Bartholomew & Company, Inc.
Thomas J. Bartholomew, AIF®
President
370 Main Street, Suite 1000
Worcester, MA 01608
508-753-8807
800-440-8807
tom@bartandco.com
www.bartandco.com

The beginning is the most important part of the work. Plato

We are here to help you get started, and to continue along the path towards your goal.

Please call us at 508-753-8807 or 800-440-8807.

Happy New Year from all of us at Bartholomew & Company!

Tom

January 2018

Bartholomew & COMPANY INCORPORATED

How Much Risk Can You Take?

Many market shocks are short-lived once investors conclude the event is unlikely to cause lasting economic damage. Still, major market downturns such as the 2000 dot-com bust and the 2008-09 credit crisis are powerful reminders that we cannot control or predict exactly how, where, or when precarious situations will arise.

Market risk refers to the possibility that an investment will lose value because of a broad decline in the financial markets, which can be the result of economic or sociopolitical factors. Investors who are willing to accept more investment risk may benefit from higher returns in the good times, but they also get hit harder during the bad times. A more conservative portfolio generally means there are fewer highs, but also fewer lows.

Your portfolio's risk profile should reflect your ability to endure periods of market volatility, both financially and emotionally. Here are some questions that may help you evaluate your personal relationship with risk.

How much risk can you afford?

Your capacity for risk generally depends on your current financial position (income, assets, and expenses) as well as your age, health, future earning potential, and time horizon. Your time horizon is the length of time before you expect to tap your investment assets for specific financial goals. The more time you have to keep the money invested, the more likely it is that you can ride out the volatility associated with riskier investments. An aggressive risk profile may be appropriate if you're investing for a retirement that is many years away. However, investing for a teenager's upcoming college education may call for a conservative approach.

How much risk may be needed to meet your goals?

If you know how much money you have to invest and can estimate how much you will need in the future, then it's possible to calculate a "required return" (and a corresponding level of risk) for your investments. Older retirees who have sufficient income and assets to cover expenses for the rest of their lives may not need to expose their savings to risk. On the other hand, some risk-averse individuals may need to invest more aggressively to accumulate enough money for retirement and offset another risk: that inflation could erode the purchasing power of their assets over the long term.

How much risk are you comfortable taking?

Some people seem to be born risk-takers, whereas others are cautious by nature, but an investor's true psychological risk tolerance can be difficult to assess. Some people who describe their personality a certain way on a questionnaire may act differently when they are tested by real events.

Moreover, an investor's attitude toward risk can change over time, with experience and age. New investors may be more fearful of potential losses. Investors who have experienced the cyclical and ever-changing nature of the economy and investment performance may be more comfortable with short-term market swings.

Brace yourself

Market declines are an inevitable part of investing, but abandoning a sound investment strategy in the heat of the moment could be detrimental to your portfolio's long-term performance. One thing you can do to strengthen your mindset is to anticipate scenarios in which the value of your investments were to fall by 20% to 40%. If you become overly anxious about the possibility of such a loss, it might be helpful to reduce the level of risk in your portfolio. Otherwise, having a plan in place could help you manage your emotions when turbulent times arrive.

All investing involves risk, including the possible loss of principal, and there is no guarantee that any investment strategy will be successful.

SERVING OUR CLIENTS & OUR COMMUNITY 20+ YEARS

Don't Delay: The Potential Benefits of Starting to Save Now

For long-term investment goals such as retirement, time can be one of your biggest advantages. That's because time allows your investment dollars to do some of the hard work for you through a mathematical principle known as compounding.

The snowball effect

The premise behind compounding is fairly simple. You invest to earn money, and if those returns are then reinvested, that money can also earn returns.

For example, say you invest $1,000 and earn an annual return of 7% — which, of course, cannot be guaranteed. In year one, you'd earn $70 and your account would be worth $1,070. In year two, that $1,070 would earn $74.90, which would bring the total value of your account to $1,144.90. In year three, your account would earn $80.14, bringing the total to $1,225.04 — and so on. Over time, if your account continues to grow in this manner, the process can begin to snowball and potentially add up.

Time and money

Now consider how compounding works over long time periods using dollar-cost averaging (investing equal amounts at regular intervals), a strategy many people use to save for retirement.[1] Let's say you contribute $120 every two weeks. Assuming you earn a 7% rate of return each year, your results would look like this:

Time period	Amount invested	Total accumulated
10 years	$31,200	$45,100
20 years	$62,400	$135,835
30 years	$93,600	$318,381

After 10 years, your investment would have earned almost $14,000; after 20 years, your money would have more than doubled; and after 30 years, your account would be worth more than three times what you invested.[2] That's the power of compounding at work. The longer you invest and allow the money to grow, the more powerful compounding can become.

