IN-PERSON

IAN AMIT
Managing Partner, Security & Innovation

Going FAIR, Works Wonders

Ian Amit, Managing Partner at Security & Innovation, Israel spoke to Dominic K on the FAIR Risk Management Framework and what can CISOs expect out of it to analyse and manage enterprise risk.

Q What is FAIR Risk Management Framework all about?

FAIR or Factor Analysis of Information Risk has been created as a platform for security professionals to be able to articulate what they should have been practicing for a long time, in a more concise and business oriented way. As veteran security practitioners, we have been using FAIR without realising it, ever since we moved on from the simple hack-and-patch cycle and the technical vulnerability game to the more practical business implications of such technical elements.

Q What are the various aspects and benefits Indian enterprises can expect post FAIR management framework implementation?

First off – once the information risk and threats are mapped and measured, an organisation can more easily manage such risks – not only on the technical information security aspect, but also on operational levels and maintenance. Furthermore, as using such a methodology for quantifying and analysing risk is not a one-off effort, FAIR enables users to keep track and measure the effectiveness of security investments over time. This puts businesses at an advantage position when making decisions in terms of choosing one solution over another, and renewing licenses for products purchased before such a quantifying process has been initiated. Surprisingly, most businesses find that after implementing a more coherent risk management framework, their security spending is reduced, while increasing their security level as risks are controlled much more tightly.

Q What are the best practices for CISOs to follow if they were to go ahead with FAIR framework?

I would suggest that CISOs should adopt a more business-oriented approach to managing their risks. The current situation is more often reliant on technologies, vulnerabilities that show up on various platforms and general risks that may or may not have a direct impact on specific organisations. My best advice would be to start mapping out the business assets that the organisation is most reliant on and that are the organisation's "crown jewels", and experiment with trying to figure out how much a loss of such an asset would cost the organisation. At that point I would also get the marketing, sales, and legal entities in the business to pitch in, in order to get the full impact of such an event. This small exercise will enable the CISOs to see the security measures already deployed in the business in a different light, as they are now able to more quantifiably compare the investment in such measures to the value of an asset.

Implementing the framework is a business enabler from my experience, and I have had a chance to see businesses realise actual value from using it. CSO