10 Considerations for Managing Risk with Professional Liability Insurance

Insights to help you protect your firm within the evolving risk environment

In brief:

- **Understand:** Be aware of your risks and the insurance solutions available to help you meet them. The risk environment for registered investment advisor (RIA) and broker-dealer (BD) firms is dynamic, and successfully navigating the inherent challenges may require evolving with the risks. Maintaining a strong and risk-savvy culture of compliance sometimes requires going beyond explicit regulation to focus on discretionary risk mitigation opportunities.
- **Align:** Professional liability insurance can be a powerful tool in this endeavor, but with the complexity inherent in covering evolving risks with insurance products that can themselves vary significantly between policies, it is critical that firms align their insurance coverage with their business. If your firm does not have sufficient insurance expertise in-house to facilitate such an alignment, consider enlisting third-party support in the form of an independent insurance consultant or broker.
- **Govern:** Be disciplined and strategic in establishing ongoing governance of your professional liability insurance program. Institutionalize a review process that monitors your risk and explores opportunities to mitigate it and enhance your firm's sustainability. Firms should complete this review at least annually, in time to support the renewal process. Beyond this, ongoing monitoring of both your business and your risk environment, to identify and respond to material changes in either, is a best practice.

CONTRIBUTORS:

Jessica Thayer, Senior Vice President and Financial Institutions Practice Leader, Starkweather & Shepley Insurance Brokerage, Inc.

Alina Gatskova, Vice President, Custody and Clearing Correspondent Credit Risk, Fidelity Investments

Jason Duffy, Vice President, Corporate Treasury Insurance and Risk Management, Fidelity Investments

Inside, you'll discover:

Fidelity INVESTMENTS

I. The Value of Being Prepared

Risk management is a primary concern for RIA and BD firms, as it is for the broader financial services industry. Its practice is central to so much of the work that we do. Yet, in response to Deloitte's 11th Global Risk Management Survey of financial institutions,[1] respondents reported a significant disparity between their ability to manage the traditional financial risks they face, and the nonfinancial risks that have become more prominent in an ever more interconnected world. More specifically, while nearly all respondents (~90%) considered their institutions to be extremely or very effective in managing traditional financial risks, only about half of them said the same about risks in several key areas:

57% Reputation

56% Operational

50% Conduct and Culture

54% Business Resilience

40% Third-Party

34% Data Integrity

This disparity raises important questions:

- If a legal claim is levied against your firm for damages due to errors, negligence, or misconduct, how will you respond?
- What resources are available to support a vigorous defense, if the claim is unfounded?
- If required, do you have the ability to make your client whole?
- How would such an incident impact your firm's financials and overall sustainability?

For many firms, better addressing these questions and the risks they reflect demands proactive enhancement of their risk management programs, including with professional liability insurance. This field of insurance provides companies and employees with financial protection from lawsuits related to their professional work.

Within the financial services industry, these policies have evolved with the risk environment and grown in complexity in recent years. Fewer firms than you might expect—given the industry's expertise in managing long-term risk for their clients—fully understand how to optimize their liability insurance portfolios, and fewer still have done so. This may be especially true among small and mid-sized firms that may not have alternative protections common to larger firms—such as bigger balance sheets or in-house counsel—that could help them to otherwise weather a liability claim.

Of particular concern is the field of cybercrime and cybersecurity insurance. We know that this is a top risk for our industry,[2] and regulators have deemed it a priority.[3] The North American Securities Administrators Association even went so far as to note a lack of adequate cybersecurity insurance as the most common cybersecurity deficiency among examined firms.[4]

A strong culture of compliance and risk management is a competitive advantage for RIA and BD firms, whether you're competing for clients, talent, or potential M&A partners. Many firms recognize this and take steps to cultivate such a culture; however, opportunities remain. With the expectation that firms attuned to their risks and risk mitigation options will take steps to better prepare and protect themselves, this article will:

1. Summarize the primary types of insurance that firms can use to help cover their major professional liability exposures.
2. Suggest considerations for firms to keep in mind when reviewing their insurance portfolios.

