CISO Cross-Industry

Expert Exchange

Q3 Executive Summary
July 11, 2023

kyndryl™

Overview

In this Expert Exchange session, several CISOs convened to discuss the topics around Risk Quantification. The agenda was determined based on mutual interest through advance interviews with participants.

Hosts

Michael Restivo
US Sales Vice President, Security and Resiliency, Kyndryl

John Feezell
Associate Director, Security Consulting, Quantitative Risk Lead, Kyndryl

Key Topics

Risk Quantification

- Calculating cyber risk in numerical terms is becoming increasingly popular, but some firms are not willing to divulge information about how their numbers are generated. Proprietary algorithms and black boxes are difficult to justify across organizations that take cybersecurity seriously, even when people do want to quantify cyber risk. CISOs must ensure they are quantifying risk using an open and defensible standard methodology to promote confidence in the process.

- The group discussed the Open FAIR [Factor Analysis of Information Risk] risk assessment methodology, from The FAIR Institute, which standard is globally managed by the Open Group. As John Feezell, Kyndryl Associate Director, Security Consulting — Quantitative Risk Lead, noted, sometimes there is no calculator involved when using FAIR. Although it can crunch the numbers when needed, FAIR is a mental model, a critical thinking approach that allows cybersecurity leaders to decompose otherwise complex issues into more manageable pieces, more accurately considering existing controls and assets within that decomposition.

- Quantifying cyber risk may run into cultural barriers around the understanding of risk. If there's a value put on it, people may think such a calculation is for a finance group, not a risk group. In other instances, convincing people that risk calculations can be made in less tangible areas like information security can be difficult. Even using the FAIR model does not guarantee that groups will understand it, meaning that some translation may need to be made before going to that audience.

- CISOs must start small and prove the value to overcome resistance to a risk model. Once this "beachhead" is established, the security team has a place of value and success from which they can further build a risk assessment model.

"Risk is a quantity—we express risk in financial terms when we're talking about CRQ [cyber risk quantification]. And so just a number, or use of a subjective ordinal scale is not CRQ; it's got to be based on real data or calibrated estimates, in financial terms, and time-bounded. So there needs to be a loss event frequency associated with that and the loss magnitudes. And then we start to decompose those."

— John Feezell, Kyndryl host

Risk Assessment Approaches

- There are competing camps for cyber risk assessment: Quantitative, and qualitative. The challenge for leadership is getting the different sides to speak the same language. The Open FAIR standard provides the necessary lexicon of terms. The strategy should be planting the seed for finding a common approach that can acknowledge the usefulness of the many forms that risk analysis takes.

- When calculating risk, there's great value in gathering data. A useful exercise is scraping for information and then working with subject matter experts to calibrate estimates. It's not about finding a single figure; it's about finding a reasonable range. An example is how often a website gets probed and hit for cross-site scripting. The numbers are seldom the same, but a reasonable range can be determined with some review, forming the risk calculation.

- Standardized approaches for cyber risk assessments continue to emerge. The National Association of Corporate Directors has published a scorecard that includes questions that corporate directors should ask. The final score follows a summary of where the organization might be on specific cyber risks. The scorecard is very high level and may not have enough detail, but it is a good starting point for further assessment.

- There are also resources available to guide assessment approaches. Books such as How to Measure Anything in Cybersecurity Risk and Jack Jones' Measuring and Managing Information Risk have proven useful in developing a strategy for quantifying risk.

"A challenge that I've faced is trying to compare apples and oranges or roll them up into some kind of overall risk score. For example, if you have an employee click rate, you've also got a percentage of systems with a critical exploitable vulnerability, right? How do you roll up those two separate things into an overall cyber risk score for leadership?"

— CISO Expert Exchange member

Talent Considerations

- Running a security organization requires people with the right skills. Organizations need people who understand risk; if they can't hire these, they will need to build up people internally. Often, the process and the tools exist, it takes the right people to understand and implement a risk approach. Those people can sometimes feel as scarce as "hen's teeth."

- Information security leaders are pressured to give raises, especially with recent wage inflation and the risk of people leaving for other jobs. This risk of attrition factors into development decisions since those who get extra training are better qualified for other jobs and opportunities. However, this risk can be offset through incentivized training programs that offer retention awards—such awards may not be a monetary raise but serve recognition of people choosing to grow their skills.

"You've got to have somebody that actually understands cyber and knows how to do the job. And if you don't, you either have to hire it, or you have to build it, and to do either you need to have resources available. Someone internally has to have the gumption and desire and the capability to actually get into that and really get through it. And that's not the easiest thing in the world."

