



WHITEPAPER

## BUILDING A SUPERIOR MODEL FOR CALCULATING RISK


---

### Overview

In a fast-changing world where security and risk management professionals are constantly looking for more effective ways to help business leaders assess and evaluate organizational risk and protect against new and emerging threats, information is currency. The problem is that that currency is often in short supply: current commonly used models and methods for calculating risk have significant limitations and/or structural flaws that limit their utility.

### Challenges

One of the primary challenges facing current models for calculating risk is a pervasive lack of *context*. To perform an accurate and holistic risk assessment, it is imperative to not only understand the threats facing an organization, but also the probability of those threats occurring—and to what degree those threats could impact business objectives. That all-important context is a critically important piece of the security puzzle: the backdrop against which all potential threats can be brought into sharp relief. Natural disasters, cybersecurity issues and economic downturns are all threats that could affect a business, but the potential *impact* of those threats depends, to a large extent, on the location of the business in question and the nature of that business's operations. For example, the underlying logic is clear that a hurricane making landfall at the mouth of the Mississippi will have a disproportionate impact on business operations for organizations in New Orleans more so than organizations in Nashville.



While this straightforward example is fairly intuitive, accurately evaluating organizational risk becomes dramatically more complex and significantly more challenging when the full spectrum of threats is applied, and the contextual complexity of a vast number of regional, industry and company-specific factors are added to the mix. It is clear that a new tool is needed that can account for that complexity and integrate those myriad contextual elements into a reliable model for calculating risk.

## Growing urgency

The need for such a model is clear. At the same time that risk calculations are becoming more complex, the need to accurately perform those calculations is becoming more urgent than ever. The growing importance of information security, combined with an increase in global instability and an uptick in the kind of one-in-fifty-year events that keep CEOs and security professionals up at night, has created a climate of uncertainty for many modern businesses. The increasingly global nature of the world economy, and the emergence of new technologies and increasingly complex international supply chains have created extraordinary opportunities, but they have also introduced complex new risk factors and vulnerabilities. Traditional parameters are changing. Long-held assumptions are being challenged. Whether it is a natural disaster or a precipitous stock market plunge, businesses are understandably worried about their ability to withstand those formerly rare but increasingly prevalent events that can shift the bedrock of an industry or a company in an instant.

## A new approach and a new formula

In the face of these new challenges, Pinkerton has adopted an entirely new way to think about and calculate risk. At a time when forward-thinking security and risk management professionals are beginning to view risk with a new appreciation for context and consequence, Pinkerton has taken it a step further and developed an entirely new risk formula that accounts for those realities. This innovative and potentially transformative approach to enterprise security risk management will not only help decision-makers better understand what risk is and how to measure it, but also appreciate how those measurements can be applied to help them focus their own risk management efforts going forward.

The traditional formula for calculating risk is:


$$\textit{Threat} \times \textit{Vulnerability} \times \textit{Consequence} = \textit{Risk}.$$

Pinkerton's risk formula, that embodies the emerging way to view risk, is:

$$\textit{Threat} \times \textit{Probability} \times \textit{Business Impact} = \textit{Risk}.$$

While the differences between the two might seem fairly modest on the surface, they represent a fairly profound and important shift:

- One change hinges on how to define the very notion of “risk” itself (a term that is all-too-often used interchangeably—and incorrectly—with words like “threat”). Traditional security approaches have generally been effective at identifying threats. In this new way of thinking about and calculating risk, however, risk is defined as *that which prevents an organization from achieving their objectives*. That helps focus in on the specific outcomes organizations are working to mitigate against. Zeroing in from *Consequence* to *Business Impact* is the first



step in crafting a new formula that evaluates threats through the prism of business impact—and strategically aligns risk assessments and subsequent remedies with business goals and objectives.

- Changing *Vulnerability to Probability* is arguably an even more significant shift. In this new formulation, *Vulnerability* should not and does not exist outside of *Threat*: threats should *incorporate* any vulnerabilities that exist. The introduction of probability into the equation is a fairly new and innovative piece of advanced risk assessment. The result is a formula that is a probabilistic expression based on quantitative analysis.

