A VaR Standard for Cyber and Operational Risk

Veteran information security executive Jack Jones created the FAIR framework and formed an educational institute to promote the modeling discipline, best practices and a collaborative ecosystem

By Jeffrey Kutler

The cyber-attack epidemic has forced a fusion of the information security and risk management disciplines. Jack Jones has specialized in both over a 25-year career that included three chief information security officer (CISO) positions starting in 2000 — at Columbus, Ohio-based companies Nationwide Mutual Insurance Co., CBCInnovis and Huntington Bank.

Jones is currently executive vice president of research and development of cyber risk management software company RiskLens, which he co-founded with president Steve Tabacek. Its Factor Analysis of Information Risk (FAIR) methodology, which Jones began working on in 2001 while at Nationwide, “has emerged as the leading value-at-risk model for cybersecurity and operational risk and as the only international standard,” RiskLens CEO Nick Sanna has noted. FAIR has, for example, been incorporated in efforts of the 500-member information technology standards organization Open Group.

With FAIR as a foundation, and with support from Spokane, Washington-based RiskLens, Jones in February announced the launch of the FAIR Institute, a nonprofit that says its mission is to “establish and promote information risk management best practices that empower risk professionals to collaborate with their business partners on achieving the right balance between protecting the organization and running the business.”

The premise is that there are knowledge and implementation gaps in assessing, quantifying and taking appropriate, proportionate actions on IT and cyber risk exposures.

“FAIR is a framework for measuring risk and organizations’ ability to manage it,” Jones explained in a recent interview. Rather than going the route of “a proprietary secret sauce,” FAIR is an open-standard solution, and FAIR Institute “is a way to create community, share and develop best practices and evolve the standard. It creates an ecosystem to leverage the methodology and help it evolve and grow.”

The technology is a response to “the recent pressure that corporate boards and executive management have placed on IT leadership for better reporting and management of cyber risk,” Sanna said. FAIR Institute is a forum for organizations

and risk professionals to “learn about standard cyber VaR practices and share use cases and real-life experiences.”

Large-Corporate Support

Sanna is the institute’s president, and Jones is chairman. Its board membership indicates the traction it is getting. Directors include former Federal Reserve System CISO Bill Barouski, now senior vice president and deputy CISO of Northern Trust Corp.; Chris Cooper, vice president, operational risk officer, RGA Reinsurance Co.; Alex Hutton, information security and risk executive, Bank of America; and Chris Porter, CISO, Fannie Mae.

The institute also lists three work groups: academics (chaired by San Jose State University lecturer Stephen Mike Jerbic), insurance (Ryan Jones, director of cyber risk intelligence, BMS Group), and operational risk (Evan Wheeler, vice president of operational risk management, Depository Trust & Clearing Corp.).

And there is a “textbook”: *Measuring and Managing Information Risk: A FAIR Approach*, published last year by Elsevier’s Butterworth-Heinemann imprint, co-written by Jones and Jack Freund, senior manager, cyber risk framework at TIAA.

The book is a 2016 inductee in the Cybersecurity Canon, an initiative launched in 2013 by Palo Alto Networks to compile a “hall of fame” of must-reads for cybersecurity practitioners.

Distinct Risk Function

“We may never get to the equivalent of a periodic table of risk, but we need to try,” Freund wrote in his preface. “We need to set stakes in the ground on what truth looks like, and begin to use scientific method to engage each other on those areas where we disagree.”

Freund said one reason for joining Jones, whom he calls a mentor, in writing the book “is because I believe we are on the precipice of something really amazing in our profession. IT risk is really starting to become its own distinct function that is slowly separating from information security proper while simultaneously becoming more intertwined with it . . . . This book is written in part to help fill out the knowledge gap that a lot of people have when faced with a job that is primarily risk-based.”

While laying out a systematic logic in its nearly 400 pages, the book says in its first chapter that FAIR is “not very” complicated. The concepts and ontology are straightforward and not laden with mathematical formulas. When applied to complex problems and environments, FAIR simplifies “by providing a relatively noncomplex lens through which to view and evaluate the complex risk landscape.”

Jones said in his preface: “First and foremost, this is a book about critical thinking.”

Other Frameworks

FAIR is far from the only framing or road-mapping methodology for IT and cybersecurity. *Measuring and Managing Information Risk* mentions such sources as the International Organization for Standardization, ISACA and National Institute of Standards and Technology.

Palo Alto Networks chief security officer Rick Howard, left, congratulates Jack Freund, center, and Jack Jones on the induction of their book, Measuring and Managing Risk: A FAIR Approach, into the Cybersecurity Canon.

The 140,000-member, 47-year-old ISACA offers educational, networking, credentialing and standardization programs including the Cybersecurity Nexus information hub and the 20-year-old COBIT enterprise technology governance framework. In March it acquired CMMI Institute, provider of the Capability Maturity Model Integration performance benchmark, now operating as a separate ISACA subsidiary. (Freund and Jones in their chapter 14, Implementing Risk Management, outline a “FAIR-based risk management maturity model.”)

IT risk and security issues are addressed directly or indirectly in the COSO Enterprise Risk Management Framework, published in 2004 and currently undergoing an update; in programs of the Information Security Forum, a global, multi-industry educational and information-sharing platform founded in 1989; and the recently launched, financial-industry-specific Certificate in Finance and Technology.

“The reality is that cyber risk is not something that can be avoided; instead, it must be managed,” Deloitte experts Mary Galligan and Kelly Rau wrote in a 2015 report, COSO in the Cyber Age. “Using a lens of what data is most important to an organization, management must invest in cost-justified security controls to protect its most important assets.”

The CISSP (Certified Information Systems Security Professional) and other earned designations are common baselines for Freund, Jones and their peers in information security.

According to the Freund-Jones book, existing frameworks can be “quite good” and are “useful for identifying basic risk management programs that are missing or deficient.” They are less useful “in helping the practitioner determine the significance of deficiencies.”

Improvement upon “gaps in coverage,” with an emphasis on risk measurement and analysis — information on loss exposures and options for dealing with them — is FAIR’s intended contribution to better governance, risk and compliance.

“The methodology has been around for more than a dozen years,” Jones underlined. It boils down to “measuring loss exposure” and “analytics to measure an organization’s ability to manage risks over time.”

Culture and Accountability

Persistent cultural challenges have to be overcome.

Jones said he has been witness to “the heads of ERM, audit, security and compliance having four different definitions of risk. That is not managing risk efficiently.”

Jones addressed cyber risk oversight and the CISO’s role in a recent post on ISACA’s Nexus, saying, “the owner(s) of risk (whether cyberrisk or some other form of risk) should be the executive(s) who will end up covering the losses if the risk (a loss event) actually materializes . . .

“The CISO’s proper role in the risk acceptance process is to ensure that the risk owner and other stakeholders clearly understand the amount of risk being accepted, as well as their alternatives (e.g., control opportunities and their expected cost and efficacy). The CISO’s signature on the risk acceptance form should hold him/her accountable for providing accurate and meaningful information to the decision-makers. That signature should not, however, hold the CISO accountable for the business choice that is made.”

Jones added that there will be no perception that “the business will accept any amount of risk” as long as “risk is measured and communicated in terms that are meaningful to executives.”