanting to leave her job after several years of dedicated service and a strong bond with the family. The family is at a loss as to why she wants to leave, so they hire an outside expert who discovers that another member of the staff made unwanted advances toward the housekeeper's underage daughter. The family is briefed on employment best practices and offered an action plan, which results in the family retaining their housekeeper and saving thousands of dollars in turnover costs and avoiding a potential lawsuit.

Teresa Leigh's firm specializes in management of the affluent household, and she operates in a world where these scenarios happen every day. Leigh stresses that whether it is an estate manager, nanny, elder caregiver, or another household role, if your family employs household staff, you are an employer with legal and ethical obligations. First, keep in mind that although it is your home, it is your employees' workplace.

"Although your staff may come to feel like members of your family, you can never forget that you have a professional relationship with them," says Leigh. "Being an employer has a set of requirements that go far beyond creating harmony and chemistry, not the least of which is understanding employment law. Knowledge of your requirements and of best practices for hiring—a good job description is a must—will help save time and preserve precious resources. For example, if you misclassify household employees as subcontractors, that's more than just getting the IRS ruling wrong—it could result in a lawsuit with monetary damages. In addition, you now have the issue of employees you want to keep feeling betrayed. Your relationship with them has to be repaired."

Leigh notes that increased restrictions in US immigration laws and work visas after 9/11 created a greater demand for domestic staff who can work legally in the US. As the pool of good candidates tightened, the number of people who can pass a stringent background and criminal history investigation diminished exponentially. A federal requirement enacted in 1986 requires employers to complete an Employment Eligibility Verification Form (a Form I-9), which verifies the identification and work status of a potential employee. An I-9 is not required for what the law says are "casual domestic services" that are provided sporadically, irregularly or intermittently, nor is it required for legitimate "subcontractors." (Changes were made to the form in January 2020; please visit uscis.gov for the latest information on the form and on definitions of subcontractors.)

If you try the DIY approach to screening household staff candidates using online search companies, you'll have to deal with what Leigh calls "a broken system." The 50 states and three US territories have a total of 3,242 different counties, parishes, census areas and independent cities, each of which is responsible for entering its criminal arrest, conviction and civil complaint information independently—and these jurisdictions are not connected by a centralized US criminal database system that can be accessed by private online companies.[4] "These computer systems may be outdated, unsecure or become hacked," says Leigh. "They may also contain multiple human reporting errors, such as incorrect names, dates and Social Security numbers. Criminal charges or civil complaints may have been dismissed, amended, sealed or lost. In addition, jurisdictions do not always allow the sale of their data to online database companies."

Time is money

On average, Leigh's firm interviews a minimum of 50 candidates before one will pass to the second stage of the interview and vetting process. "That may sound overblown to some people," says Leigh, "but let's assume we are talking about a nanny—do you really want to take a chance with your children?"

Knowledge and best practices can help save money. According to Leigh, the cost of household staff turnover is, at a minimum, seven times the employee's annual salary, based on loss of productivity, employer's time, recruiting fees and risk exposure. As for your time as an affluent family? Leigh says that when individuals try to hire staff on their own, without guidance, the time spent can be between 200 and 300 hours.

"Potential clients will often look astounded when we mention this number to them, saying that there's no way it would take them 200 hours to hire a nanny," says Leigh. "Our point about expert help is: Why would you spend any of your time searching, screening, vetting, interviewing and hiring the best nanny for your children?"

Leigh estimates that only about 5% of affluent families take advantage of professional staff hiring and management services. She also notes that families are often advised on staffing by lawyers, who have a different viewpoint and framework regarding risk. "We approach it from the philosophy of lowering a family's stress, shortening their learning curve and getting everybody on the right track," says Leigh. That right track includes new policies on COVID-19—"because it looks like COVID-19 could be with us for quite a while. We now are addressing COVID-19 in our rules and regulations manuals for clients, including requiring household employee testing and other guidelines."

Exposure to risk

If you fail to properly vet, hire and manage your employees, any one of these things could become an ugly reality:

- A lawsuit from a disgruntled employee
- A claim of a hostile, toxic or unsafe work environment
- A wage and hour complaint, including overtime and misclassification
- An Equal Employment Opportunity Commission (EEOC) claim of discrimination or sexual harassment
- Unauthorized access to your home and to personal and financial accounts

If you employ household staff, it's easy to overlook how far your circle of family, close friends and acquaintances can expand. While most people like to think they take common-sense safeguards to protect their privacy, if your family has multiple residences, you may fail to consider the number of contacts made with your household by outside vendors. According to Leigh, during the lifecycle of just one large home, an average of 40 subcontractor and vendor companies will work for a homeowner. Add in all the auxiliary and personal service companies (hairdresser, holiday decorator, car detailer, yoga teacher and the family dog groomer, for example) who make house calls, and the number will easily exceed

[4] https://teresaleigh.com/wp-content/uploads/2024/09/2024-Teresa-Leigh-Outsourcing-Trust.pdf

175. Ask yourself: Are you familiar with the vendors and contractors that enter your home? Does each business entity have a certificate of insurance should something go wrong? And are you carefully reviewing their invoices for errors or over charges?

The risk potential with vendors and contractors can be uncomfortably high, says Leigh. "It's not that household staff or vendors are inherently manipulative or seeking to harm you, but they have a circle of family and friends, too, and may be under pressure. Your financial risk could begin when an extended family member of one of your household employees starts having financial difficulty, resulting in your employee trying to 'help' that family member—just this one time. This situation could expose you or your family to a fraudulent service bill, identity theft, a theft of possessions or a violent crime."

A thorough understanding of the best practices for employing household staff can result in household harmony, well-integrated employees and a significantly lower exposure to financial risk by avoiding the scenarios that can create it. Safeguards in hiring and managing household staff are not about assuming the worst about people, says Leigh. "They're about safeguarding your time, money and, most importantly, your family members."

Liability exposure: Are you a lawsuit waiting to happen?

According to some experts, the risk environment today is, in some ways, no different than it always has been: Affluent families or those with a high-profile lifestyle can feel like they have targets on their backs. To those with unscrupulous motives, the goal of the target is money. But even a lawsuit for what appears, on the surface, to be valid reasons—you were negligent, although unintentionally so, by kindly letting your neighbor's teenagers use your jet skis—can have disastrous financial results.

According to insurance giant Chubb, wealthy individuals increasingly worry that their wealth alone makes them a prime target for a high-stakes liability lawsuit. But many wealthy families remain poorly prepared for such lawsuits, in spite of their concern. They fail to appreciate the different aspects of their lifestyle that can lead to a lawsuit. They underestimate the cost of the potential damages, and they misunderstand the affordability of effective protection. As a result, wealthy families often lack the proper types and amounts of liability insurance.[5]

"People are generally aware of the need to insure for replacement cost of their home, but they may not think enough about what they could be sued for," says John Pullara, vice president and team leader at EPIC Insurance Brokers. "If, for example, you kill or disable someone in an accident, juries may look at the value of the future wages of the victim. Let's say the victim is a 35-year-old hedge fund manager—his or her future earnings potential is most likely quite significant and could be factored into the financial award. Many affluent families are afraid of things such as needing medical care in a foreign country, but that's a risk that is easy to insure against. Liability lawsuits pose the greatest risk—you could incur far greater costs from a liability claim than any other type of claim."