II. Types of Professional Liability Insurance Retained by RIA and BD Firms

Following is an overview of the four primary types of policies that firms typically employ to cover their major risk exposures:

1. **Crime Bonds**
2. **Errors & Omissions**
3. **Directors & Officers**
4. **Cybersecurity**

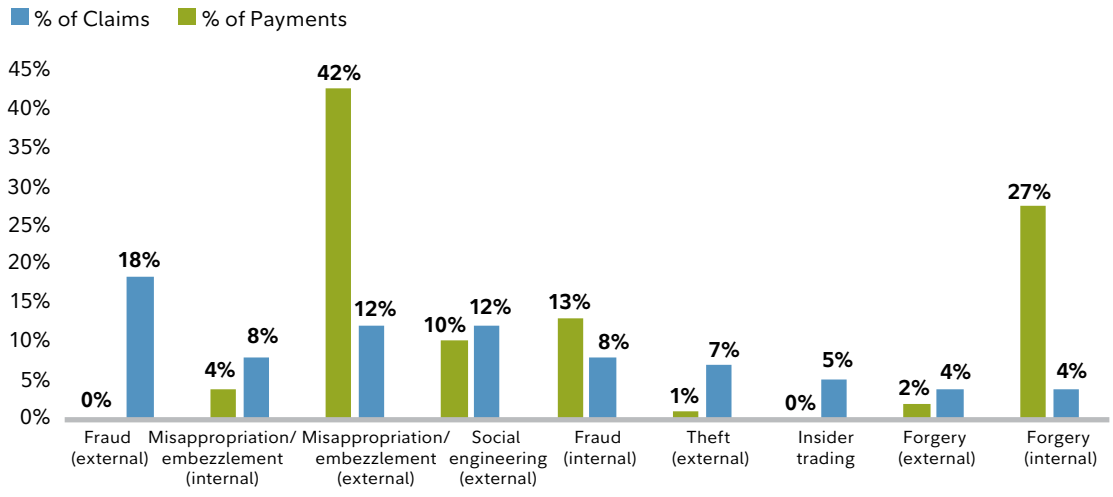
Crime Bonds

In some circumstances, industry regulations require firms to maintain commercial crime policies. These policies, typically referred to as Fidelity Bonds or Crime Bonds, protect against losses due to employee dishonesty or third-party crime. Common types of bonds include:

- **Securities Dealer Blanket Bonds**—These bonds are required for all FINRA members. FINRA's requirement under Rule 4360 is that all member firms join the Securities Investor Protection Corporation (SIPC). SIPC, in turn, requires members to purchase and maintain a blanket fidelity bond.
- **ERISA Bonds**—The Employee Retirement Income Security Act of 1974 (ERISA) requires every fiduciary and handler of funds or property of qualified employee benefit plans to be bonded, to protect these plans from losses due to fraud or dishonest acts.
- **Investment Company Bonds**—Similar to FINRA and ERISA bonds, Rule 17g-1 of the Investment Company Act of 1940 requires registered investment companies to retain bonds against mutual fund losses resulting from certain types of employee crime.

FREQUENCY AND SEVERITY OF CRIME LOSSES BY TYPE

In assessing your crime risk, it can be tempting to focus on the most common types of crime. However, as shown below, less common types of crime can have an outsized impact. Know your risk and protect yourself appropriately.



Source: Willis Towers Watson 2019 Intelligence & Risk Insights Report. Loss types with < 4% representation have been excluded for illustrative purposes.

In addition to coverage for traditional forms of theft, Crime Bonds can also include coverage for losses due to cybercrime. While firms may separately purchase cybersecurity insurance, those policies are focused on third-party privacy liabilities and expenses related to failures to protect intangible data. Crime Bond provisions on cybercrime, on the other hand, address losses resulting from the digital theft of tangible assets such as money, securities, or other property.

Some firms also opt to acquire supplemental bond coverage, above and beyond any regulatory requirements. These general bonds, often referred to as Financial Institutions Bonds, can help provide comprehensive coverage for the loss of money, securities, and other property for which a firm is legally liable.

