Evolving Cyberrisk Practices to Meet Board-level Reporting Needs

Imagine being an executive sitting on the board of directors for an organization. Of the following two risk report statements, which one would likely be more meaningful and useful?

1. The current deficiency in control X represents a high level of risk. By spending US $400,000 to implement technology Y, the organization will bring control levels into alignment with best practice and reduce the potential for significant loss.
2. The current deficiency in control X represents an annualized loss exposure of US $22 million. By spending US $400,000 to implement technology Y, the organization can reduce this exposure to US $4 million. The risk reduction benefit is represented visually in **figure 1**.

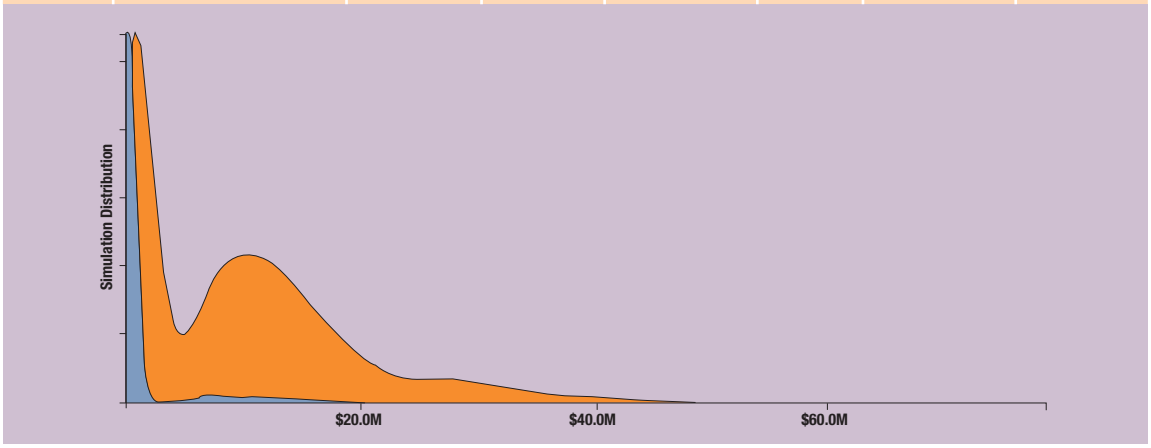
For most executives, the second statement and its visual representation will be more meaningful and more useful, because it helps them to clearly understand the financial benefit and risk reduction of a proposed investment.

Changing the Conversation

As a profession, cyberrisk and security practitioners have dreamed of the day when boards would take a greater interest in cyber and technology risk. For

Figure 1—Loss Exposure Distribution

	Analysis	Period	Minimum Loss	10th Percentile of Simulation Results	Average Loss	90th Percentile of Simulation Results	Maximum Loss
	Current State	Q1 2016	$25k	$200k	$9M	$22M	$80M
	With Additional Control	Q3 2016	$2.5k	$15k	$1M	$4M	$32M



Source: J. Jones. Reprinted with permission.

Jack Jones, CISA, CRISC, CISM, CISSP
Is chairman of the FAIR Institute, executive vice president of research and development for RiskLens Inc., and serves on the (ISC)² Ethics Committee. In his more than 30 years of experience in the industry, he has served on the ISACA® Risk IT task force, helped to launch ISACA's CRISC™ program, and been a chief information security officer for three companies. Jones received the Information Systems Security Association Excellence in the Field of Information Security Award in 2006 and the CSO Compass Award for his leadership in risk management in 2012. The book he wrote with Jack Freund, *Measuring and Managing Information Risk: A FAIR Approach*, was inducted into the Cybersecurity Canon in 2016.

many organizations, that day has arrived, and with it has come a new challenge—how to communicate effectively with that executive audience. Vulnerability statistics and malware infection numbers simply are not meaningful to senior executives, nor are risk measurements that give precisely ambiguous values, like 3.4. At the other end of the spectrum, qualitative risk ratings (high, medium, low) and heat maps are inherently imprecise and subjective. As a result, today's typical reports do not provide answers to important questions senior executives are concerned about, such as:

- Is a proposed risk reduction initiative likely to be worth the cost? (For example, is it similar to the quantitative example described at the beginning of this article?)
- How much more risk will the organization incur if it does x, y or z?
- How much risk does the organization have overall?
- Is the organization focusing on the most important things?
- What benefit has the organization gotten from its past risk management investments?

Figure 2 displays an example of how to answer the question in the last bullet point. Specifically, it shows the historical aggregate change in organization risk at the 90th percentile, average and 10th percentile, quarter over quarter. This helps to illustrate the progress an organization has made over time. In addition, it can illustrate the effect that events such as an acquisition, major technology changes and control improvements have had on the organization.

Clear, meaningful answers to these questions can fundamentally change the conversations between cyberrisk professionals and senior executives.