Even if you have tried hard to "hire smart" and then to manage your household staff well, you can be at risk from a lawsuit filed by a former employee if your relationship later sours and you terminate the employee. The liability risks from household staff include wrongful termination, discrimination, harassment, untenable working conditions, and wage and hour disputes. Lawsuits are not the only risk—damage to public image can also carry financial consequences.

In general, homeowner's insurance does not cover these types of claims, because it is designed to cover bodily injury and property damage. An employment practices liability insurance (EPLI) policy can provide a broad range of coverage, including for wage and hour claims, harassment or discrimination, employment-related defamation and wrongful reference. Many top private client insurers can provide EPLI coverage easily via an endorsement on an umbrella policy with little or no additional underwriting, according to Pullara.

[5] "Uncertain Economy Making Wealthiest Americans More Fearful of Costly Liability Lawsuits, ACE Private Risk Services Survey Finds," news.chubb.com, 05.05.2012.

A second big risk that can damage financial security is that of directors and officers (D&O) liability. The need for D&O insurance is essential under two scenarios:

- If you serve on the board of directors for a private company or nonprofit group
- If you own a privately held company and have a board of directors

Lawsuits naming directors and officers are unfortunately quite common today, and serving on a board can put your personal assets at risk. According to Pullara, a disturbing trend in nonprofit D&O litigation is employment liability, attributable in part to more "informal" management styles often found in nonprofit settings. If you serve on the board of a nonprofit group—common among influential people who want to act in good faith for an organization or cause they care about—you are subject to personal liability.

Always ask to see the board's D&O policy, advises Pullara. Many individual umbrella policies cover property damage and bodily injury under the nonprofit D&O provisions, "but that is not typically the type of lawsuit brought against nonprofit board members," says Pullara. "It is usually a breach of fiduciary duty, discrimination, misappropriation of funds or wrongful termination. Most D&O policies afford defense costs, but they could be included in the policy limit; coverage is shared by all D&Os. You'll want to determine if the limit on the board's policy will be enough to protect you against a loss. If not, you can purchase additional levels of coverage, just for you, that will be in excess of the D&O policy limits, with the cost varying depending on what type of organization you are serving and the insurance company. These days, an insurer may view Greenpeace and the local school board in the same risk category."

If your family owns a privately held business, D&O insurance is a must. Because executives and managers of privately held businesses are often involved in many of the day-to-day operations and decisions, directors and officers are more likely to be named in lawsuits. In addition, the personal net worth of owners of privately held businesses is often tied to the fiscal health of the company. For private companies, the types of claims can include employment-related, fiduciary, regulatory and direct shareholder/investor suits. It bears repeating that directors and officers of privately held companies have the same fiduciary obligations to investors and limited partners as do directors and officers at publicly held companies. In the worst-case scenario, directors and officers may have to use their own assets to defend themselves in a lawsuit.

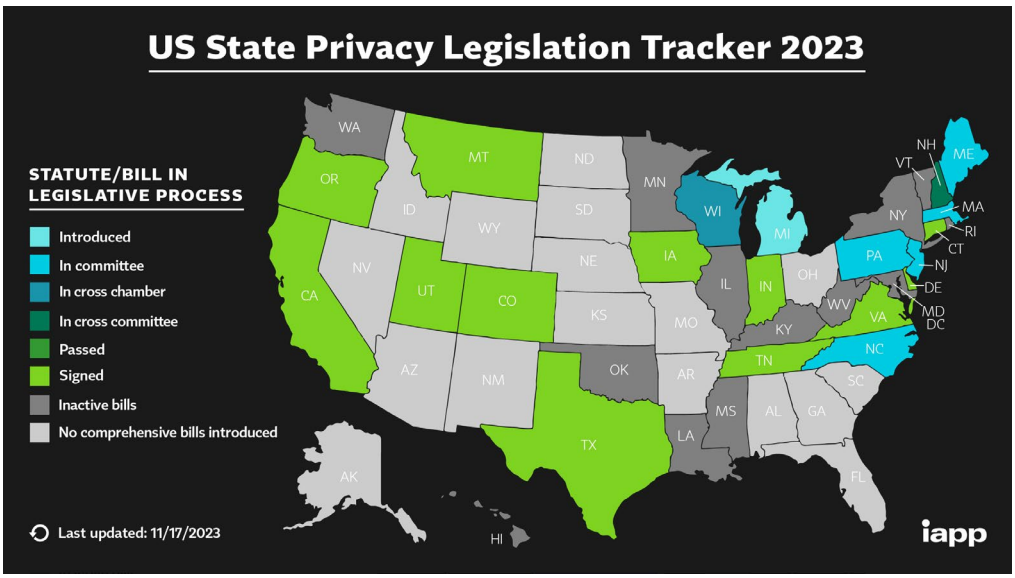
A safer online life

An increasingly digital world presents new challenges on a regular basis. Smartphones are ubiquitous, and many people rely on them for a wide spectrum of day-to-day activities, from banking to shopping to photo storage. When "everything online" is the norm, what is "privacy" anymore? What should our expectations about privacy be? What don't we know about what others know about us?

Looking at the big picture of privacy, it's helpful to start with the high-level issue of compliance and the laws that address privacy, says Craig Sherwood, a partner at Shambliss Security in Schaumburg, Illinois. In 2018, California enacted the California Consumer Privacy Act of 2018 (CCPA), which became law in 2020. It establishes new consumer privacy rights and expands liability for consumer data breaches. Unlike the General Data Protection Regulation (GDPR), which was enacted in the European Union, the CCPA gives consumers the right to prevent businesses from selling or disclosing their personal information.

"Consumers now have the right to learn categories of personal information that businesses collect, sell or disclose about them, and to whom information is sold or disclosed," says Sherwood. "If you're in California, you're now protected as a consumer, employee, patient, tenant, student, parent or child. This includes any information that relates to a particular consumer or household. The CCPA defines personal information as any information that relates to a particular consumer or household, as well as 'inferences' drawn from any of the information identified. For example, web browsing history and purchasing tendencies are regulated as personal information, even if no names are associated with them."

The CCPA is important because it's the first personal security act in the US to protect individuals and their data. It only covers California residents but, as Sherwood notes: "As goes California, so goes the rest of the country. It's very typical for California to be at the forefront of acts, rules and litigation around consumer protection. I wouldn't be surprised at all if multiple other states enact this type of legislation in the next two to three years. Currently, only a dozen states have any type of state privacy laws. (See chart below.) That is likely to change very soon as consumers become more aware of how their personal information is used, and as they become less tolerant of it."