Errors & Omissions

Errors & Omissions (E&O) insurance is a type of professional liability insurance that firms can purchase to protect themselves and their employees against losses stemming from alleged negligent acts, errors, omissions, or breaches of duty by the firm or its employees, while performing brokerage, investment advisory, or other professional services. It is essentially a form of malpractice insurance.

These policies often cover costs related to litigation, settlements, and judgements, and coverage extends up to the amount specified by the insurance contract, in excess of the deductible. Defense costs associated with formal regulatory investigations may also be covered.

While custody and clearing partners may require firms to maintain E&O coverage as a business requirement, there is no regulatory requirement for a firm to maintain an E&O policy.

Directors & Officers

Similar to Errors & Omissions insurance, Directors & Officers (D&O) insurance is optional and protects firms against losses related to alleged misconduct or negligence. However, D&O insurance is focused on actions taken by officers and directors in the management of the firm. D&O coverage is often included as part of a BD firm's E&O policy form. When it is not already covered in this way, firms can typically purchase D&O coverage as an additional component on E&O policies.

Insured persons, as well as the organization, are generally covered for liability to third parties (investors, regulatory authorities, and other potential litigants) that arises out of their activities while serving in their official capacities. Coverage also applies to an insured person's spouse, domestic partner, and other beneficiaries in the event that a suit is continued against these individuals after the insured person's death or incapacity.

Triggers for D&O coverage include the filing of civil or criminal judicial proceedings, arbitration or mediation proceedings, administrative or regulatory investigations or proceedings, and written demands for monetary or non-monetary relief.

Cybersecurity

Cybersecurity Insurance, also referred to as Network Security and Privacy Liability Insurance, largely guards against losses incurred from data breaches. These policies are designed to help organizations mitigate risk exposure by addressing claims brought by individuals or organizations whose privacy, or confidential information, may have been affected by a breach.

Policies come in many shapes and sizes, with some providing very little coverage and insuring only against litigation, while others provide coverage for a host of services that minimize exposure and help firms recover from a breach with minimal damage. This coverage is distinct from the cybercrime protections that your crime bonds may offer.

While it is imperative for firms to update policies and procedures to help prevent breaches, the right cybersecurity insurance policy can be a significant asset for firms focused on the resiliency and sustainability of their business. It can also be a critical asset for firms that experience a cyber incident.

WHAT'S COVERED BY A CYBERSECURITY POLICY?

State laws govern the world of cybersecurity, and if you have clients in various states, properly responding to incidents can be a challenge. Getting the right support is imperative. While actual policies can vary significantly, they commonly include coverage for the following types of recovery support:

- **Cyber Extortion**—Expenses incurred, and extortion ransoms paid, in the event of a credible extortion threat.
- **Data Forensics**—Expenses for system repair and information recovery, in cases where data may have been lost, damaged, erased, or corrupted.
- **Public Relations Expenses**—Approved public relations firm assistance, in the protection of brand reputation, in the event of a data breach.
- **Business Interruption**—Business income loss and interruption expenses incurred in the event of a data breach.
- **Dependent Business Interruption**—Loss of income and interruption expenses as a result of the compromise of a third-party service provider's system.
- **Access to a Data Breach Coach**—Access to consultants to walk you through next steps in the event of a breach or potential data breach.
- **Credit Monitoring**—Costs to offer potentially affected third parties the ability to use credit monitoring services to mitigate damages.
- **Notification Costs**—Expenses to notify affected parties of a breach, where required by law. In some policies, coverage is also extended to voluntary notification expenses, beyond legal requirements.
- **Liability, Including Defense Expenses**—Claims and defense expenses for liability stemming from your failure to protect confidential information or prevent virus attacks, denial of service attacks, or malicious code.
- **Coverage for Fines and Penalties**—Fines and/or penalties for privacy-related regulatory body proceedings or investigations.

Importantly, cybersecurity coverage is not necessarily contingent on where the breach occurs, as some policies provide coverage for breaches that occur on third-party systems too. As with all coverage provisions, coverage may be specific to or contingent on certain factors. Ensure that you review the relevant language in your policy to understand how well the policy covers your firm's practices as it relates to protecting client data.