The cost of waiting

Now consider how much it might cost you to *delay* your investing plan. Let's say you set a goal of accumulating $500,000 before you retire. The following scenarios examine how much you would have to invest on a monthly basis, assuming you start with no money and earn a 7% annual rate of return (compounded monthly).

Time frame to retirement	40 years	35 years	30 years	25 years
Retirement accumulation goal	$500,000	$500,000	$500,000	$500,000
Annual rate of return	7%	7%	7%	7%
Monthly contribution needed	$190	$278	$410	$617

So the less time you have to pursue your goal, the more you will likely have to invest out of pocket. The moral of the story? Don't put off saving for the future. Give your investment dollars as much time as possible to do the hard work for you.

[1] Dollar-cost averaging does not ensure a profit or prevent a loss. It involves continuous investments in securities regardless of fluctuating prices. You should consider your financial ability to continue making purchases during periods of low and high price levels. All investing involves risk, including the possible loss of principal, and there is no guarantee that any investment strategy will be successful. Review your progress periodically and be prepared to make adjustments when necessary.

[2] Assumes 26 contributions per year, compounded bi-weekly.

These hypothetical examples are used for illustrative purposes only and do not represent the performance of any specific investment. Fees and expenses are not considered and would reduce the performance shown if they were included. Actual results will vary. Rates of return will vary over time, particularly for long-term investments. Investments with the potential for higher rates of return also carry a greater degree of risk of loss.

What Is Cyber Insurance and Should Your Business Have It?

Forty-eight states and the District of Columbia have laws requiring private or governmental entities to notify individuals of security breaches of personally identifiable information. In addition, the Health Insurance Portability and Accountability Act (HIPPA) requires HIPAA-covered entities and their business associates to provide notification following a breach of unsecured protected health information.

Does your company use electronic data? Does it store or communicate potentially sensitive information about customers, employees, or competitors? If so, then a breach of that data could cost your company plenty. Some well-known organizations have experienced data breaches, including WalMart, JP Morgan Chase, Yahoo, eBay, Target, the IRS, and, more recently, Equifax. Unfortunately, just about any size company or organization that retains personal information can be hit with a cyber attack. One way to transfer some of the risk and costs associated with a data breach or network security failure is through cyber insurance.

What is cyber insurance?

Cyber insurance provides protection against potential costs and financial losses resulting from data breaches caused by cyber attacks, viruses, and other threats. It also helps cover third-party lawsuits filed against your company resulting from data breaches or your failure to adequately protect sensitive or confidential information.

What does cyber insurance cover?

While individual policies may differ, cyber insurance can help cover:

- Loss of data: Cyber insurance may help cover the cost of restoring or reconstructing data that was lost, stolen, or damaged.
- Losses from data breach or security failure: Cyber insurance assists in covering some of the costs of investigating how and where the breach occurred; expenses associated with regulatory fines; legal costs of defending against lawsuits and settlement of claims brought by victims whose information was inappropriately accessed, shared, or lost; expenses related to notifying victims of the data breach, such as customers and employees.
- Costs associated with extortion or ransom demands: That's right, often a cyber criminal will demand a ransom or try to extort money from your company in exchange for your data. Cyber insurance covers some of the costs of paying the ransom for the data or for the restitution to victims whose information was captured.
- Losses from business interruption: If your company must close while the data breach is investigated and resolved, cyber insurance can help offset the ordinary costs and expenses of your business during its down time.

Who needs cyber insurance?

Your company or organization may be a candidate for cyber insurance if it does any of the following:

- Sends or receives documents electronically
- Communicates with customers or third parties via email, text messages, or social media
- Stores third-party information on a computer network that may be considered sensitive or private, such as an individual's identity, tax information, income, address, Social Security and/or credit card numbers
- Stores confidential company information or data (e.g., tax documents, sales or marketing figures or projections, trade secrets) on a computer network
- Advertises company services or products via a website or social media

Aren't these risks covered by business insurance?

Unfortunately, most of the risks and losses resulting from data breaches or losses are not covered by standard commercial general liability insurance. In fact, many policies contain a specific electronic data exclusion. In addition, loss or damage to electronic data isn't considered property damage under a business policy, so coverage wouldn't apply.

