Brown & Brown

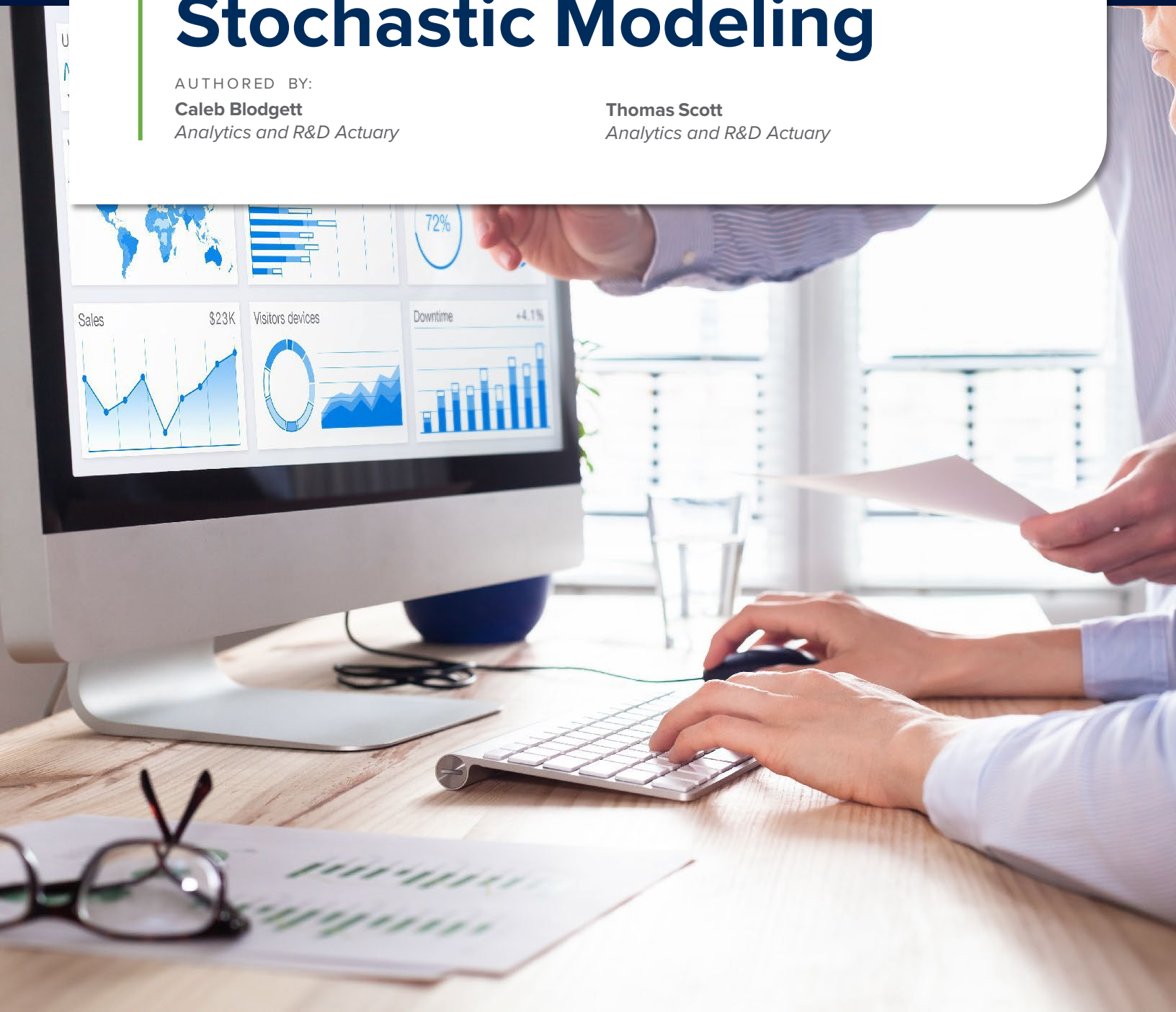
WHITE PAPER 2 OF 3

A Case Study Using Advanced Stochastic Modeling

AUTHORED BY:

Caleb Blodgett
Analytics and R&D Actuary

Thomas Scott
Analytics and R&D Actuary



Introduction

In our first white paper, *The Need for Efficient Risk Financing Strategies*, we discussed the value that can be unlocked when firms view risks holistically and optimize their total cost of risk. Producing a portfolio view of risk requires one to first quantify risks on an individual basis. The best tools for such an analysis, as we reviewed, are stochastic risk models. We turn now to ground these concepts in a practical context. For the remainder of this series, we will walk through a case study involving a fictional company to show the risk quantification and subsequent analysis of selecting an optimal risk financing program.