III. 10 Considerations for Firms Reviewing Their Professional Liability Coverage

1 Establish a Strategic Review Process

Perhaps the most important consideration for firms to keep in mind is the importance of regularly reviewing your risk profile and coverage. While professional liability insurance is generally not a requirement, cultivating a culture of compliance and effectively managing your firm's long-term risk may require thinking beyond minimum requirements to establish a formal strategic review process. Firms should use their discretion to assess their professional liability risk and evaluate their risk mitigation program. If this is not expertise that your firm retains in-house, consider consulting with an insurance expert who understands your business. That could be a broker or an independent consultant. Regardless, a regular review process can enable firms to stay abreast of, and address, evolving risk factors in a timely fashion. A thorough review may be incorporated into your annual renewal process, but with the ability to amend policies as needed, it's also important to develop an ongoing awareness of any material changes in your risk exposures that may arise during the year.

For insight into how much coverage firms like yours purchase, as well as how much firms pay for different amounts of coverage, please refer to the benchmarking provided within the appendix.

2 Consider Coverage Holistically

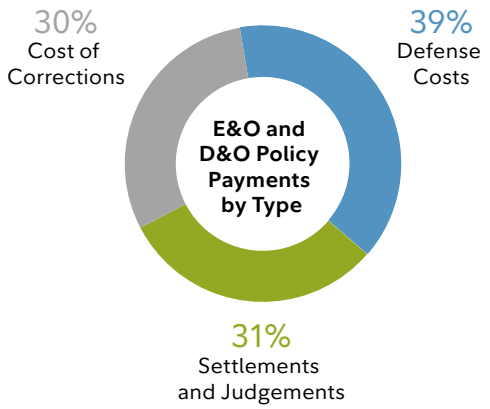
These types of insurance policies have grown in sophistication, and firms that purchase them should ensure that they know what coverage they're buying, and—to the extent possible—align their coverage with their firm's major risk exposures. While all of the policy types outlined in this article often do largely align with the provided definitions, real world policies in the market may differ.

On top of that—after riders and exclusions—a policy that began in one form may end up looking quite different. For example, an E&O policy could exclude transactions involving a certain class of securities, while adding elements more commonly found in a cybersecurity policy. It is important to holistically understand the full range of coverage you have, how well it aligns to your business, and how you can customize it to reduce risk exposure and avoid redundant coverage. Bundling policies may also offer opportunities for cost savings.

3 Be Proactive

Consider adding Cost of Corrections coverage to your policies. This add-on allows firms to be proactive in addressing issues prior to any claims, instead triggering coverage based on their own identification of errors, omissions, negligence, or other breaches of duty. According to ICI Mutual Insurance, nearly a third of E&O policy payments from 2008 to 2018 were for Cost of Corrections. Trading error corrections are common situations where this coverage would come into play. This coverage feature typically comes with separate requirements that may include acquiring the insurer's approval prior to taking corrective action.

E&O AND D&O POLICY PAYMENTS BY TYPE



Source: ICI Mutual Insurance Company's 2019 Claims Trend report. Based on claims submitted between 2008 and 2018.

4 Align Your Coverage with Your Business

It is important to understand how "insured services" and "insured products" are defined within your policy. As an example, an E&O policy typically states that you are covered for professional services, which can mean different things for differently structured firms. For RIAs, for example, this could cover the core advisory function of the firm. For BDs this generally refers to the sale of securities. However, whether or not key services such as financial planning or trust services are covered can vary from one policy to the next. Additionally, activities that may pose a higher insurable risk—such as private placements or underwriting activity for BDs—are often not covered in a standard policy. Policies are written for a general set of services that are automatically covered, and it is up to the firm to review these policies and negotiate any additional coverage that they may require. Simply acknowledging the existence of activities or products within the application does not guarantee their coverage within the policy.

