

RSA Archer® Cyber Risk Quantification

Use case for IT & security risk management

The challenge

With continual changes in technology and rising cyber threats, organizations struggle to translate and understand cyber risks in the context of business risk. Many organizations' current cyber risk management processes are manual, leading to disconnected efforts, ineffective controls or large amounts of data with little value. While implementing layers of IT and security technology, organizations' processes still lag behind, leaving them unable to address the increasing cyber risk the business faces. In addition, IT risk and security teams are struggling to prioritize issues, meet compliance obligations, form a complete picture of cyber risk and make informed decisions.

A key to addressing these challenges is bridging the "gap of grief"—translating IT and security risk into business terms. For IT and security teams to adequately communicate security threats to the business, the business must be able to understand the risk in the context of the business. Most often, cybersecurity is treated as a technical concern, and important business questions such as "Are we doing enough?" and "Are we spending too much or too little?" get unsatisfactory responses, if any.

In today's connected world fueled by the digital transformation, the more digital the business, the less differentiation there is between cyber risk and business risk. As part of their fiduciary responsibility toward shareholders and customers, executives and board members are expected to incorporate cyber risk management as part of the business strategy. Translation of technical risks into business and financial terms adds considerable challenges to already overwhelmed IT risk and security teams.

Overview

RSA Archer® Cyber Risk Quantification quantifies an organization's financial risk exposure to cybersecurity events. The Cyber Risk Quantification use case helps CISOs (Chief Information Security Officers) to prioritize risk mitigation efforts based on business and financial impact, and to communicate the impact of cyber risk in financial terms to senior management and the board. Armed with this financial data, organizations can make more informed decisions regarding their risk and security investments.

RSA Archer Cyber Risk Quantification utilizes a purpose-built platform that leverages the Factor Analysis of Information Risk (FAIR) methodology, the de facto standard for quantitative risk management for IT and cybersecurity risk management. This new use case under the RSA Archer IT & Security Risk Management solution area

Key features

- Built-in risk calibration and analysis engine for cyber risk calculation
- Templated workflow for easy scenario modeling
- On-demand risk analytics for answers to questions on the fly
- Mathematical simulations to build a risk profile with limited data
- Existing loss tables based on industry data
- Easy-to-use SaaS application
- User-friendly interface

Key benefits

RSA Archer Cyber Risk Quantification is designed to help organizations:

- Quantify cyber risk in financial terms
- Visualize the impact of cybersecurity initiatives
- Assess the efficacy of cyber risk programs
- Prioritize top risk-reduction opportunities
- Identify the areas of loss to purchase cyber insurance

provides a set of modular applications to help organizations get started quickly quantifying cyber risk in financial terms, including mathematical simulations to build a risk profile with limited data. RSA Archer Cyber Risk Quantification utilizes a built-in risk calibration and analysis engine, and a templated user interface and workflows provide a user-friendly process for risk data collection and quantification. On-demand risk analytics provides answers to questions on the fly, eliminating the need to create time-consuming and outdated reports.

RSA Archer Cyber Risk Quantification enables businesses to quantify and communicate their cyber risk in the standard business language of money. Armed with the understanding of cyber risk in financial terms, the business can calculate and demonstrate the value of cybersecurity initiatives.

About RSA

RSA offers business-driven security solutions that provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change. For more information, go to rsa.com.

