WIKIPEDIA

Factor analysis of information risk

Factor analysis of information risk (**FAIR**) is a taxonomy of the factors that contribute to risk and how they affect each other. It is primarily concerned with establishing accurate probabilities for the frequency and magnitude of data loss events. It is not a methodology for performing an enterprise (or individual) risk assessment.[1]

FAIR is also a risk management framework developed by Jack A. Jones, and it can help organizations understand, analyze, and measure information risk according to Whitman & Mattord (2013).

A number of methodologies deal with risk management in an IT environment or IT risk, related to information security management systems and standards like ISO/IEC 27000-series.

FAIR seeks to provide a foundation and framework for performing risk analyses. Much of the FAIR framework can be used to strengthen, rather than replace, existing risk analysis processes like those mentioned above. It is not another methodology to deal with risk management, but complements existing ones. It is in direct competition with the other risk assessment frameworks, if complementary to many of them.[1]

Although the basic taxonomy and methods have been made available for non-commercial use under a creative commons license, FAIR itself is proprietary. Using FAIR to analyze someone else's risk for commercial gain (e.g. through consulting or as part of a software application) requires a license from RMI.[2]

Contents

Adoption

As a standards body, The Open Group aims to evangelize the use of FAIR within the context of these risk assessment or management frameworks.[1]

ISACA cites FAIR and its concepts in its Risk IT Framework that extends COBIT.

The Build Security In initiative of the United States Department of Homeland Security cites FAIR.[3]

Documentation

FAIR's main document is "An Introduction to Factor Analysis of Information Risk (FAIR)", Risk Management Insight LLC, November 2006;[4]

The contents of this white paper and the FAIR framework itself are released under the Creative Commons Attribution-Noncommercial-Share Alike 2.5 license. The document first defines what risk is. The Risk and Risk Analysis section discusses risk concepts and some of the realities surrounding risk analysis and probabilities. This provides a common foundation for understanding and applying FAIR. The Risk Landscape Components section briefly describes the four primary components that make up any risk scenario. These components have characteristics (factors) that, in combination with one another, drive risk. Risk Factoring begins to decompose information risk into its fundamental parts. The resulting taxonomy describes how the factors combine to drive risk, and establishes a foundation for the rest of the FAIR framework.

The Controls section briefly introduces the three dimensions of a controls landscape. Measuring Risk briefly discusses measurement concepts and challenges, and then provides a high-level discussion of risk factor measurements.

Main concepts

FAIR underlines that risk is an uncertain event and one should not focus on what is possible, but on how probable is a given event. This probabilistic approach is applied to every factor that is analysed. The risk is the probability of a loss tied to an asset.

Asset

An asset's loss potential stems from the value it represents and/or the liability it introduces to an organization.[4] For example, customer information provides value through its role in generating revenue for a commercial organization. That same information also can introduce liability to the organization if a legal duty exists to protect it, or if customers have an expectation that the information about them will be appropriately protected.

FAIR defines six kind of loss:[4]

1. Productivity – a reduction of the organization to effectively produce goods or services in order to generate value
2. Response – the resources spent while acting following an adverse event
3. Replacement – the expense to substitute/repair an affected asset
4. Fines and judgments (F/J) – the cost of the overall legal procedure deriving from the adverse event
5. Competitive advantage (CA)- missed opportunities due to the security incident
6. Reputation – missed opportunities or sales due to the diminishing corporate image following the event

FAIR defines value/liability as:[4]

1. Criticality – the effect on the organization productivity
2. Cost – the bare cost of the asset, the cost of replacing a compromised asset
3. Sensitivity – the cost associated to the disclosure of the information, further divided into:
    1. Embarrassment – the disclosure states the inappropriate behaviour of the management of the company
    2. Competitive advantage – the loss of competitive advantage tied to the disclosure
    3. Legal/regulatory – the cost associated with the possible law violations
    4. General – other losses tied to the sensitivity of data

Threat

Threat agents can be grouped by Threat Communities, subsets of the overall threat agent population that share key characteristics. Threat communities must be precisely defined in order to effectively evaluate effect (loss magnitude).

Threat agents can act differently on an asset:[4]

- Access – read the data without proper authorization
- Misuse – use the asset without authorization and or differently from the intended usage
- Disclose – the agent let other people to access the data

- Modify – change the asset (data or configuration modification)
- Deny access – the threat agent do not let the legitimate intended users to access the asset

These actions can affect different assets in different ways: the effect varies in relationship with the characteristics of the asset and its usage. Some assets have high criticality but low sensitivity: denial of access has a much higher effect than disclosure on such assets. On the other hand, an asset with highly sensitive data can have a low productivity effect if not available, but embarrassment and legal effect if that data is disclosed: for example the availability of former patient health data does not affect a healthcare organization's productivity but can cost millions of dollars if disclosed. [5] A single event can involve different assets: a [laptop theft] affects the availability of the laptop itself but can lead to the potential disclosure of the information stored on it.

The combination of an asset's characteristics and the type of action against that asset that determines the fundamental nature and degree of loss.

See also

- Information security management
- ISACA
- ISO/IEC 27001
- Risk management
- Vulnerability (computing)

Notes and references

1. Technical Standard Risk Taxonomy ISBN 1-931624-77-1 Document Number: C081 Published by The Open Group, January 2009.
2. "Frequently Asked Questions" (https://web.archive.org/web/20131030003951/http://www.cxoware.com/resources/faq-2/). *CXOWARE*. October 30, 2013. Archived from the original (http://www.cxoware.com/resources/faq-2/#open) on 2013-10-30.
3. https://buildsecurityin.us-cert.gov/bsi/articles/best-practices/deployment/583-BSI.html
4. "An Introduction to Factor Analysis of Information Risk (FAIR)", Risk Management Insight LLC, November 2006 (http://www.riskmanagementinsight.com/media/docs/FAIR_introduction.pdf)
5. CNN article about a class action settlement for a Veteran Affair stolen laptop (http://www.cnn.com/2009/POLITICS/01/27/va.data.theft/index.html)

External links

- Risk Management Insight (http://www.riskmanagementinsight.com)
- FAIR Basic Risk assessment guide (http://www.riskmanagementinsight.com/media/docs/FAIR_brag.pdf)
- Patent application (http://www.freepatentsonline.com/y2005/0066195.html)