5 Maintain Continuity of Coverage

Familiarize yourself with your policy's continuity and retroactive date to facilitate continuity of coverage. If you change carriers—or even sometimes in renewals—the effective date of your coverage may be reset as your new policy inception date. In that instance, any claims arising from incidents pre-dating the policy would not be covered. To avoid this issue, some firms will request a retroactive effective date—including back to the date the firm first purchased that type of insurance with any carrier. To accomplish this, firms are typically required to sign a "no known loss warranty," attesting that they are not aware of any past incidents that could be claimed as losses.

6 Consider Final Adjudication Language

Most policies have conduct-based policy exclusions for illegal activity and fraud. However, the specific language within a policy determines the treatment of claims made against firms and their employees, with regard to the costs associated with their defense. Even in the case of groundless allegations, defense costs can add up. A clause may be included in your policy stipulating that defense costs will be provided until a final (non-appealable) adjudication of liability. If this language is not currently included in your policy's exclusions, you may want to consider adding it to enable the defense of your firm and employees throughout the entire life cycle of a lawsuit.

7 Know Your Role in Litigation

Firms should look at their insurance policy's terms relative to selection of counsel. Some policies stipulate that an insurer has a duty to defend the insured. This language simply indicates that the insurer is responsible for your firm's legal defense, including selecting counsel and controlling defense strategy. Policies without this language allow firms to select their own counsel and set strategy. However, they may include restrictions as to what costs are covered, and they may require firms to select counsel from an approved list of attorneys.

8 Communicate Cautiously and Deliberately

To acquire professional liability insurance, you'll be required to provide a completed application. You may also be required to complete a warranty, if you need to establish a retroactive effective date. It's important to recognize that any written representations that you provide to your insurance carrier surrounding known losses or potential claims may be referenced in the event of a claim. If the insurance carrier believes there was specific knowledge of an action that could give rise to a claim, and that action took place prior to purchasing the insurance policy (regardless of your designated retroactive date), coverage may be denied based on the information you provided. Such representations should only be made carefully and as required to procure coverage.

9 Plan on Variations Between State Laws

Some carriers will amend their policy so that the limitation against matters that are uninsurable under law will be determined in accordance with the law that is most favorable to coverage. The enhanced language typically provides that the law

where the policy holder is domiciled, the law where the underlying matter is being adjudicated, or the law where the insurance company has issued the policy may be used to determine coverage. As with most types of policy enhancements, this one often comes with additional costs and/or higher deductibles.

10 Anticipate Potential Cybercrime

As cybercrime and other cybersecurity risks continue to grow, firms should understand their exposures, along with how they may amend or supplement their insurance policies to cover them. Cybercrime, specifically, is an emerging area of significant concern. Keep in mind that your primary defense against this risk is your crime bond. If you haven't already, consider expanding the coverage grants under your bonds to specifically include social engineering/impersonation fraud, by covering fraudulently induced payments or transfers. In the face of potential cybercrime, it is good to be prepared.

Keeping these considerations in mind can inform your firm's decisions around your professional liability insurance program. More broadly, firms should also remember that value in your insurance is derived from using it. This may seem obvious, but in fact, many firms don't do enough to promote internal awareness of the availability of insurance, or to develop sufficient controls and processes around handling claims. Rank-and-file employees often don't know that there's a policy, and senior leaders are not always made aware of their notification responsibilities. In such cases, firms may inadvertently provide late notice of claims under the policy requirements, resulting in a coverage denial on that basis. To mitigate this issue, firms can build internal awareness of their insurance products and incorporate policy language that limits the notice requirement to apply only once a designated leader familiar with the policy is aware of the matter. Firms should understand their claim-reporting responsibilities and establish processes to ensure that they meet them.

IV. Expert Perspectives

We asked our contributors to share their key insights on using professional liability insurance to protect your firm.

"Lack of uniformity in E&O insurance policies, coupled with increased sophistication of the insurance companies and policy underwriters, means that policies are crafted in a way that requires much greater attention to the fine print. But E&O insurance is a necessity in this industry, and, when structured correctly, it can be invaluable."

