From: FAIR Institute, Jack Jones
Proposal: 1550 (RIN 7100--AE-61) (Ver 1)- Enhanced Cyber Risk Management Standards
Subject: Enhanced Cyber Risk Management Standards

Comments:

Date: Jan 12, 2017

Proposal: Enhanced Cyber Risk Management Standards [R-1550]
Document ID: R-1550
Revision: 1
First name: Jack
Middle initial: A
Last name: Jones
Affiliation (if any): FAIR Institute
Affiliation Type: Other (Oth)
Address line 1: 601 W. Main Ave
Address line 2: STE 917
City: Spokane
State: Washington
Zip: 99201
Country: UNITED STATES
Postal (if outside the U.S.):
Your comment:

34. What current tools and practices, if any, do covered entities use to assess the cyber risks that their activities, systems and operations pose to other entities within the financial sector, and to assess the cyber risks that other entities activities, systems and operations pose to them? How is such risk currently identified, measured, and monitored?

Comments: A number of large and mid-sized financial services organizations are using FAIR-based (Factor Analysis of Information Risk) methods and tools to evaluate and quantitatively measure cyber risks. This enables them to prioritize with much more granularly than is possible with qualitative measurements. It also makes it possible to understand and communicate the benefit component of a cost-benefit analysis for proposed, in-flight, or completed risk management initiatives. Because these analyses express risk in economic terms, the results are often more meaningful to business executives. Risks in these organizations are identified thru a combination of 3rd party technology (e.g., scanning software), internal and external audits, and internal risk management processes (e.g., risk and control self assessments). Control deficiencies and other concerns identified thru these methods are evaluated using FAIR so that they can be appropriately prioritized. Cost-benefit analysis is then performed on risk mitigation options to help ensure that the organizations are optimizing their resource utilization, and so that management understands the value proposition of these investments. Quantitative risk analysis using FAIR also enables Boards of Directors to set quantitative risk appetites and then govern their organizations within those objectives. It is important to note that achieving this kind of success requires more than a tool or practices;it requires normalizing risk terminology and the mental models of risk management professionals within these organizations. Absent that, no tool or practice is going to be effective in overcoming the confusion and religious debates that surround risk measurement in the complex and dynamic risk landscapes that exist in financial institutions. Adoption of, and training in, FAIR provides this normalized foundation. These organizations have overcome perceptions often believed to be associated with quantitative analysis; e.g., that it can't be done, that it requires too much work, that there isnt enough data, that intelligent adversaries make it impossible to measure risk, etc. Modern risk measurement practices (e.g., calibrated estimation, Monte Carlo, etc.) are designed to account for incomplete and uncertain data, which enables pragmatic analysis of even complicated scenarios in a difficult landscape.

35. What other models, frameworks, or reference materials should the agencies review in considering how best to measure and monitor cyber risk?

Comments: There is some confusion in the industry regarding models and frameworks. In part, this is due to misunderstandings regarding risk measurement. For example, although the NIST CSF provides a good framework for identifying gaps and deficiencies in an organizations risk management program, it does not provide a means of measuring the significance of those findings in real terms (loss exposure levels), which is necessary in order to prioritize or understand the business value of improvements. Furthermore, because relationships between the elements in NIST CSF (and similar checklists) are not accounted for in those frameworks, dependencies and overlaps arent recognized. For example, NIST CSF correctly includes both logging and monitoring as important capabilities. The framework does not, however, capture the fact that those two elements are dependent on one another; i.e., if you have one but not the other, then the one that is in place is hamstrung in terms of its value. In other words, checklist frameworks are not analytic measurement models. As a result, the significance of any perceived deficiencies are dependent on some other means of measurement. In most organizations, this boils down to someone applying a qualitative and subjective high/medium/low risk rating. The accuracy of these ratings is largely dependent on the skills and experience of the professional who makes them. Unfortunately, most risk management professionals although skilled in common practices and specific subject matters are operating from their personal uncalibrated mental models of risk and are not trained to analyze or measure risk. At this time, FAIR is the only broadly recognized and widely used quantitative risk analysis model. It is often referred to as a framework because using the model involves methods beyond the basic FAIR ontology. Note that agencies should consider requiring that personnel who measure cyber- and technology-related risk be trained in, or at least familiar with basic risk analysis methods (e.g., scoping scenario-based analyses, making calibrated estimates, basic understanding of probability concepts, limitations of qualitative measurements, etc.). Resources for this include:The Open Groups Open FAIR materials and professional certification (www. opengroup .org/security) Materials offered thru the FAIR Institute (www. fairinstitute.org; How to Measure Anything (by D. Hubbard) How to Measure Anything in Cybersecurity Risk (by D. Hubbard) Measuring and Managing Information Risk: A FAIR Approach (by J. Freund & J. Jones) The FAIR Institute is a non-profit organization with over 800 members from around the globe, many of whom work for major financial institutions like Bank of America, PNC Bank, etc. The FAIR Institute provides a forum for cyber, technology, and operational risk management professionals to evolve and share best practices regarding the adoption and use of FAIR in quantitative risk analysis. It is also important to recognize that Carnegie Mellons Goal-Question-Indicator-Metric approach, although excellent for risk-related metrics, does not measure risk. Unless used in conjunction with a risk measurement method like FAIR, GQIM metrics themselves lack an explicit loss exposure context that is needed in order to understand the significance of the metrics.