As discussed in the prior white paper, to produce a portfolio view of risk requires not just quantifying risks individually but also understanding how they interact, an exercise that may reveal causal relationships between risks or unexpected correlations that are significant in risk quantification.

Cyber risk and directors & officers (D&O) liability are two lines whose interactions should be carefully analyzed. In recent years, extreme cyber losses, such as a large-scale data breach or an extended shutdown of operations, have led to shareholders filing securities class action lawsuits against several publicly traded U.S. firms. The typical allegations include the company's misrepresentation of cybersecurity posture or withholding material information from a cyber incident. Going forward, the dependencies between D&O and cyber are expected to become even further intwined. In July 2023, the SEC adopted new rules requiring timely disclosures on material cyber incidents and annual disclosures regarding cybersecurity risk management plans, including the role and oversight of key managers and the board of directors.

In part to address this new risk landscape, Brown & Brown has recently released two new stochastic modeling frameworks, Cyber In-Site™ and D&O In-Site™. Both leverage heavily researched quantification methodologies to help companies assess their cyber and D&O risk profiles and evaluate risk financing strategies. Our case study will include an in-depth analysis of these two risks for illustrative purposes. Each presents its own challenges, underscoring the necessity for robust modeling approaches.

Case Study: Company XYZ – Quantifying Portfolio Risk

For our case study, we will focus on a simplified setting involving a fictitious company, Company XYZ. XYZ has approached Brown & Brown with the aim of better understanding its cyber and D&O risk profiles, whether its existing insurance program leaves the firm with a level of retained exposure within its corporate risk appetite and what alternative risk financing options are available to help optimize its total cost of risk considering all hazard risks. Historically, it has selected its insurance programs based exclusively on peer benchmarks for limits and retentions.

Before reviewing any risk financing options, we will first quantify XYZ's risk profile for cyber and D&O separately and address any line-specific concerns. To quantify each risk, we utilize Brown & Brown's corresponding stochastic modeling frameworks. Each considers various aspects of XYZ's risk profile, runs an extensive Monte Carlo simulation and outputs probability distributions of potential losses.

Cyber Risk Quantification

Conducting a cyber risk quantification exercise that extends beyond just a qualitative judgment is critical for any company. Cyber risk quantification capabilities will be key to materiality assessments as part of the SEC 8-K incident disclosures. From this exercise, key stakeholders from XYZ, including the risk manager and chief information security officer, would like to answer the following questions:

- What is the overall level of cyber risk exposure, and which cyber risks pose the biggest threat to XYZ?
- How does the current cybersecurity posture impact cyber risk, and how should security investments be prioritized?
- What would be the financial impact of a large-scale data breach or extended outage of a critical business unit?

To answer these questions and ultimately enable more informed risk financing decisions, we leverage Brown & Brown's Cyber In-Site Quant™. This stochastic modeling framework covers the most common types of cyber loss scenarios, from massive data breaches to minor wire fraud scams. It considers relevant firmographics of XYZ, including the size of the company, its industry, the number of sensitive data records it holds and the state of its security control environment (e.g., Are critical controls such as multi-factor authentication in place?).

Cyber In-Site Quant™

Cyber In-Site Quant™ is Brown & Brown's suite of advanced stochastic loss models for quantifying cyber risk, built on over a decade of historical cyber loss data, rate filings and market pricing research, consultations with incident response vendors and cybersecurity firms, and other proprietary data.

The framework aggregates outputs from various sub-models:

- **Cyber In-Site Data Breach™** quantifies third-party liability costs, associated legal fees and defense costs, and incident response costs such as forensics breach coaches, notifications, and credit monitoring.
- **Cyber In-Site Business Interruption™** simulates various operational downtime events and their associated revenue loss, saved operating costs, system reconstruction from bricking events, and extra expenses.
- **Cyber In-Site Ransomware™** estimates extortion payments and associated incident response costs.
- **Cyber In-Site Fund Transfer Fraud™** estimates the financial impact of fraudulent wire transfers from social engineering attacks and other scams.
- **Cyber In-Site Residual Risk Model™** adjusts a company's cyber risk for its unique cybersecurity control environment and risk exposures, informed by a proprietary weighting system of critical and non-critical controls.

