FAIR vs. Squalify: A Decision-Maker’s Guide to Cyber Risk Methodologies

The Case for Business-First Cyber Risk Quantification

AS SEEN IN

Forbes yahoo!finance CYBER DEFENSE MAGAZINE Cybersecurity INSIDERS

SQUALIFY

Squalify - Cyber Risk Quantification for the Boardroom
www.squalify.io

Executive Summary

A question that we get asked a lot is: **"Squalify is doing cyber risk quantification (CRQ), you must be using the FAIR methodology, right?"**

When we explain that **"no, Squalify doesn't use FAIR"** we get met with looks of curiosity, surprise, and scepticism. And sometimes relief.

"OK so how does Squalify do it then?" is the question that quickly follows.
This Whitepaper answers that question.

Unlike FAIR-based tools, Squalify uses a proprietary methodology to quantify cyber risk based on over a decade's experience of cyber insurance pricing and underwriting from our parent company Munich Re.

Combined with our unique historic dataset of cyber events and associated losses, this gives Squalify users many benefits over FAIR:

- We leverage historic cyber incident data from more than 100.000 companies
- Focus on aggregation of risk assessment at company level makes reporting on the "big picture" much simpler.
- Scenario-based approach eases executive level storytelling.
- Greatly simplified estimation of key quantification parameters.

This guide explains in detail how the various components from FAIR relate to Squalify's own quantification methodology.

It can be used by FAIR users to quickly assess how existing work under FAIR can be reused, how Squalify simplifies some aspects of CRQ, and ultimately the pros and cons of each methodology.

This guide is structured as follows:

- First, the core principles of the FAIR and Squalify methodologies are compared. Squalify shares many of the same principles with FAIR, and as such FAIR users will quickly feel familiar with the Squalify approach.
- Next, the input parameters of FAIR are discussed, and we walk through how Squalify approaches each of those concepts in its model. Some parameters can be easily reused from FAIR, some parameters are made easier to estimate in Squalify, and some parameters from FAIR are not needed in the Squalify model.
- Finally, the overall pros and cons of each methodology are summarized and compared to help you decide which approach is best suited for your needs.

FAIR vs Squalify: Principles

What does Squalify have in common with FAIR?

The FAIR and Squalify methodologies have many principles in common that make the Squalify approach familiar for FAIR users:

- **Clearly understand & describe the loss event**: the "loss event' in Squalify terms is a Consequence Scenario, a scenario describing in non-technical language the *consequences* (or primary and secondary losses in FAIR language) of a cyber event. This could be interruption to the business, for example ransomware causing an outage at a factory, a breach of personal data, or financial theft and fraud.

- **Start with the absurd**: in the Squalify approach, you start by identifying Worst- Case Scenarios. These are far-fetched scenarios where almost all controls are assumed to have failed which stretch credibility but provide an upper bound to estimating costs and durations. From the Worst-Case Scenarios, assumptions are identified and tested to define the realistic Consequence Scenarios.

Focus on accuracy rather than high precision: as with FAIR, Squalify users should approach quantification with a mindset of identifying inputs in the right ballpark rather than extreme precision. Squalify provides a set of questions for common Consequence Scenarios to make it easier to identify the relevant input data.

Consider where data may exist and seek out SMEs: we have written separately about what data are needed for a Squalify quantification and where to find it. (See How to Plan a Successful Cyber Risk Quantification Project on the Squalify website). In summary, the Squalify methodology requires three categories of input:

- **Scenario information**: the definition of the loss event. Usually informed by Business Continuity or Crisis Plans.
- **Financial information**: both company level financial data such as revenue and profitability and scenario cost data. Squalify uses this data to inform several parameters within the model (described in detail below).
- **Information Security information**: Squalify users must provide security maturity data for the organizational unit in scope of the quantification (i.e. the company or business unit to which the Consequence Scenario applies).

Importantly, Squalify does not require users to estimate the equivalent of Security Threat Event Frequency or Vulnerability parameters directly, instead the equivalents in the Squalify model are derived from our historic loss database, and other inputs.

What makes Squalify different to FAIR?

The Squalify methodology is different to FAIR in a number of key ways:

Squalify is designed to quantify cyber risk for a strategic audience. Our “Top-Down” approach focuses on assessing risks to the entire company, or large sub-units thereof. We focus on high impact business scenarios that will have the attention of executives and the board rather than quantifying smaller technical risks to individual assets that, while important, may not be material overall.

Squalify prioritises simplicity over customisability. The Squalify platform is designed for quantifying cyber risks specifically, and we provide built in features to accelerate cyber risk quantification. The main way that Squalify simplifies the assessment is in the area of threat analysis.

Our model comes with built-in threat modelling covering the most common cyber threats and greatly simplifies the quantification process by avoiding the need to estimate most of the probability parameters needed for a FAIR quantification. With Squalify, these estimates are derived from our historic loss data set and other input parameters. The general threat model is adjusted per company based on other inputs (described in detail below).