36. What methodologies should the agencies consider for the purpose of measuring inherent and residual cyber risk quantitatively and qualitatively? What risk factors should agencies consider incorporating into the measurement of inherent risk? How should the risk factors be consistently measured and weighted?

Comments: In most (if not all) cyber-related contexts, inherent risk can not be reliably measured using methods that are common today (refer to this article for an explanation of why this is true, and an alternative approach; http ://www. fairinstitute .org/blog/using-the-fair-model-to-measure-inherent-risk). Unless the agencies consider adopting an alternative approach like that described in the article, attempting to quantitatively measure inherent risk is likely to result in confusion (at best) and poorly informed decision-making. Weighted values should be avoided for risk analysis because they are highly context dependent. For example, an argument could be made that authentication should be weighted higher than logging under the premise that an ounce of prevention. Placing a greater emphasis on authentication would NOT be appropriate however, if the threat actor legitimately had authorized access to the assets of concern. In other words, if the bad actor is an insider with legitimate access, then logging is the more important control. The bottom line is that weighting schemes can not be pragmatically and reliably applied to the myriad scenario types prevalent in the cyber space.

37. What are the potential benefits or drawbacks associated with each of the options for implementing the standards discussed above?

Comments: The first option offers greater flexibility to organization in how they align with regulatory expectations. Although flexibility can be a good thing, the downside is that organizations will often take the path of least resistance and simply tweak the practices they are familiar with today, but that are not effective. This would enable checking the compliance box without meeting the regulatory intent. The second option could drive organizations to meaningfully evolve their risk management practices, while allowing some degree of flexibility and minimizing the potential for guidance that paints organizations into a risk management corner. It also can set the stage for more specific guidance as the industry evolves its understanding of, and approach to, mature risk measurement practices. The third option reduces the potential for organizations to put lipstick on pigs but has the greatest potential for institutionalizing ineffective practices if the requirements being set forth are highly specific and fundamentally flawed in some manner. Because there are a lot of misperceptions and ineffective practices regarding quantitative risk analysis, the agencies must be very careful about any highly specific requirements they define. A potential option is to be very specific about some basic and relatively clear requirements, and more general about those that are less well understood. For example, the agencies could require organizations to: Normalize their risk terminology and risk models. Organizations could accomplish this by adopting an established standard (e.g., FAIR) or by defining their own. If defining their own, more specific guidance could exist regarding characteristics of the terminology and models being used. Ensure that anyone responsible for measuring risk (either quantitatively or using qualitative terms) has been trained in analysis principles, techniques and tools, without specifying which techniques and tools are required. Ensure processes are in place to periodically review risk analyses to ensure that risk measurements/ratings stand up to careful scrutiny, Leverage well-established methods (e.g., Monte Carlo) when performing quantitative risk analysis. Use risk measurement and reporting methods that faithfully represent the level of certainty in risk measurements (which is another benefit of using methods like Monte Carlo that produce output as distributions). These relatively general requirements would allow organizations to choose their approaches and yet not stray into methods that are fundamentally flawed (e.g., performing math on ordinal risk measurement scales).

38. What are the trade-offs, in terms of the potential costs and other burdens, among the three options discussed above? The agencies invite commenters to submit data about the trade-offs among the three options discussed above.

Comments: Organizations that take risk measurement seriously will incur greater costs in terms of specialized risk analyst personnel and toolsets. These organizations also sometimes incur initial political costs that come from requiring that everyone normalize their use of terminology and the mental and formal models being used to measure risk. These costs are invariably compensated for by greater cost-effectiveness due to improved prioritization and by understanding the benefit (or lack thereof) of proposed risk management improvements.

39. Which approach has the potential to most effectively implement the agencies expectations for enhanced cyber risk management?

Comments: This depends on the agencies goals, their willingness to research deeply, and their tolerance for backlash. If the agencies are interested in driving major improvements into the financial industry quickly, then the third option has the greatest chance for success as long as the regulatory expectations are carefully researched and clearly defined. Note, however, that this approach is also likely to generate the most resistance from organizations that resist change and that have an immature understanding of modern risk measurement practices. For this reason, the agencies should seek out organizations and individuals who are on the leading edge of risk measurement, rather than those who cling to old methods. By understanding the facts regarding newer methods from those who have successfully applied them, the agencies will be able to make informed decisions about what is pragmatic to expect from the industry in the near-term, and what to set as longer-term expectations.