With this information, the framework produces probability distributions of aggregate cyber losses for the prospective policy period (Table 1):

	Percentiles	Return Period	Total Cyber Loss	*Data Breach*	*Business Interruption*	*Ransomware*	*Fund Transfer Fraud*
	99.9	1,000	$362,902,181	*$126,927,304*	*$329,813,962*	*$88,585,665*	*$15,240,608*
	99.8	500	$295,332,661	*$62,486,247*	*$255,911,645*	*$86,919,105*	*$12,668,814*
Typical Range for Insurance Consideration	99.6	250	$165,924,631	*$37,534,258*	*$116,310,535*	*$86,919,105*	*$9,971,026*
	99.4	167	$102,340,234	*$28,069,265*	*$58,230,455*	*$67,640,905*	*$8,669,653*
	99.2	125	$87,317,292	*$20,737,954*	*$27,228,694*	*$50,387,568*	*$7,773,035*
	99	100	$86,919,105	*$16,711,059*	*$14,697,392*	*$37,999,061*	*$7,153,309*
	98	50	$37,120,167	*$8,162,589*	*$299,207*	*$9,251,204*	*$5,101,474*
	95	20	$8,800,651	*$942,715*	*$0*	*$381,797*	*$2,630,516*
	90	10	$3,243,363	*$281,262*	*$0*	*$0*	*$1,165,304*
	75	4	$573,498	*$0*	*$0*	*$0*	*$79,985*
	50	2	$0	*$0*	*$0*	*$0*	*$0*
		Mean	$3,512,853	*$870,945*	*$1,365,281*	*$1,030,273*	*$430,642*

Table 1: Aggregate loss table for cyber risk.

Those familiar with P&C loss model outputs will recognize that return periods, or 1-in-X events, are used to describe the frequency or likelihood of aggregate annual losses exceeding a certain threshold over a specified amount of time, typically a one-year period. The return period provides a simple interpretation of the likelihood of extreme events. A 1-in-100 loss of $86.9M means a 1% (1/100) probability of losses being at least $86.9M or greater over one year. This does not mean a loss of $86.9M will happen only once every 100 years, but rather that a loss of at least $86.9M is expected to occur on average once every 100 years (holding the company's exposure profile constant). Though unlikely, Company XYZ could experience cyber losses exceeding $86.9M multiple times over a 100-year period.

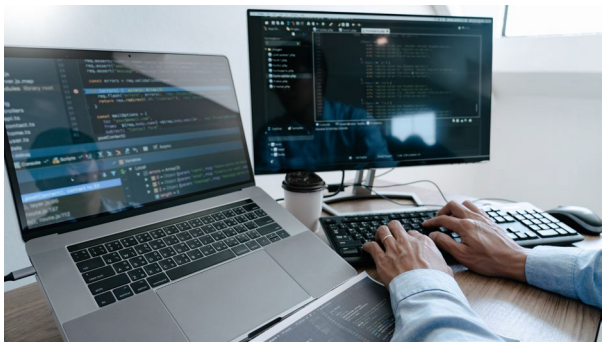
These interpretations enable more informed decision-making around insuring extreme losses. A worst-case scenario data breach involving every record of every XYZ customer that results in large class-action suits and regulatory fines is possible, yet highly unlikely. Stochastic models provide that essential context. It is evident from the table above that ransomware and business interruption are the larger drivers of XYZ's tail risk–at least within the typical range of insurance consideration, a proxy for distress losses. XYZ can leverage this information and the provided stochastic outputs to understand reasonable starting ranges for limits and coverage sub-limits (e.g., XYZ could consider a Fund Transfer Fraud coverage sub-limit between the 100-year and 250-year events, or $7M to $10M) to help design and optimize a cyber insurance program that provides sufficient coverage against catastrophic losses. However, as we will discuss in the next white paper, selecting an optimal risk financing strategy involves more than just a monoline view of risk. Other sources of risk must be quantified first and aggregated into a portfolio view.

Note: The Total Cyber Loss mean is not additive of the individual sub-peril means due to associated incident response cost savings arising from multi-scenario claims

D&O Liability Risk Quantification

For many of the same reasons (see cyber risk quantification section), Company XYZ's risk manager would also like to quantify the risk for D&O. Key stakeholders would like to know the answers to the following questions:

- What is the overall level of D&O risk exposure? Are there particular sources of D&O risk with which the firm should be especially concerned?
- What does the current litigation environment look like? Are there any insights to be gleaned by comparing companies of similar size or in a similar industry?
- What is the impact of a large securities class action or derivative claim? Has the firm purchased enough coverage to withstand these events?

