RSA® Conference 2019

BETTER.

Peer2Peer

Getting Started with a Quantitative Cyber-Risk Program

P2P1-R05: Getting Started with a Quantitative Cyber-Risk Program

Anthony Martin-Vegue Director, Information Security Risk, Informatica

Quantitative risk methodologies have become increasingly common in the Information Security Risk field, and adoption is reaching a tipping point. Risk analysts, the boardroom, government regulators and management alike are recognizing the need for data-driven, evidence-based techniques. The RSAC 2019 Peer2Peer session, *Getting Started with a Quantitative Cyber-Risk Program,* brought together attendees from diverse backgrounds to discuss different methodologies, common models, tips for obtaining executive support and resources on how to get started.

Getting Started with a Quantitative Cyber-Risk Program

This topic proved to be quite popular – the session was full, with a stand-by line outside. Attendees were mostly risk management practitioners, but several auditors, banking regulators and members of senior management were also in attendance. We went around the room for brief introductions, and the level of experience was impressive – some had many years of cyber risk experience, and others were beginners - but all expressed a desire to learn from each other and advance the profession. The reasons for attending followed three general themes:

- Current or aspiring risk managers wishing to broaden their skillset and learn quantitative techniques
- Senior executive and board members seeking to influence their risk programs, and
- Auditors and regulators looking to see where the field is headed so that they can better assess risk programs.

One common theme throughout the session was the sentiment that qualitative risk techniques – expressing risk using colors (red, yellow, green) or adjectives (high, medium, low) – are not adequate for high-stakes decisions and more rigorous methods are required. There is a strong desire for risk reporting that is quantitative; in other words, expressing probability and impact with numbers, while retaining the level of certainty (or uncertainty) about forecasts. This is a quality that softer methods lack, and proves difficult to make some decisions, such as those that require a cost-benefit analysis.

Other topics of conversation included:

- Some participants that successfully implemented quantitative risk programs shared their successes and several tips on how to get started. Several books were mentioned (listed at the end of this post).
- There was a vibrant discussion on different models that are used in cyber risk. Nearly all participants were familiar with Factor Analysis of Information Risk (FAIR), and others used models repurposed from other fields.
- Concern was expressed on how to get executive support, if not already present. Several tips were given, including involving executives very early in the design process, showing risk exposure

reduction in currency alongside security investments and creating visually appealing reports and dashboards.

- Where to get data? This is a common question that many participants asked and some of the more experienced participants chimed in. There is a variety of sources, from external industry reports to internal telemetry from logging sources. A cheap, but effective, data source is conducting structured interviews of subject matter experts to fill in some gaps.
- Attendees shared how they report risk. The methods ranged from fitting quantitative data to heat maps to loss exceedance curves.
- Attendees shared their favorite resources, such as books, conferences, and websites (listed at the end of this post).
- Last, we discussed the skills needed for the risk analyst of tomorrow. It's clear that this field is interdisciplinary, using knowledge from mathematics, economics, psychology and much more.

The following is a list of resources that were mentioned throughout the session:

Groups and Conferences

- Society of Information Risk Analysts (SIRA) and the annual conference
- FAIR Institute; also holds an annual conference

Books

- Measuring and Managing Information Risk: A FAIR Approach by Jack Freund and Jack Jones
- The Failure of Risk Management: Why It’s Broken and How to Fix It by Douglas Hubbard
- How to Measure Anything in Cybersecurity Risk by Douglas Hubbard and Richard Seiersen