Conducting that analysis requires hard data, however, which is perhaps one of the reasons why probability has not previously been included in traditional risk formulae: the data required to quantify it was vast and variable, and reliable probability metrics were consequently extremely difficult to predict.

## A data breakthrough

Happily, that data is now available in the **Pinkerton Risk Index**, a sophisticated and comprehensive risk assessment tool designed to distill different dimensions of risk into a single in-depth analysis. The Risk Index is the first truly global risk analysis tool: a matrix of threats and potential consequences that is correlated to individual markets, real-world risks and current events.

The Risk Index integrates a wide range of different variables, including specific risk factors, the likelihood of an event occurring, and a comprehensive impact analysis, to provide a detailed picture of business risk (for any business, in any industry, in any part the world). Country-specific and regional considerations range from complex geopolitical calculations to the state of the legal landscape in different nations. Statistically significant correlations connect inherent risks to specific business indices, creating an overall threat analysis tailored for businesses. The Risk Index incorporates threats like natural disasters, infectious disease, population health, violent crime, property crime, terrorism, business operations, supply chain and employee negligence. It also covers technology, information, market and economic risks, including risk factors like economic structure, human capital, social and institutional structures, societal upheaval, and information and technology. A sophisticated spatial analysis of those risks and more results in an overall risk profile that is available on a country level internationally and on a county level in the United States.

All told, the Risk Index integrates 60 different threat vectors divided into five groupings, and, ultimately, four distinct threat categories:

- Hazard & Event Risk
- Operational & Physical Risk
- Technology & Informational Risk
- Market & Economic Risk

Those 60 vectors are based on hundreds of public and private data sources, including decades of insurance data and information from the United Nations, the World Health Organization and a number of other international organizations.



## Probability and utility

The power of a tool like the Risk Index comes from its inherent impartiality: its ability to provide an agnostic expression of inherent threat *irrespective of vulnerability*—which allows security and risk management professionals to assess the probability of those threats impacting business operations. Working with a much larger quantitative data set also yields more comprehensive and subsequently more meaningful conclusions. Facts and figures from the last year or two are not sufficient: a longer-term approach that blends historical trends and new and emerging threats is required.

Critically, this information also makes the new risk **formula** an extremely useful tool: something that provides *clarity* rather than simplicity, and generates actionable intelligence with specific strategic and practical applications. Applying this formula to a client's real-world circumstances allows Pinkerton's security professionals to design a customized enterprise security risk management program that accounts for that client's risk tolerance, operational model and business objectives, as well as the constellation of threats facing their business. It is important to remember that this kind of detailed risk assessment is truly holistic in nature: it inherently encompasses potential *positive* impacts as well as negative outcomes and *opportunities*, as well as potential challenges.

To put the value of this both-sides-of-the-coin approach in context, let us revisit the hurricane example outlined above. The negative outcomes of a major natural disaster like the one described are relatively easy to understand, and are understandably top of mind for risk management professionals responsible for business resiliency or supply chain management in regions susceptible to such storms. But the same hurricane that negatively impacts business continuity for some organizations can potentially positively impact sales growth and new construction development for others. This scenario illustrates how a single event can impact different organizations in profoundly different ways. This dynamic can even be observed *within the same organization* from one department to the next. This reinforces the value of a model for calculating risk that provides a balanced/holistic perspective.

## Conclusion

The good news is that the industry as a whole seems to be moving in the right direction and embracing the ideas expressed in Pinkerton's innovative new risk formula. More businesses and security professionals are beginning to adopt more of a holistic approach to risk assessment and enterprise risk management. Challenges remain, however. The speed with which new threats are emerging makes it extraordinarily difficult to fully understand the features on an evolving threat landscape without the right tools. Recognizing threats and prioritizing protective resources requires a deep and nuanced appreciation for market- and industry-specific factors, and the corresponding ability to evaluate real-world risks in a real-world context. Fortunately, Pinkerton's groundbreaking new risk formula provides the perspective and data needed to do just that. At a time when risk is becoming more complex than ever before, this innovative new approach is a powerful new tool with which to evaluate and mitigate business risk.