Lessons from Jeff Bezos

If you think you've secured your mobile device, consider the Jeff Bezos incident. The smartphone of billionaire Bezos, executive chairman and founder of Amazon and its related businesses, was hacked in 2018 after receiving a message through WhatsApp that included a malicious file that infiltrated Bezos's phone. Large amounts of data were exfiltrated from Bezos's phone in a matter of hours. Among the sensitive and embarrassing outcomes were explicit photos of Bezos and a woman with whom he was having an affair.

The sensitive information on Bezos's phone was stored in the cloud. What lesson can we take from this? "To be blunt, the cloud is not 'safe,'" says Sherwood. "Remember that the cloud is simply an offsite repository for data. Service providers have simply outsourced their own server management to cloud providers because it's far less expensive than to maintain their own servers. You're in Florida doing business with a bank, and their servers are in a big building in South Dakota—that's the cloud."

Global cloud computing was a $371 billion industry in 2020 and is expected to grow to $832 billion by 2025.[6] Eighty-two percent of the workload in all enterprises now resides in the cloud, and every day the average person uses 36 cloud-based services. As of Q1 2023, Amazon Web Services has the largest cloud computing market share at 32%.[7] Data stored in the cloud is almost always stored in an encrypted form (which makes the files look like gibberish) that would need to be cracked to make the information available to an intruder. There's a short gap in time before information is encrypted—photos, for example, aren't encrypted from the moment they're taken.[8] Of concern is that, as of 2024, 80% of organizations do not have a dedicated cloud security team or lead, while the top cloud security concerns are data loss and leakage (69%), and data privacy/confidentiality (66%), followed by accidental exposure of credentials (44%).[9]

[6] "Cloud Computing Industry to Grow from $371.4 Billion in 2020 to $832.1 Billion by 2025, at a CAGR of 17.5%," globenewswire.com, 08.21.2020.
[7] "34 Heavenly Cloud Computing Statistics for 2024." techjury.net 01.03.2024
[8] "How Secure Is Your Data When It's Stored in the Cloud?" scientificamerican.com 01.25.2018
[9] "50 Cloud Security Stats You Should Know in 2024." expertinsights.com, 04.23.204

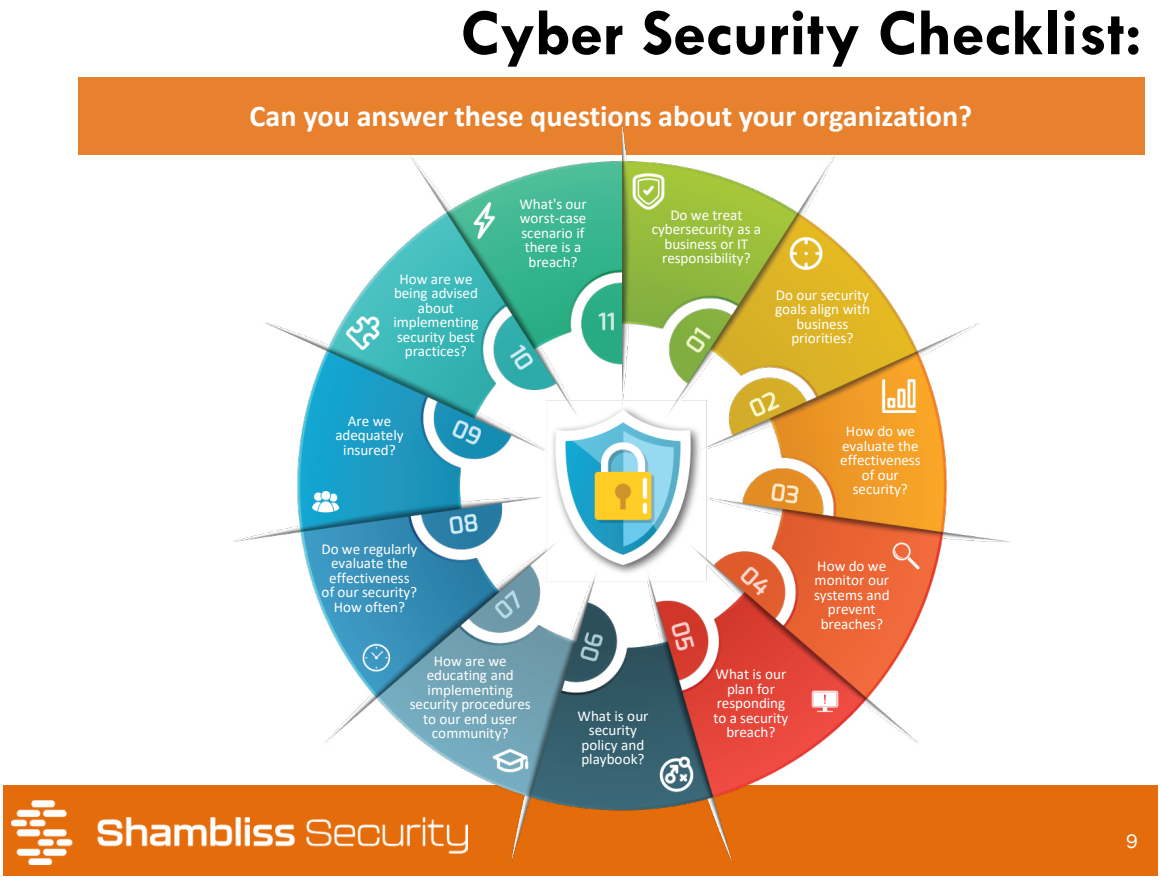
Of course, cloud storage for individuals has distinct advantages: It gives you the ability to synchronize and have access to your files on smartphones, tablets, laptops and workstations, and to collaborate with others. Be aware, however, that people with whom you share your files usually have access to modify and delete them, so consider carefully which files you share and with whom.

"Rather than be unsettled by the Jeff Bezos incident and your own use of the cloud, the best lesson is to understand more about online security and create your own plan for managing it," says Sherwood.

What's your privacy threshold?

In today's online world, your email address, phone number, contacts, lists of friends, locations you've been, photos, and social media sites you visit are all shared with third parties who can keep this information for themselves for as long as they like. "Your children or grandchildren have grown up in a world where this is so commonplace that they don't even quite absorb what they're giving up," says Sherwood. "The youngest generation using smartphones and social media typically doesn't understand what's behind the curtain that is manipulating sales and services. Ten years ago, people just took security for granted. Now, we know that there are not only malicious actors out there at every turn, but also that we're being bought and paid for by our lack of privacy. Remember that if it is free, it's you that is the product."

Marketing data is the consequence of giving up your privacy online. You may think that a company is not hurting you by suggesting a product they know you'll like from your past browsing habits. In fact, you may have been quite impressed years ago when you first realized that a company could customize information for you. (Today, it often takes the form of "Hello, Siri: show me new hiking boots.") You just have to ask how much you want any company to know about you—and to remember that once your information is sold, you can't buy it back.