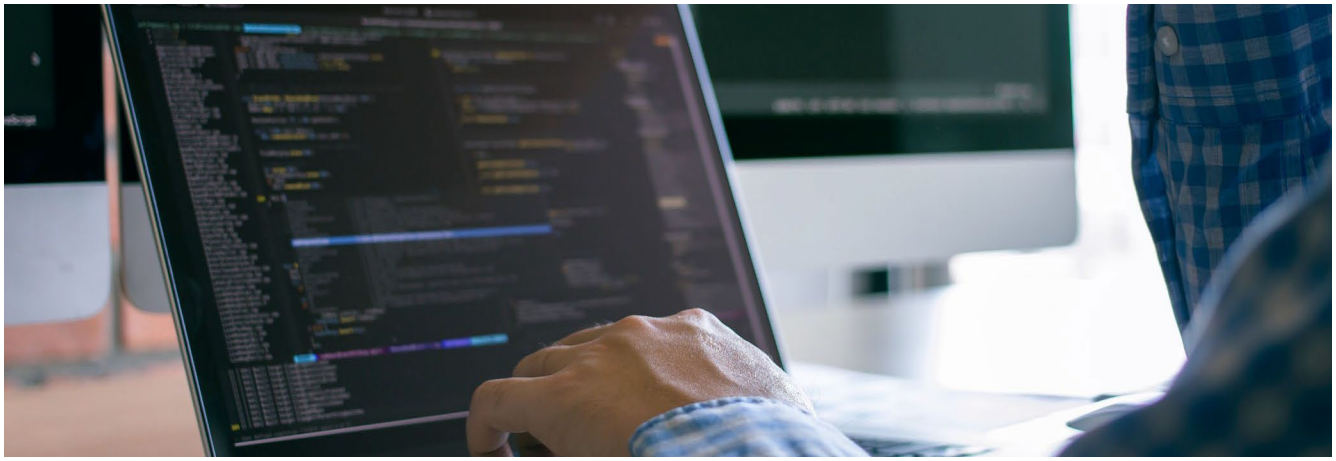


D&O In-Site™

D&O In-Site™ is a stochastic risk modeling platform which applies predictive analytics and other risk assessment techniques to directors and officers liability exposures. The model leverages multiple data sources, including annual financial reports, accounting metrics and ratios, equity market trading activity, and third-party corporate governance scores to forecast prospective policy year customer D&O risk profiles.

The framework aggregates outputs from various sub-perils:

- **Derivative Claims -** Claims against individual directors and officers for which the company is unable or legally prohibited from indemnifying them.
- **Securities Class Action Claims -** Lawsuits filed by investors who bought or sold a company's publicly traded securities within a specific period of time and suffered economic injury as a result of a violation of securities laws.
- **Regulatory Claims -** Claims initiated by a judiciary or regulatory agency.
- **Other Side B/C Claims -** Claims involving Securities Individual Actions, Control Persons violations, books and records demands, proxies and solicitations violations, and Sarbanes-Oxley Act violations.



Like cyber, the firm employs the Brown & Brown D&O In-Site™ model to answer these questions. This model quantifies the frequency, severity and annual aggregate loss estimates for each sub-peril within the D&O peril using information from current financial statements and other publicly available data. Given these inputs for Company XYZ, the model provides an output of annual aggregate losses on a sub-peril basis in Table 2.

	Percentiles	Return Period	Total Loss	*Derivative*	*Securities Class Action*	*Regulatory*	*Other Side B/C*
	99.9	1,000	$192,189,973	*$17,955,066*	*$154,826,684*	*$2,895,713*	*$3,584,242*
	99.8	500	$110,038,120	*$6,828,539*	*$80,081,793*	*$98,339*	*$0*
Typical Range for Insurance Consideration	99.6	250	$47,299,816	*$1,190,641*	*$27,950,518*	*$0*	*$0*
	99.4	167	$23,531,140	*$0*	*$9,192,372*	*$0*	*$0*
	99.2	125	$11,858,017	*$0*	*$1,096,291*	*$0*	*$0*
	99	100	$6,002,331	*$0*	*$0*	*$0*	*$0*
	98	50	$0	*$0*	*$0*	*$0*	*$0*
	95	20	$0	*$0*	*$0*	*$0*	*$0*
	90	10	$0	*$0*	*$0*	*$0*	*$0*
	75	4	$0	*$0*	*$0*	*$0*	*$0*
	50	2	$0	*$0*	*$0*	*$0*	*$0*
		Mean	$990,002	*$89,177*	*$546,034*	*$143,119*	*$211,673*

Table 2: Aggregate loss table for D&O liability.