Questions to think about

Cyber insurance has policy exclusions, terms, and conditions. When thinking about the purchase of cyber insurance, here are some questions to consider:

- What specific risks are covered, and what risks are not covered?
- What deductibles or coverage limits apply?
- Will the insurer require your company to undergo a security risk review?
- Are there security controls your company can adopt that will decrease the premium?
- Will the insurer identify security risks and offer alternatives to minimize or eliminate those risks?

Plan ahead

Cyber attacks and loss of data can be devastating to a business. Plan ahead before a cyber attack occurs. Evaluate your business and determine areas of particular vulnerability. Then create cybersecurity policies and procedures for company employees to follow. Finally, consider the purchase of cyber insurance to help cover at least some of the risks associated with a cyber attack.

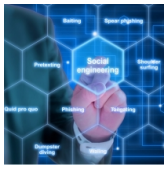
Bartholomew & Company, Inc.
Thomas J. Bartholomew, AIF®
President
370 Main Street, Suite 1000
Worcester, MA 01608
508-753-8807
800-440-8807
tom@bartandco.com
www.bartandco.com

What can I do to crack down on robocalls?

You may not mind if a legitimate robocall provides a helpful announcement from your child's school or an appointment reminder from a doctor's office. But sadly, criminals often use robocalls to collect consumers' personal information and/or conduct various scams. Newer "spoofing" technology displays fake numbers to make it look as though calls are local, rather than coming from overseas, which could trick more people into answering the phone.

Robocalls have been illegal since 2009 (unless the telemarketer has the consumer's prior consent). In mid-2017, federal agencies announced they are ramping up enforcement by fining violators and encouraging blocking technologies. What should you do if you want to help put an end to this nuisance?

1. Don't answer calls when you don't recognize the phone number. If you pick up an unwanted robocall, just hang up. Don't answer "yes" or "no" questions, provide personal information, or press a number to "opt out." Responding to the call in any way verifies that it has reached a real number and could prompt additional calls.
2. Look into robocall blocking solutions that may be offered by your phone service provider. If they're available, you may need to follow specific instructions to "opt in." Otherwise, consider a mobile app or cloud-based service designed to block robocalls; some of them are free or cost just a few dollars.
3. Consider registering your phone number on the National Do Not Call Registry. While taking this step can help mitigate the amount of robocalls you receive, it's only a partial solution to the problem. The Federal Trade Commission advises consumers whose numbers are on the registry but still receive unwanted calls to report robocall violations at complaints.donotcall.gov. The phone numbers provided by consumers will be released each day to companies that are working on call-blocking technologies, which largely depend on "blacklists" with numbers associated with multiple complaints.



How can I protect myself from digital deception?

Imagine that you receive an email with an urgent message asking you to verify your banking information by clicking on a link. Or maybe you get an enticing text message claiming that you've won a free vacation to the destination of your choice — all you have to do is click on the link you were sent. In both scenarios, clicking on the link causes you to play right into the hands of a cybercriminal seeking your sensitive information. Just like that, you're at risk for identity theft because you were tricked by a social engineering scam.

Social engineering attacks are a form of digital deception in which cybercriminals psychologically manipulate victims into divulging sensitive information. Cybercriminals "engineer" believable scenarios designed to evoke an emotional response (curiosity, fear, empathy, or excitement) from their targets. As a result, people often react without thinking first due to curiosity or concern over the message that was sent. Since social engineering attacks appear in many forms and appeal to a variety of emotions, they can be especially difficult to identify.

Take steps to protect yourself from a social engineering scam. If you receive a message conveying a sense of urgency, slow down and read it carefully before reacting. Don't click on suspicious or unfamiliar links in emails, text messages, and instant messaging services. Hover your cursor over a link before clicking on it to see if it will bring you to a real URL. Don't forget to check the spelling of URLs — any mistakes indicate a scam website. Also be sure to look for the secure lock symbol and the letters *https:* in the address bar of your Internet browser. These are signs that you're navigating to a legitimate website.

Never download email attachments unless you can verify that the sender is legitimate. Similarly, don't send money to charities or organizations that request help unless you can follow up directly with the charitable group.

Be wary of unsolicited messages. If you get an email or a text that asks you for financial information or passwords, do not reply — delete it. Remember that social engineering scams can also be used over the phone. Use healthy skepticism when you receive calls that demand money or request sensitive information. Always be vigilant and think before acting.