Today, we're also living in the environment of the Internet of Things (IoT), a connected world in which your phone can control smart devices in your home. The convenience is attractive, but the risks are mostly underestimated by individuals. In October 2016, a hacker found a vulnerability in a specific model of security camera. Nearly 300,000 IoT video recorders started to attack multiple social network websites and brought down Twitter and other high-profile platforms for almost two hours. This attack is just an example of what can happen to IoT devices with poor security, and the problem isn't just in video cameras. Anything with an internet connection—from a refrigerator, smart locks, thermostats, lightbulbs, vehicles and even smart toys—can be vulnerable.[10] In another example, a hack of a smart refrigerator exposed Gmail login credentials.[11] Lack of compliance by IoT device manufacturers is the most common reason for these breaches.

Shambliss Security provides soup-to-nuts cybersecurity services for businesses. Sherwood suggests that you think about the questions in the graphic above, created for businesses, as an individual or family, and you'll be well served in creating your own online security protocols. For example: Adapt question #2 and ask yourself if your security goals as a wealthy family align with your family priorities. Perhaps you aren't bothered by your children posting pictures to Facebook of your beach house (even if your privacy settings are "friends only"). Maybe it's central to your "brand" as a business entrepreneur to have a very visible and very personal "authentic you" on Instagram. Maybe you like being known by Google as a person with a carpentry hobby and getting recommendations for a fancy new tool. But be very aware that in the era of big data, a huge treasure trove of personal and business information can be hacked and sold that can expose you to fraud, identity theft and personal safety risks. Wealthy families typically aren't the target for the common online criminal; those people are usually going after the low-hanging fruit of more vulnerable individuals (the elderly, in many cases) or very small businesses with little protection in place but still with some financial assets. The wealthy are attractive targets for today's sophisticated cybercriminals with access to very sophisticated, and ever-evolving, technology and skilled people. (Please see "Phishing, vishing and smishing.")

Minimize your footprint

Many people, even wealthy individuals, feel that they have nothing to hide. On the other hand, almost everybody has information, current or from their past, that could be misinterpreted by professional contacts, neighbors or even friends. (Even if you have nothing to hide, do you still want somebody looking through your phone?) "A lot of us just want a place free of public scrutiny," says Sherwood. "This is especially true of business owners who don't want competitors to know everything about them."

Or maybe you just don't want others to know what your house looks like. Is that a drone overhead? Federal Aviation Administration regulations do not specifically address drone flights over residential areas, and current regulations don't care if you're wealthy and don't want others to see your new multimillion-dollar house.

The most important point to remember from a personal perspective is to take a proactive approach to minimizing your online footprint. Too often, people fail to realize that scrubbing information such as a cell phone number or address (or an ill-advised tweet) doesn't mean the data disappears—there's a reason for the saying, "The internet never forgets." If this concerns you, don't put information like that out there in the first place. Hidden risks lurk everywhere. Did you know that Amazon Wish Lists are publicly searchable? What would a journalist or other third party learn about you if they saw what you post there?

The most important defense you have is education: Make sure you understand your own devices and software, mitigation tools, and what information can be collected about you and your activities. In fact, it's important that all family members, from preteens on up, get educated on cybersecurity. One of the newest tools for businesses and individuals is cyberinsurance. "For an individual, this is typically part of their homeowner's liability insurance," says Sherwood.

[10] "Top 10 Biggest IoT Security Issues, intellectsoft.net," 07.30.2020.
[11] "Smart refrigerator hack exposes Gmail login credentials," networkworld.com, 08.26.2015.

"Businesses must buy it separately. It generally covers your business's liability for a data breach involving sensitive customer information, such as Social Security, credit card, account and driver's license numbers."

As far back as 1963, Earl Warren, former chief justice of the US Supreme Court, said, "The fantastic advances in the field of electronic communication constitute a greater danger to the privacy of the individual." [Lopez v. United States, 373 U.S. 427]. Warren was right, but he also couldn't have known that the defenses against privacy invasions would develop in the robust way that they have. But, says Sherwood, "Let's not forget the best defense against security and privacy invasions: common sense."

Phishing, vishing and smishing

Online criminals represent a persistent and evolving threat to our information security. Exploiting our willingness to share information and connect with others online, cybercriminals target individuals and organizations to gain access to sensitive information.

They do this by phishing. Cybercriminals create and send emails that trick the recipient into divulging personal information, performing an action that is fraudulent, or downloading malware by opening attachments or clicking on links. The emails often look real and look like they come from legitimate companies. Even the most alert and aware can be fooled.

Who's doing the phishing?

Organized crime syndicates and individual fraudsters. These cybercriminals target sensitive information (e.g., credit card and bank account information, Social Security numbers, proprietary corporate information) that can be used for identity theft and financial gain.

Nation-states. Cybercriminals are directed by, or act on behalf of, governments to target rival nation-states using cyberespionage and sabotage tactics. Activities include stealing government and industrial secrets, and sabotaging information networks to disrupt a nation's critical infrastructure (e.g., utilities, financial services, transportation services).

Hacktivists. These are individuals or groups committing acts of cybertheft, espionage or vandalism who are motivated by social or political causes.

Recognizing common phishing tactics

Cybercriminals hook you by taking advantage of habits and emotions that drive action, such as fear, urgency, curiosity, compassion and greed, to entice you to click on a link or open an attachment.

- Greed: Messages may promise financial rewards (e.g., "Click here for a gift card").
- Fear: Cybercriminals try to create heightened anxiety (e.g., "The following charges have been applied to your credit card. Click here to view invoice details").
- Curiosity and desire: Messages may offer additional information related to matters of personal interest (e.g., celebrity news, hobbies, current events, social and sporting events).

- Compassion: Cybercriminals use the generosity and caring nature of recipients (e.g., "Click here to donate to a charitable organization"). Spear phishing is a very targeted form of phishing that uses emails that appear to come from a known source (e.g., your manager, a vendor, a client, your friend). Since they appear to be normal, relevant, and/or from a trusted source, they can be particularly difficult to spot.

Cybercriminals are not just using email to trick victims. They are also:

- Vishing: using the telephone
- SMishing: using text (SMS) messaging

1. What to do with a suspicious email or text. Before responding, ask yourself:

- Do I know the sender?
- Am I expecting this message?
- Is the message out of character, inconsistent or poorly written?
- Is this how the sender typically communicates with me?
- Is the message provocative and compelling me to click on embedded links or attachments?

2. Still suspicious?

- Do not click on any embedded links or file attachments.
- Hover over any links—without clicking—to investigate where the link will go. Does the main part of the link match what you would expect from the sender?
- Do not reply to the message sender, even to ask the sender to stop contacting you. Test the authenticity of the message using trusted alternative contact information not provided in the email/text.
- Do not copy anyone on these messages as this increases the chances that the email/text could be opened and the malware released.