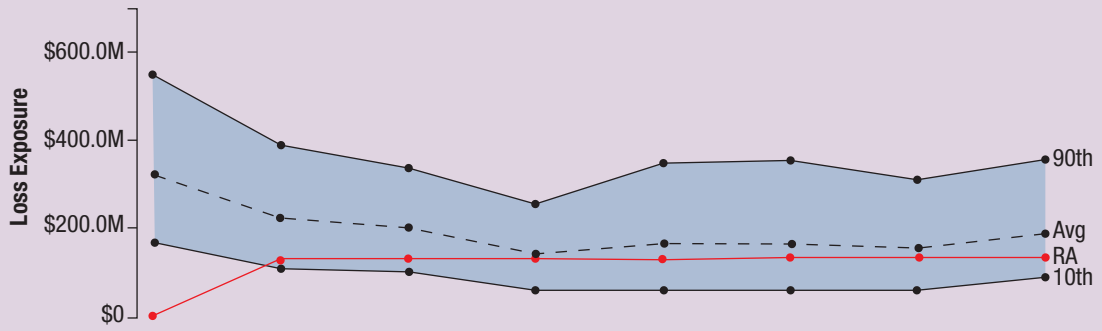
> **"Unless metrics like these are evaluated and communicated in terms of the loss exposure they represent, their interpretation is entirely subjective and too easily misunderstood."**

Metrics

Commonly reported metrics in board reports include things such as:

- Patching compliance levels

Figure 2—Aggregate Risk Trend Report



Note: The red line represents an organization's defined risk appetite.

Source: J. Jones. Reprinted with permission.

- Audit findings
- Employee security awareness levels
- Progress on security initiatives

And although this is good information for management, senior executives have no way to understand how much any of that information matters from a business perspective. For example, how much should they care that employee awareness levels are only at 95 percent vs. 99 percent, or 100 percent, for that matter? Unless metrics like these are evaluated and communicated in terms of the loss exposure they represent, their interpretation is entirely subjective and too easily misunderstood. If, instead, the board could be told that the difference in annualized loss exposure between 95 percent awareness and 99 percent awareness is roughly US $500,000, then they would be able to understand whether to be concerned about it. Maybe an exposure of US $500,000 makes it something about which to care. If, on the other hand, the additional exposure associated with 95 percent awareness vs. 99 percent is only US $5,000, then a) it is unlikely the issue would be taken to the board, or b) if the analysis was taken to the board, the board would probably decide not to worry about it.

The benefit is that with risk-based financial quantification, it is possible to leverage common metrics appropriately and meaningfully at an executive level.

Challenges of Quantitative Risk Measurement

Today, the common approach to measuring cyberrisk is the analytic equivalent of sticking a wet finger in the air to determine which way the wind is blowing. There is a heavy reliance on the mental models of individual practitioners, limited use of data and inherently imprecise ordinal scales (e.g., high/medium/low, red/yellow/green, 1 through 5 scales). Although this may be fine for quick-and-dirty triage assessments, it simply cannot answer the strategic business questions listed earlier.

The good news is that the required frameworks, methods and technologies to derive those answers are available today. For example, the open standard Factor Analysis of Information Risk (FAIR) framework was developed specifically to answer these questions. Combined with other well-established elements, e.g., estimate calibration and tools that support Monte Carlo functions, leading organizations are already performing these kinds of quantitative risk analyses.

“The benefit is that with risk-based financial quantification, it is possible to leverage common metrics appropriately and meaningfully at an executive level.”

The not-so-good news is two-fold:

- There is resistance to change within the industry.
- There is a skills shortage.

Enjoying this article?

Learn more about, discuss and collaborate on risk management in the Knowledge Center. *www.isaca.org/risk-management*

Often, change of any sort is not a welcome prospect. Adopting something commonly believed to be impossible or impractical is all the more unwelcome. Therefore, the first priority is overcoming the prevalent misconceptions surrounding quantitative risk analysis.

The organizations already leveraging these next-generation quantitative methods are struggling to find qualified staff. As if it is not difficult enough to recruit experienced cyber and technology risk professionals, finding those who have the requisite critical-thinking skills, comfort with numbers and grounding in basic probability principles makes staffing significantly more challenging. This deficit represents an opportunity for professionals who want to break into a burgeoning new field.

The Bottom Line

Now that senior executives have begun to take a serious interest in cyber and technology risk, it is necessary to provide meaningful and useful answers to the questions they are beginning to ask. To do that, the cyberrisk and security profession has to evolve.

References

Hubbard, Douglas W.; *How to Measure Anything: Finding the Value of "Intangibles" in Business*, Wiley, USA, 2014

Jones, J.; J. Freund; *Measuring and Managing Information Risk: A FAIR Approach*, Butterworth-Heinemann, USA, 2014

The FAIR standard and professional certification, The Open Group, *www.opengroup.org*

The FAIR Institute, *www.fairinstitute.org*