We can interpret Table 2 in the same manner as the cyber annual aggregate distributions. For example, there is a 99.6% probability that losses from securities class action suits within the next year are equal to or less than $27,950,518. Equivalently, there is a 0.4% probability of securities class action losses in the next year exceeding $27,950,518.

A table such as this one can help answer the first question previously posed, namely, what is the overall D&O risk exposure? We can answer this from the table by looking at the Total Loss column. We can also answer the second part of the first question by observing that the Securities Class Action sub-peril has the largest share of total D&O risk. The second question about comparing Company XYZ against a group of similarly sized peers in their industry can be answered by benchmarking Company XYZ's metrics against their peers. This is another feature of the D&O In-Site™ report. The final question about whether the firm has purchased sufficient coverage will be answered in the final installment of this series.

Portfolio Point of View

With XYZ's individual risks quantified, we now consider its aggregated hazard risk profile. To do this, a dependency or correlation assumption set must be assigned to produce a joint loss distribution. This can be as simple as using a single rank correlation that assumes risks are correlated equally across the entire loss distribution or as complex as fitting a bespoke copula to describe varying correlations across the loss distributions. The latter can be particularly useful for risks exhibiting a high correlation for adverse tail losses but minimal correlation otherwise. In the case of cyber risk and D&O liability, it can even capture the effects of extreme events from one risk (network security breaches) causing the other (shareholder derivative suits).

For our aggregation and subsequent program structure analysis, we consider other risks that XYZ is exposed to (Workers' Compensation, Property, EPL, etc.), leveraging proprietary Brown & Brown joint distributions that best describe the dynamics between each of XYZ's risks.

Simulating joint losses yields the following aggregate distribution:

	Percentiles	Return Period	All Lines	*Cyber*	*D&O*	*Other Lines*
	99.9	1,000	$574,626,637	*$362,902,181*	*$192,189,973*	*$453,024,753*
	99.8	500	$479,543,548	*$295,332,661*	*$110,038,120*	*$353,400,656*
Typical Range for Insurance Consideration	99.6	250	$349,851,467	*$165,924,631*	*$47,299,816*	*$272,347,016*
	99.4	167	$254,034,480	*$102,340,234*	*$23,531,140*	*$219,753,768*
	99.2	125	$228,878,145	*$87,317,292*	*$11,858,017*	*$190,543,862*
	99	100	$220,213,193	*$86,919,105*	*$6,002,331*	*$172,395,664*
	98	50	$135,601,065	*$37,120,167*	*$0*	*$119,074,161*
	95	20	$66,232,013	*$8,800,651*	*$0*	*$64,742,926*
	90	10	$46,396,547	*$3,243,363*	*$0*	*$37,391,534*
	75	4	$22,975,908	*$573,498*	*$0*	*$15,870,959*
	50	2	$12,708,616	*$0*	*$0*	*$6,675,594*
		Mean	$22,348,423	*$3,512,853*	*$990,002*	*$17,845,568*

Table 3: Portfolio view of risk for all lines

As demonstrated previously, imperfectly correlated risks often yield tail diversification benefits when aggregated. Taking the 99.6% Value-at-Risk (VaR) as an example, we quantify the diversification benefit as follows:

$$\textit{Diversification Benefit}_{VaR(99.6\%)} = \textit{VaR(Cyber, 99.6\%)} + \textit{VaR(D\&O, 99.6\%)} + \textit{VaR(Other Lines, 99.6\%)} - \textit{VaR(All Lines, 99.6\%)}$$

$$= \$165.9M + \$47.3M + \$272.3M - \$349.9M$$

$$= \mathbf{\$135.7M}$$

While this diversification benefit is significant, its value remains unrealized unless integrated into a comprehensive risk financing strategy. In the concluding white paper of this series, we delve deeper into how XYZ can harness such insights, translating its portfolio view of risk and the program structuring process into tangible financial value.

About the Author

Caleb Blodgett, *Analytics and R&D Actuary*

Caleb works as a research actuary for Brown & Brown, specializing in cyber risk modeling. Caleb graduated with a Bachelor of Science in Mathematics from the University of Minnesota and is a Fellow of the Casualty Actuarial Society (FCAS).

Thomas Scott, *Analytics and R&D Actuary*

Thomas works as a research actuary for Brown & Brown, specializing in property and D&O risk modeling. Thomas graduated with a Bachelor of Arts in Mathematics from Cornell University and is an Associate of the Casualty Actuarial Society (ACAS).

Brown & Brown

Find Your Solution at BBrown.com