In the past, grammar and spelling mistakes, formatting errors and generic salutations (e.g., "Dear Customer,") were common phishing red flags. While these can still be warning signs, the increased sophistication of cybercriminals means they are not as reliable indicators as they once were.

What to do with a suspicious phone call (vishing)

- Ask for the caller's name, phone number and department (or organization if it is someone claiming to be from a supplier). Tell the caller that you'll get back to them.
- Before providing any information, attempt to verify the caller's information using an alternate trusted source, such as contact information from a website.
- Do not be pressured into providing information or taking some action. Threats are common tactics.
- If you're uncomfortable with the questions being asked over the telephone, do not respond. Tell the caller you are ending the conversation and then call back using an independently verified phone number.

- If you receive a phone call or voicemail message you suspect might be "vishing" and feel you must respond, contact the organization using trusted alternative contact information not provided in the message.

CIBC and your online security

We take all reasonable steps to preserve the confidentiality and privacy of CIBC information. This includes accessing and using CIBC information only for the purposes intended, as directed by our leadership or business procedures, and disclosing that information only to those who have a specific and authorized business need to know.

How do we protect client information?

At CIBC, we take the protection of our clients' information seriously. We make reasonable efforts to prevent unauthorized use, sharing, loss and theft of information. We regularly audit our security measures and assess that they remain effective and appropriate. Our employees who have access to client information are made aware of the importance of keeping it confidential.

Information may be shared with or accessed by our service providers so that they can perform services on our behalf. We are careful when selecting our service providers and require them to have privacy and security standards that meet CIBC's requirements. We use contracts and other measures with our service providers to maintain the confidentiality and security of our client information and to prevent it from being used for any other purpose other than that for which it was intended.

We use multiple layers of protection when you access any of our digital products or services, such as digital banking, including:

- Web browser encryption: All browsers supported by CIBC digital services offer industry standard encryption. This provides a high level of protection for transmitting confidential data over the internet.
- Firewalls: We have secure firewalls designed to prevent unauthorized access to our systems.
- Monitoring: We monitor activity on CIBC digital services to enhance security and to protect client personal information.

How do we protect CIBC information?

- We never use personal email accounts for CIBC information classified by CIBC as internal, confidential or restricted.
- We only install authorized CIBC software on devices when using them for work. We ensure we follow approved processes for doing so (approved apps from a corporate store).
- We do not share our passwords for CIBC systems, and we protect our devices from unauthorized access.
- When we conduct work for CIBC on any device or network, we must only use electronic messaging channels approved and provided by CIBC.

How should you share electronic CIBC information?

When sharing CIBC information with internal and external recipients, we must ensure it is protected from loss or exposure to unauthorized parties. When selecting a method of moving digital CIBC information, we consider the following:

- What is the classification of the information?
- Is the information being sent to a CIBC recipient, or a non-CIBC recipient?
- How much information am I sending?
- How often do I need to send this information?
- Do I need to encrypt information that I am sending?

We encourage our clients to take an active role in monitoring their data security. A good first step is to make sure our clients understand the business credit bureaus and how important it is to regularly monitor what is being reported about their businesses. It is not uncommon for the public record to include mistakes, and regularly monitoring their business credit will allow our clients to find evidence of identity theft earlier, rather than later.

Please visit the following link for more information on privacy and security tips for CIBC clients and customers: ***https://www.cibc.com/en/privacy-security/mobile-banking-security.html***

David Griffin, Chief Information Security Officer, CIBC US.

CIBC

CIBC PRIVATE WEALTH

Preserving family wealth

Protecting those you love: Personal safety risk

Protecting those you love

Cybercrime, inadequate travel intelligence, workplace violence, political unrest, extortion, kidnapping—these are the things that keep personal security experts for the wealthy up at night, and rightfully so. Add in simmering sociological change and disruption, and you have a concentric circle of risk with the wealthy sitting at its middle, says Paul Viollis, founder and CEO of Viollis Group International. "In addition, a culture of divisiveness, and a plethora of misinformation, has also resulted in distrust of those in authority—even if they're not wealthy," says Viollis.

According to Viollis, a wealthy family shouldn't focus on fear and "the negative stuff" out there, although there's plenty of it. "These issues are not intended to frighten people," says Viollis. "They're simply very practical, and very important, bits of knowledge that you should incorporate into your safety protocols for your family."

Education: The key to personal security risk management

Viollis suggests that wealthy families think of personal protection strictly as a business model, with an investment and a return on investment—a necessity in these times, and a position that will make you feel empowered, not fearful. Like managing other areas of risk, the process for assessing the risk to you and your family's personal security should follow a clear methodology that identifies areas of vulnerability, followed by a plan for eliminating or reducing those vulnerabilities. Fear of risks is normal, but unnecessary and unnecessarily expensive solutions aren't the answer. "Part of the job of a security expert is to temper people's fear," says Viollis. "Neither the security expert nor the client is served by solutions that aren't right or by an overly broad and jaundiced view of the human race, because that's inaccurate." And done properly and professionally, including the use of thorough intelligence-gathering, a strategy for personal security shouldn't infringe on a family's life and activities, a bonus in the return-on-investment equation.

The most important thing you can do as a wealthy family is have a thorough awareness of the potential for risk to you and your family. If you've decided to remodel or add on to your home, residential security should be of paramount importance. "It makes little sense to 'save' on a cheap security system when your family is at risk," says Viollis. "Your security system should be multilayered—a camera system, detection system and good outdoor lighting, for example. Consider constructing a room for a shelter-in-place option. In addition, I can guarantee you that if I took a survey of people, wealthy or not, maybe one out of 10 would have conducted background checks on the contractors they're inviting into their homes."

As for travel security, many people are more concerned today that they'll be exposed to germs on the plane than they are that their designated driver at their destination might not be trustworthy. Proper vetting by you or an expert is a must. Good travel intelligence also includes knowledge and analysis of the local political climate, organized crime activity, health risks and medical care availability, labor instability and emergency assistance or evacuation.

Good intelligence—as well as a lot of common sense—can also help prevent the nightmare of the wealthy: kidnapping. "It's uncomfortable to think about, but it's a multimillion-dollar business," says Viollis, "and the affluent traveler is often the commodity."

