To direct investment and manage exposure to loss, organisations need to embrace the unknown by learning how to measure and reduce their uncertainty.

Quantitative techniques provide an arsenal of tools that account for uncertainty, with the potential for accurate measurement of information risk to direct decision making. These techniques have been tested through trial and error in numerous industries – insurance, healthcare, oil and finance – over hundreds of years. They can be used with minimal disruption or increased investment, and with the promise of accumulative value over time.

Adopting a quantitative approach will enable organisations and their teams, from information risk analysts to the board, to:

– reduce uncertainty
– accurately measure information risk
– determine return on investment and prioritise information risk mitigation
– inform effective and meaningful strategic decision making.

The wide-ranging benefits of a quantitative approach empower organisations to articulate their risk in a universal language that resonates with stakeholders across the business.
ISF research identified a number of issues that prevent organisations from extracting value from uncertainty. The ISF Approach for Using Quantitative Techniques in Information Risk Analysis equips organisations to reduce uncertainty through accurately estimating and calculating information risk, helping to direct investment and manage exposure to loss.

<table>
<thead>
<tr>
<th>PROBLEM</th>
<th>THIS REPORT HELPS BY</th>
<th>ISF APPROACH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information risk language is abstract and imprecise, leading to errors and reinforcing biases.</td>
<td>Defining a common lexicon to direct activities throughout information risk analysis.</td>
<td><strong>SCOPE</strong></td>
</tr>
<tr>
<td>Organisations recognise that information risk is often calculated using spurious mathematics.</td>
<td>Providing an information risk calculation that exploits meaningful numbers to deliver robust analytical results.</td>
<td><strong>COLLECT DATA</strong></td>
</tr>
<tr>
<td>Risk is often modelled in a way that masks uncertainty, leading to ineffective decision making.</td>
<td>Providing distribution models that communicate information risk based on accurate estimates and calculations, facilitating cost-benefit analysis.</td>
<td><strong>SIMULATE RISK</strong></td>
</tr>
</tbody>
</table>

**SCOPE** | **SCENARIO**

**COLLECT DATA** | **CALCULATE RISK**

**SIMULATE RISK** | **COMMUNICATE RESULTS**
THE ISF APPROACH FOR USING QUANTITATIVE TECHNIQUES IN INFORMATION RISK ANALYSIS
WHERE NEXT?

Quantitative Techniques in Information Risk Analysis is aimed at those considering, planning, or using a quantitative approach to information risk analysis in their organisation. It equips organisations to gain value from using quantitative techniques in information risk analysis by:

- providing three fundamental techniques that are essential for understanding and undertaking quantitative information risk analysis
- demonstrating how quantitative information risk analysis can be conducted to provide accurate and informative results
- presenting ways in which the results of quantitative information risk analysis can be communicated to support decision making.

Organisations should also consider the ISF resources related to this report including The Standard of Good Practice for Information Security 2018, Information Risk Assessment Methodology 2 (IRAM2), Protecting the Crown Jewels: How to secure mission-critical information assets, Threat Intelligence: React and prepare and Aligning Information Risk Management with Operational Risk Management.

Consultancy services from the ISF provide Members and non-Members with the opportunity to purchase short-term, professional support activities to supplement the implementation of ISF products.

The report is available free of charge to ISF Members, and can be downloaded from the ISF Member website www.isflive.org. Non-Members interested in purchasing the report should contact Steve Durbin at steve.durbin@securityforum.org.

CONTACT

For further information contact:

Steve Durbin, Managing Director
US: +1 (347) 767 6772
UK: +44 (0)20 3289 5884
UK Mobile: +44 (0)7785 953 800
steve.durbin@securityforum.org
securityforum.org

ABOUT THE ISF

Founded in 1989, the Information Security Forum (ISF) is an independent, not-for-profit association of leading organisations from around the world. It is dedicated to investigating, clarifying and resolving key issues in cyber, information security and risk management by developing best practice methodologies, processes and solutions that meet the business needs of its Members.

ISF Members benefit from harnessing and sharing in-depth knowledge and practical experience drawn from within their organisations and developed through an extensive research and work programme. The ISF provides a confidential forum and framework, which ensures that Members adopt leading-edge information security strategies and solutions. And by working together, Members avoid the major expenditure required to reach the same goals on their own.

DISCLAIMER

This document has been published to provide general information only. It is not intended to provide advice of any kind. Neither the Information Security Forum nor the Information Security Forum Limited accept any responsibility for the consequences of any use you make of the information contained in this document.