—Alina Gatskova, Vice President, Custody and Clearing Correspondent Credit Risk, Fidelity Investments

"In buying insurance, you are transferring risk by purchasing an insurer's promise to pay, as a result of certain unforeseen events. It is imperative that you have a clear understanding of the efficacy of your insurance program. This includes identifying how the coverage and exclusions apply to the risk that you transfer, the financial condition of the insurer, the willingness of the insurer to pay your claims as measured through the claims experience of the insurer's clients, and the cost of the policy relative to the amount of risk it transfers."

—Jason Duffy, Vice President, Corporate Treasury Insurance and Risk Management, Fidelity Investments

"It is important to adopt and implement risk management policies and procedures, but it is also important to ensure that, should there be a breakdown in your practices or unforeseen circumstances, you have a backstop to protect your firm. Insurance policies need to be carefully crafted and negotiated to address these exposures."

—Jessica Thayer, Senior Vice President and Financial Institutions Practice Leader, Starkweather & Shepley Insurance Brokerage, Inc.

Professional liability insurance, in its many forms, can be a significant tool for firms focused on managing their risk. As with so many financial solutions, the keys to its value are to understand your firm's relevant needs, to ensure that the solution you choose aligns well with those needs, and to apply a disciplined governance process to the ongoing review, maintenance, and enhancement of your program.

Appendix

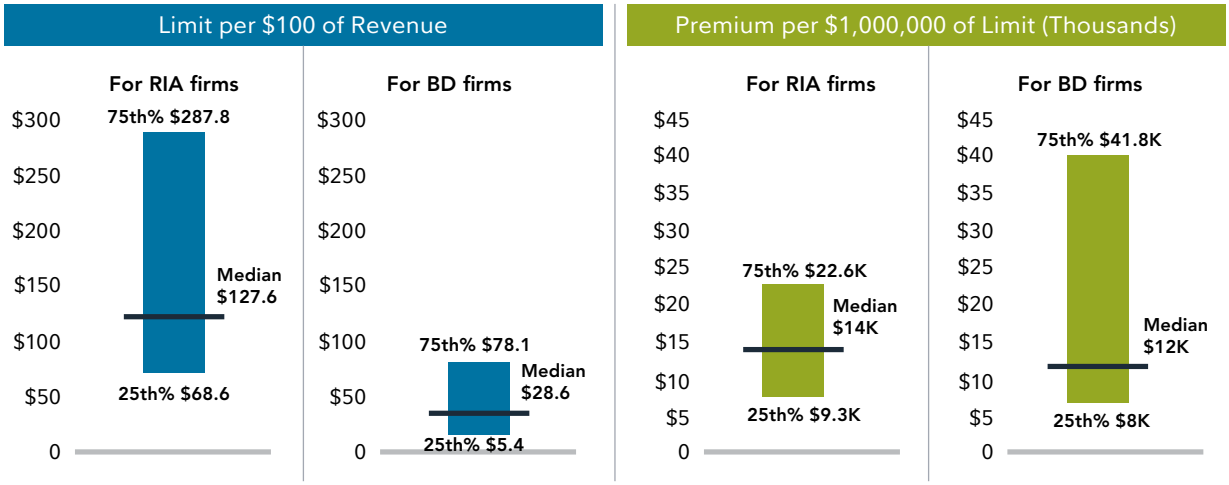
GLOSSARY OF TERMS

- **Cybercrime**—Any criminal activity that involves a computer, network device, or network.
- **Cybersecurity Insurance**—Insurance designed to help companies recover from cyberattacks.
- **Cost of Corrections**—Policy add-on that provides coverage based on a firm's own identification of errors or negligence, without the requirement of a written demand.
- **Duty to Defend**—Policy language requiring insurers to select counsel and manage defense strategy for your firm, in the event of a covered claim.
- **Effective Date**—The day on or after which covered claims reported would be covered under a policy.
- **Endorsements**—Sometimes called riders, endorsements are amendments that change the scope of a policy.
- **Final Adjudication Clause**—Language requiring defense costs to be provided until a final (non-appealable) adjudication of liability.
- **Retention**—Also known as a deductible, this is the amount the insured must pay before the insurer will pay a claim.
- **Retroactive Date**—The day on or after which covered events would be covered by a policy.
- **Law Most Favorable**—Provision stating that matters that are insurable by law be defined by the applicable law most favorable to coverage.
- **No Known Loss Warranty**—Statement to an insurer that no known potential losses exist, to secure a retroactive date.
- **Social Engineering**—Deceptive manipulation of individuals into divulging confidential information to facilitate fraud.