Minimize your risk by understanding several variables at play today. According to the United Nations (UN) Office of Crime and Drugs, terrorist groups have taken to using kidnapping and ransom to help fund their operations. The UN found that between 2008 and 2014, al Qaeda and its direct affiliates made at least $125 million in revenue from kidnappings. In April 2019, the US State Department introduced a new risk indicator on its individual country Travel Advisories to warn Americans about the risks of kidnapping and hostage taking by criminal and terrorist actors.[12] In developing countries, according to Viollis, kidnapping is a highly organized enterprise often run by gangs as a volume

[12] "Keeping Ahead of the Kidnappers : Adapting to Evolving Kidnapping Trends," https://www.asisonline.org/security-management-magazine/articles/2020/04/adapting-to-evolving-kidnapping-trends/ 04.01.2020.

business, with the kidnappers having little interest in hurting the victim. "Express" kidnappings, common in resort cities in Mexico, are characterized by this scenario: A small group of young people get into a cab to go to nightclubs and suddenly find themselves being taken to a place other than their intended destination, and then being forced to withdraw money from an ATM. It's easy money, especially when the kidnappers can repeat it four or five times a night, and generally without physical harm. A smart and sensible plan for risk management to help prevent kidnapping is to make plans in advance to use only vetted and trusted transportation in a foreign country.

Education about risks, and their likelihood and consequences, is the best defense for a wealthy family. "The more empirical data we can use to help educate clients, the better," says Viollis. "When people know the facts, they feel more empowered to manage their risk, because they're not operating from a position of fear based on ignorance."

Common-sense pointers: Keep yourself—and your family—safe

Don't let fear be your mindset, but do let knowledge of the risks that can be out there help you make smart, practical decisions about personal security for you and your family. Here are some common-sense tips:

- If you decide you need physical protection—aka, an old-fashioned bodyguard—perform thorough due diligence on the firm's or person's credentials, experience in personal protection and insurance. Not all states require a license for personal protection services, but you should insist on a firm with liability insurance.
- International travel poses the biggest risk. It also offers some of the easier risk management tactics. Start by using an experienced security consultant to prepare travel intelligence before you leave home.
- Invest in a high-quality home security system. You may also want to look into constructing a shelter-in-place room.
- Although you don't want to dampen the fun completely, have a serious conversation with the college students or young adults in your family about keeping safe on vacations. Stay together in a group, use only pre-vetted and prearranged, reputable transportation, and minimize the "look" of a wealthy American tourist.
- Limit your social media profile, and don't use location services or reveal that "the family departs next Sunday for two weeks in Europe."
- For you, your children and/or your business, embrace the highest risk probability of all, cybercrime, by:
  - assessing the existing vulnerabilities with all your devices at home and work
  - installing a properly encrypted firewall in your home
  - monitoring all the accounts your children have
  - reassessing yearly, given the ever-evolving threat trajectory. (Please see "Tips for protecting yourself online" for more on online security.)

CIBC

CIBC PRIVATE WEALTH

Preserving family wealth

Protecting what is yours: Financial risks of divorce

Protecting what is yours

Loving union, legal contract

It isn't just the oft-referenced sad statistic on marriage—that approximately 50% of marriages end up in divorce. (It's actually more complex than that. A more relevant figure is that today's lifetime risk of divorce is between 42% and 45%.[13]) The big-picture reason for considering a prenuptial agreement is the increasing complexity of lifestyles, of assets that come from numerous and varying sources (inheritance, gifts, an interest in a family business, a lawsuit), career pressures, or "issues" among the generations—or all of these. And don't think of it as an exit plan for a marriage, or "just" a legal document. At the heart of a prenuptial agreement is a conversation that can help a couple understand what they could be facing in their union.

"People often forget that a marriage is a legal contract," says Robert J. O'Regan, partner with Nixon Peabody LLP of Boston, Massachusetts. "A prenuptial agreement can address ahead of time the financial ramifications of the marriage dissolution and the legal rights and obligations two people may have to each other and to children. Or, in the case of a second marriage, what the expectations are for the disposition of an estate to the heirs of each party. It's both good marital planning—because it's based on honest communication—and asset protection. In many of the premarital agreements that I have been part of, it's a healthy and loving exercise. A couple that is comfortable talking about their dreams and aspirations, and equally comfortable talking about 'what if?' scenarios, enters their marriage in an honest partnership. They're talking about ensuring each person's financial protection and honoring each person's vision for the future, while also assessing the risk that is present in any marriage."

O'Regan says that while it's difficult to project significantly varying circumstances—for example, how a couple may feel about disposition of assets if they're married only four years versus 20 years—a common scenario can be a good exercise to encourage deep discussion. "One spouse might anticipate stepping away from a career for a while, or taking a reduced role, because the couple mutually agrees that person will be the primary caregiver for children. That certainly affects future income, as well as eventual retirement. Unfortunately, if this hypothetical couple were to later get divorced, there is one spouse who's made a career sacrifice and is more dependent than the other. A prenuptial agreement could address situations of potential financial inequality such as this one."

The intersection of prenups and trusts

Prenuptial agreements are recognized and accepted in most states; 28 have enacted the Uniform Premarital Agreement Act (UPAA), says O'Regan. In the states that have not adopted the UPAA, prenuptial agreements are permitted and governed by statutory and case law. The UPAA allows marrying couples to contract with respect to a number of areas, including, but not limited to: the rights and obligations of each person in any of the property of the other; the disposition of property upon separation or marital dissolution; the modification or elimination of spousal support; the making of a will or trust and various other matters, provided the agreement is not in violation of public policy or any statute imposing a criminal penalty. For example, a child's right to support cannot be affected in a prenuptial agreement, because public policy prevents parents from bargaining away the rights of their children.

Understand fair disclosure. To be enforceable under the UPAA, a prenuptial agreement must have been entered into voluntarily and must not have been "unconscionable" at the time of signing, according to O'Regan. The issue of whether an agreement is "unconscionable" is decided by the court as a matter of law. Some state statutes are even more stringent than the UPAA with regard to the validity and enforceability of prenuptial agreements. In Massachusetts, for example, the courts have established a "fair disclosure rule" under which each person must fully and accurately disclose to the other his or her financial situation prior to executing a prenuptial agreement. In practice, this has meant putting everything on the table—assets, income and liabilities. Disclosure of income, cash and investment accounts, retirement

13 "What Is the Divorce Rate, Really?" psychologytoday.com, 02.02.2017.

assets, real estate holdings, a beneficial interest in a trust and any expected amounts and sources of inheritances may make some people uncomfortable about entering into such an agreement.

Consider future inheritance. Trusts, of course, are a common wealth planning tool. O'Regan explains that children who know they have a trust interest must disclose that information in a prenuptial agreement. However, the law governing prenups is based on disclosure by the parties of their financial circumstances as currently known, not of the future circumstances they may have if they would benefit from an estate or a life insurance policy they don't know about. What about children at the age of considering marriage who don't know they're a trust beneficiary or that they stand to receive a significant inheritance? That's a bigger family issue that goes beyond legal documents.

"Parents may want to be intentionally vague about what children may inherit, rather than being specific," says Judy Saxe, director of research and education for the Wealth Strategies Group at CIBC Private Wealth. "For some families, full disclosure of potential inheritance is at the outer limits of what they want to discuss. But if the direction or suggestion to do a prenup comes from within the family, the family needs to be prepared for that discussion. Families may use a confidentiality agreement to protect the privacy of financial information leading up to the prenup being prepared. It's easy to understand the tension between full disclosure and asset protection, but it needs to be resolved before a prenup is executed."