— CISO Expert Exchange member

Working with Leadership

- Many CISOs face the challenge of communicating and positioning risk to senior leadership and the board in a way that helps them understand and adopt what's needed to move security programs forward. The best way to lead as a risk professional is to build a culture where executives and the corporate board ask their questions about cyber risk. Building such a culture requires collaboration—the security teams cannot do this alone without bringing in other stakeholders.

- Being at the same company for a long time and having relationships can help CISOs gain the trust of their organization's leadership. The industry also matters, as does the business. Some businesses have slim margins—the smaller the margins, the more aware of risks the company will be, and cyber has very high downside risks.

"You've got to be very, very cautious and careful about how much you try and consume, and how much you try and push through the organization, and how fast you try and push it through the organization."

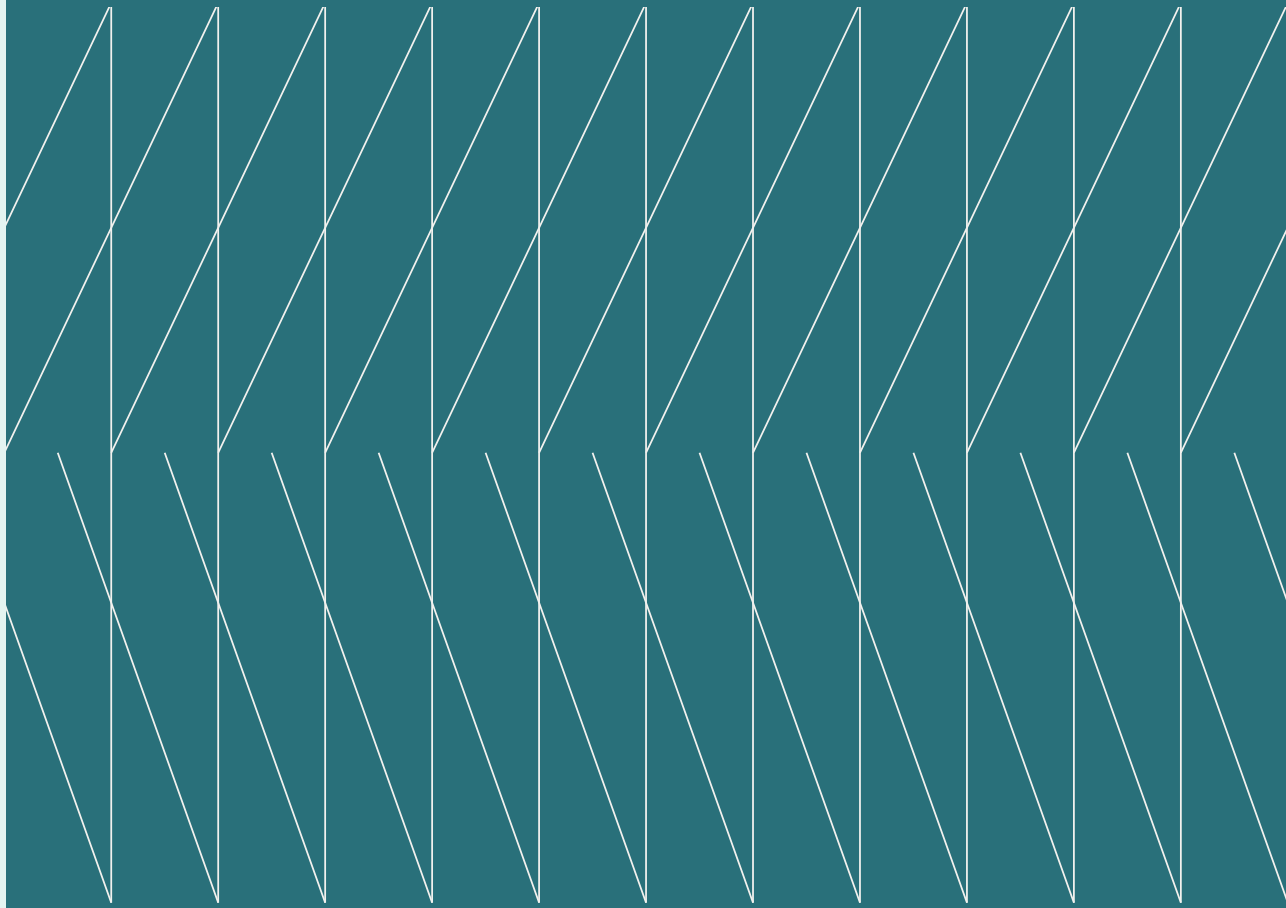
— CISO Expert Exchange member

Cyber Resilience Maturity Assessment

Learn more →

kyndryl™

The Expert Exchange is hosted by Kyndryl, Inc. Please contact Mike Restivo or John Feezell with any questions about Kyndryl or the CISO Cross-Industry Expert Exchange.



08-17-2023