Errors & Omissions Insurance Benchmarking

To assist firms in their assessment and enhancement of their professional liability insurance programs, we've included key benchmarking data, sourced from Advisen's proprietary database.[5] This data includes amount of coverage purchased ("limit") and rate/cost of insurance ("premium"). Both metrics are provided in the form of a ratio, enabling firms to explore the data with different variables.

The following chart provides Limit per $100 of Revenue and Premium per $1,000,000 of Limit. This includes medians, as well as 25th and 75th percentiles, for BD and RIA segments.

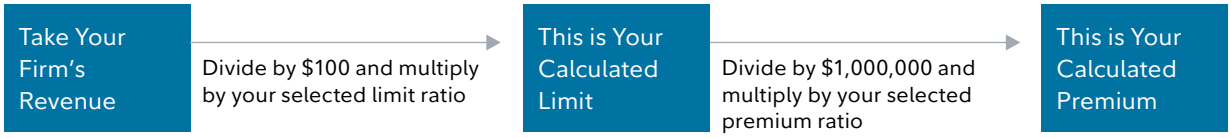


For illustrative purposes only.

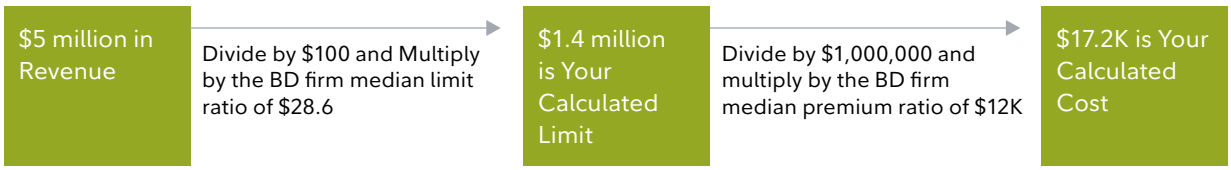
As shown in the chart above, there can be quite a bit of variability in both the amount of insurance purchased and the price paid for that insurance—even for similar firms. Add to that the variability that is to be expected in these ratios across firms of different type, size, and scope of work, and it becomes clear that illustrative calculations that leverage this data are limited to providing firms with rough approximations and an overall sense of scale. Fortunately, these types of estimations can still offer firms that are developing their understanding of this insurance market a solid head start.

In that light, consider your overall risk tolerance, as well as your best estimation of your firm's risk relative to peers. Based on your evaluation, and using the ratio charts above as a guide, select a ratio for each limit and premium calculation. If you'd like to start in the middle, use the median; if you'd prefer to explore more or less coverage or costs, adjust from there.

Once you've selected ratios, you may calculate hypothetical limits and premiums as follows:



Here's an example:



For illustrative purposes only.

Please also note that the top drivers of limit often differ between RIA and BD firms. For this reason, attempts to draw meaningful apples-to-apples comparisons across these segments are not feasible with the available data.

200 Seaport Boulevard, Boston, MA 02210

For more information, please contact your Home Office or Fidelity relationship manager.

Endnotes

[1] Global Risk Management Survey, 11th Edition, Deloitte & Touche, LLP, 2019.

[2] Allianz Risk Barometer: Top Business Risks for 2019.

[3] 2019 Examination Priorities, U.S. Securities and Exchange Commission Office of Compliance Inspections and Examinations.

[4] 2019 Investment Adviser Coordinated Exams, North American Securities Administrators Association.

[5] Advisen, Ltd. proprietary database. Data pulled 9/27/19, covering policies over the previous 24 months.

For investment professional use only.

902384.1.0 1.9890012.100