Account for state laws. Inclusion of inherited wealth in the event of a divorce depends on the state. According to O'Regan, some include it, others don't. Keep in mind that a prenup is enforced in the state in which the divorce happens, not where the marriage or prenup took place. O'Regan was recently involved in a divorce case in South Carolina, which excludes inherited wealth from the marital estate. "In my home state of Massachusetts, that inherited wealth can be divided," says O'Regan. "That's not a subtle distinction; it could be very significant for many people. In addition, in some states a prenup is directly enforceable as a stand-alone contract, not subject to review under divorce laws."

Provide clarity with postnuptial agreements. A postnuptial agreement can cover any or all of the same things that a prenup can, but is written during the marriage rather than prior to it. "There might a health issue, or an unexpected inheritance, or something more unusual, such as one person suddenly getting a patent that could result in a long-term income stream," says Saxe. "In addition, a more common situation would be one spouse contributing more of his or her separate assets to purchase property or maintain a lifestyle, and the need to reestablish the parameters of the agreement."

O'Regan points out that a postnup can be especially beneficial if one person loses his or her capacity to make decisions or can't communicate wishes. "A postnup done during the marriage that deals with potential inheritances by the spouse's children and similar issues, but before a health crisis becomes acute, legally binds guardians and conservators to ensure heirs are protected," he says. "Like a prenup, a good postnup clarifies expectations and asset disposition as circumstances evolve. It shouldn't be thought of as glue to repair a broken marriage."

Lessons from a landmark Massachusetts case

For a family who has set up trusts for multi-generational wealth planning, it's vitally important to understand the interplay between a prenup and a testamentary instrument. It's even more important to understand the implications of a legal challenge to a trust in the absence of a prenup. A big question for a trust beneficiary is whether that interest is considered a property interest that can be divided at divorce. A recent landmark case in Massachusetts, Pfannenstiehl v. Pfannenstiehl, illustrates this point acutely.

The divorcing couple was in court for several years over the husband's status as one of 11 beneficiaries of a $24 million discretionary, spendthrift trust set up by the family's patriarch. The trust's beneficiaries were the patriarch's lineal descendants, with no designation of any particular interest by any of them. The husband, employed in the family business, had received trust distributions of $800,000 during the last two years before the couple separated. The wife

had left a position when she was about to give birth, two years before her pension would have vested, to care for the baby, who was a special needs child. After the divorce, the Massachusetts Appeals Court ruled that the wife should continue to receive money from the trust because it was "vested in possession," "woven into the fabric of the marriage" and "integral to the family unit."[14] The court awarded her what it said was 60% of the husband's share of the trust money, plus interest, or about $1.4 million. But the Massachusetts Supreme Judicial Court (SJC) reversed the decision, ruling the trust interest did not constitute property, so was not subject to the state's marital property division statute. An error by the Appeals Court, in the opinion of many legal experts, was that the court simply took the current value of the trust and divided it by 11, one share per each then-living descendant of the settlor, and based the award on that. That, says O'Regan, is too "speculative," in part because the trust was discretionary and also because the trust allowed for an "open class" of beneficiaries, meaning beneficiaries will be added as more children are born in the family.

O'Regan knows the case well, as he was the winning attorney at the SJC level. "No beneficiary had a 'right' to receive anything," he says. "Any beneficiary of the trust had an interest so indefinite and uncertain that nobody would be able to determine who would get what at any particular time, and there wasn't a legally enforceable right by the husband to make the trustees give him money. The divorce was between the husband and wife, not between the wife and her husband's family. You can't simply apply 'the facts'—in this case, trust distributions in the last two years of the marriage—to define the trust interests. A trust is a legal instrument and should be interpreted based on trust law. The SJC upheld the notion that the trust's creator did not intend for an ex-spouse of one of his descendants to get part of his estate. The important lesson from this is that the Massachusetts SJC ruled properly that the husband's interest in the trust was not marital property. A person's interest in an asset is a question of law based on a legal document that specifies what the interest is. It is not fact-driven."

Pfannenstiehl also highlighted the importance of precise language in a trust document—there's a significant difference in "shall make" trust distributions vs. "may make" them—and of having an independent trustee. In Pfannenstiehl, the trust's co-trustees were another son and the family's lawyer. The moral of the story: When trusts are part of a family's planning, make sure that the terms are clear enough to withstand a court challenge later.

Short of avoiding marriage altogether, there's no way to avoid the possibility of divorce. A prenup can be thought of as like a will—while state laws do make provisions for both death and divorce, people can make better choices about their assets than a state's laws. But in the big picture, says O'Regan, the most basic concept of a prenup is being honest about expectations. "Don't view a prenup as a jinx on the marriage. With luck, they get signed and nobody ever reads—or needs—them again."

[14] "SJC rules heir can refuse to pay $1.4m to ex-wife," bostonglobe.com, 08.05.2016.

How to have *that* conversation

"It's not you, it's not me—it's them."

The conversation about a prenuptial agreement is likely not a favorite topic for most. Even though parents or grandparents may feel it desirable, even necessary, for a soon-to-marry child to have a prenup, bringing up and discussing the subject is not easy. In some situations, the creators of trust documents with children as beneficiaries simply build into the trust the requirement for a beneficiary to have a prenup in place.

"Clients sometimes include this as a requirement before a child can receive distributions at either a certain age or on a certain date," says W. Scott Thompson, III, CTFA, managing director, southeast regional team executive and co-executive director of CIBC Family Office. "The young beneficiary is in a position to say, 'They put this restriction in here, and I and my siblings have to abide by it.'"

Sometimes conversations about prenups can be surprising for both people in a relationship. "There's no reason a prenup can't be generous," says Thompson. "People tend to think of a prenup as walling off assets, but it also can be explicitly setting out assets for a spouse. For example, we've seen prenups that have 'incentives' based on length of a marriage."

Regardless of the specifics in the legal document, the process of talking about a prenup can be a very healthy exercise. "It's about transparency, communication and laying to rest uncertainties, among other things," says Thompson. "I've had enough conversations with clients over the years to recommend that people not think of a prenup as a dreaded topic. Rather, make the conversation positive and just get on with the business of loving each other."

CIBC

CIBC PRIVATE WEALTH

Preserving family wealth

Resources

Resources: Tips for protecting yourself online

Use the tactics below to mitigate your risk online:

1. Manage your devices

- Use the screen lock on your smartphone to ensure no one can access it in your absence.
- Ensure all your computers and smartphones are password protected. Use strong passwords that are difficult to crack and, above all, don't use passwords that are easy to guess (like your birthday or name).
- Ensure your main computer account is not at an administrator or root level. If hackers get in, this will limit what they can do to your system since they won't have administrator privileges.
- Change the default username and password on your router. Changing the name will stop hackers from being able to guess the device or network you're using. Use Wi-Fi Protected Access (WPA) authentication to create a secure network.
- Use firewalls on any computers and on your router. Most routers have a firewall built into their hardware, but it must first be enabled by the user.
- If your existing router doesn't offer you good security features, replace it with one that does.
- Use strong security software on your computers and smartphones to avoid installation of malware or infection by viruses. Get software that will provide an all-in-one cybersecurity solution for your smart home.
- Always run security patches and updates and keep your software up to date. Outdated software has vulnerabilities that are easy for hackers to exploit.
- Change the default passwords. Leaving a default password on a device enables anyone who owns the same device to gain access. That's almost as bad as having no password at all.
- Changing the passwords every 90 days can significantly increase your security.
- If you have voice-activated devices such as smart speakers, change the alert word from "OK Google" or "Hey Alexa" to something only you and your family know. That way, an intruder won't be able to use your system.
- Before you buy a new device, make sure you have adequate information about its security protection. Find out whether the manufacturer provides regular firmware updates. Six months is a long time in the Internet of Things, and if you're buying a device that will last a decade or more, you need to be sure you'll be protected against emerging threats.
- Buy smart home devices from reputable suppliers, like Samsung, LG, Google or Amazon.
- Examine the privacy policy on a device before you buy it. How is the manufacturer going to make use of your personal data? What data does the device have access to? If you don't intend to use voice activation on a device, you may want to turn the microphone off so that other conversations are not picked up and transmitted.
- Remember to keep the devices updated, either using automatic updates or doing so manually. This might involve checking the manufacturer's website to get updates and then linking the device to a computer to update it. Hackers are always coming up with new ways to compromise devices. Security patches will protect you against those new threats.

- Consider which devices really need to be connected. If you don't use the connected functionalities of your coffee maker or oven, use the device offline.
- Turn off Universal Plug and Play (UPnP). Most smart devices have this feature, which enables them to find other smart devices and connect to them automatically. However, UPnP protocols are vulnerable to outside attack, allowing a criminal to gain control of multiple devices once a single device has been hacked.
- Check the permissions for apps running on your devices. Anything that asks for permission to edit your router's settings is a potential security threat.
- Be wary of cloud storage for devices. Since it requires a cloud connection for upload and download, outsiders could hack into that connection and gain access to your network. If you want to use cloud technology, ensure you understand the right measures to take to secure your data and privacy.

2. Protect your passwords

- Some password management evangelists suggest using passphrases instead of passwords. Passphrases are longer passwords that use sentences, series or combinations of words. They can also contain numbers and special characters. For example, a passphrase could look like this: 2BorNot2B,ThatIsThe?
- Use a different password for each of your accounts. While it might seem like an easy option to reuse the same password for multiple applications and devices, what happens when that password is stolen? The hacker can gain access to all your accounts, both personal and work-related. Using the same password could seriously compromise you or your company. If you make each password or passphrase long and unique, you'll decrease the odds a hacker can access your accounts.
- Store passwords in a password manager.

3. Go online safely

Social networking sites are a convenient means for sharing personal information with family and friends. However, this convenience also brings a level of risk. To protect yourself, do the following:

- Avoid posting information such as address, phone number, place of employment and other personal information that can be used to target or harass you.
- Limit access of your information on a site like Facebook to "friends only" and verify any new requests by phone. Instagram has a privacy function that allows you to block anyone you don't know; those who want to follow you on Instagram must be invited or approved by you.
- Review the security policies and settings available from your social network provider quarterly or when the site's terms of use change. Opt out of exposing personal information to search engines.
- Refer to email best practices concerning unsolicited requests and links: Do not click on attachments or links, in either texts or emails, from a sender you don't know.
- Use a virtual private network (VPN), your own private network across a public network. A VPN still allows you to send and receive data across a public network as if your devices were directly connected to the private network.

4. Implement multifactor authentication

Multifactor authentication (MFA) adds another layer of security and protection beyond just entering a password. MFA is an authentication method that grants a user access to applications, websites, databases, etc. after the user presents two or more pieces of evidence (factors) to verify identity. It verifies the user logging in by requiring both a password as well as other forms of identity.

Multifactor authentication is predicated on the factors of:

- Something you know: password or personal identification number
- Something you have: smartphone, mobile phone, or token
- Something you are: fingerprint or face recognition

A subset of multifactor authentication is two-factor authentication. This method requires two forms of authentication from the three factors—something you know, something you have, something you are—to verify your identity. For example, you may need to enter your password as well as a code on your authenticator app to gain access to a system.

5. Other smart tips for safety

- Don't access sensitive data/sites while on public Wi-Fi.
- Monitor all your online accounts and review statements regularly.
- Be selective in emails saved to a folder on your computer.
- Empty virtual trash often.
- Read those privacy policies from service providers or websites.

CIBC Private Wealth Management includes CIBC National Trust Company (a limited-purpose national trust company), CIBC Delaware Trust Company (a Delaware limited-purpose trust company), CIBC Private Wealth Advisors, Inc. (a registered investment adviser)—all of which are wholly owned subsidiaries of CIBC Private Wealth Group, LLC—and the private banking division of CIBC Bank USA. All of these entities are wholly owned subsidiaries of Canadian Imperial Bank of Commerce.

This document is intended for informational purposes only, and the material presented should not be construed as an offer or recommendation to buy or sell any security. Concepts expressed are current as of the date of this document only and may change without notice. Such concepts are the opinions of our investment professionals, many of whom are Chartered Financial Analyst® (CFA®) charterholders or CERTIFIED FINANCIAL PLANNER™ professionals. Certified Financial Planner Board of Standards Inc. owns the certification marks CFP® and CERTIFIED FINANCIAL PLANNER™ in the US.

There is no guarantee that these views will come to pass. Past performance does not guarantee future comparable results. The tax information contained herein is general and for informational purposes only. CIBC Private Wealth Management does not provide legal or tax advice, and the information contained herein should only be used in consultation with your legal, accounting and tax advisers. To the extent that information contained herein is derived from third-party sources, although we believe the sources to be reliable, we cannot guarantee their accuracy. The CIBC logo is a registered trademark of CIBC, used under license.

Private banking solutions are offered through CIBC Bank USA, Member FDIC and Equal Housing Lender. CIBC Bank USA and CIBC Private Wealth Group, LLC are both indirect, wholly owned subsidiaries of CIBC. CIBC Private Wealth Group and its subsidiaries do not provide, and are not responsible for, the products and services offered by CIBC Bank USA. CIBC Bank USA (Bank) will not pay employees of CIBC Private Wealth Group or its subsidiaries for referring clients to Bank, but to the extent permitted by applicable laws and regulations, the referral of clients to Bank for eligible products or services may be considered by CIBC Private Wealth Group in determining discretionary compensation to employees.

Investment Products Offered are Not FDIC-Insured, May Lose Value and are Not Bank Guaranteed.