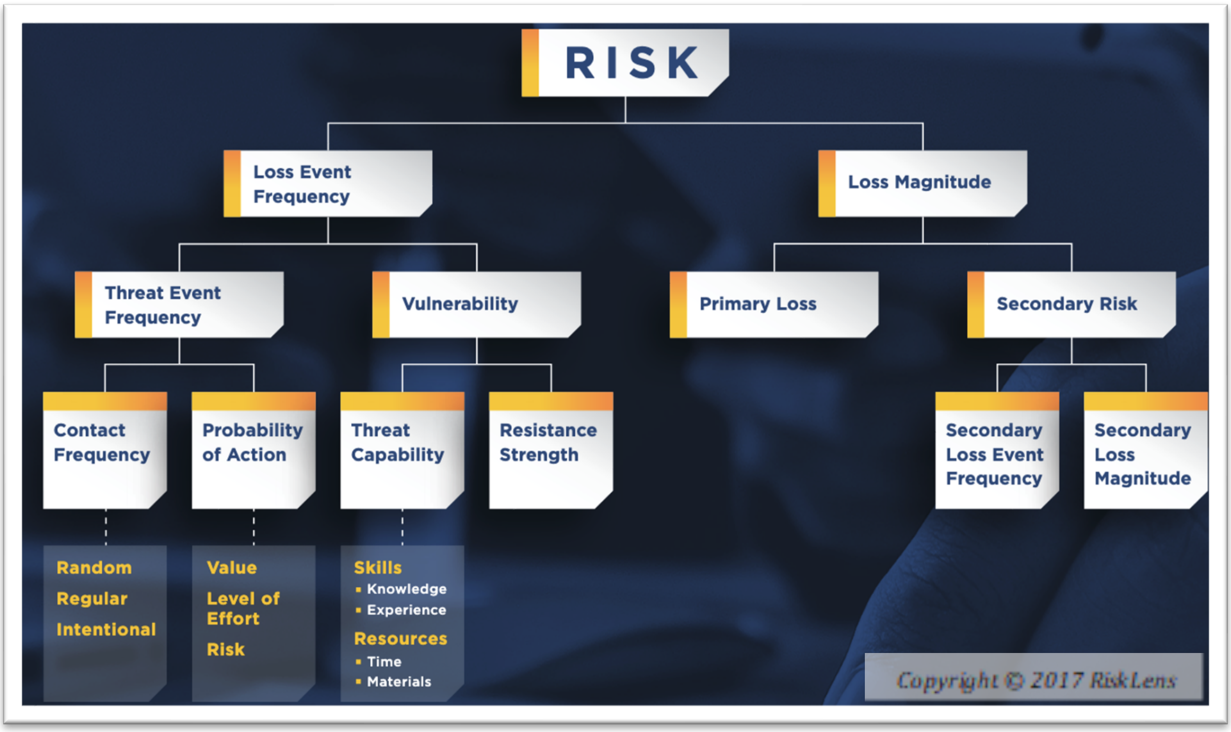
This focus on simplicity extends to the definition of loss scenarios. We have sets of questions to prompt the shaping of Consequence Scenarios and gather the necessary cost driver inputs.

In short, a Squalify user focuses their time on building the scenarios that are specific to their company, rather than crystal ball-gazing threat event frequency probabilities.

Squalify takes care of the model and the mathematics. Continuing the theme of simplicity, the Squalify model is provided to Squalify users ready-to-go. You do not need to build a quantification model (we’ve done that for you), you do not need to code a Monte-Carlo Simulation (we’ve done that as well), and you do not need to spend time maintaining parameters, spreadsheets or other internal parts of the model (we update the core model at least annually to take into account changes in regulations, the threat landscape and other important factors).

FAIR vs Squalify: A Detailed Comparison

The parameters of the FAIR model are shown in the image below. This section walks through each of those parameters and explains how Squalify approaches the same concepts.



At the highest level, FAIR considers two sides to risk: the probable frequency and the probable magnitude of a future loss.

Loss Event Frequency

The Loss Event Frequency is the “frequency, within a given timeframe, that loss is expected to occur.” This is often the most difficult part of the FAIR methodology to estimate, requiring detailed analysis of threat intelligence and security control data, and extrapolating from this the values of the detailed sub-parameters.

The most important difference between FAIR and Squalify is that Squalify users do not need to directly estimate the Loss Event Frequency. Instead, Squalify addresses this concept in two ways. Firstly, by using our historic loss database containing details of cyber events that have occurred and their associated costs, and secondly by combining these insights with other user-specified inputs.

Threat Event Frequency

The Threat Event Frequency is the "frequency, within a given timeframe, that threat agents are expected to act in a manner that could result in loss." FAIR users must build custom threat event scenarios for each quantification and make estimates of how often these threat events could occur.
In the Squalify model, the concept of Threat Event Frequency is handled differently. Importantly, Squalify users do not need to estimate how often a threat event might occur.

The Squalify model contains a built-in threat model that broadly cover the cyber threat landscape.
The Squalify threat model covers confidentiality, integrity, and availability losses; malicious and accidental actions; internal and external agents; and events impacting information and business processes.

Each threat event scenario in the threat model comes with pre-defined threat event frequencies that are derived from our historic loss database and tailored to the company being assessed by adjusting these frequencies based on other inputs in the model.

Contact Frequency and Probability of Action

In the FAIR model the Threat Event Frequency is calculated from the combination of the Contact Frequency, the "probable frequency, within a given timeframe, that threat agents will come into contact with assets" and the Probability of Action, the "probability that a threat agent will act upon an asset once contact has occurred".

These concepts are also addressed in the Squalify model, though again do not require direct estimating by a Squalify user. Instead, the pre-defined threat event frequencies are adjusted based on the Exposure parameter in the Squalify model.

The Exposure of a company in the Squalify model takes into account the size of the company (revenue, number of employees), its geography (which country is it headquartered in, does it operate in heavily regulated data protection jurisdictions) and its industry. These parameters combine to give an indication of the "attractiveness" of a company to malicious agents, which in turn addresses the Contact Frequency, Probability of Action, and Threat Event Frequency.

Vulnerability

The second component of the Loss Event Frequency is Vulnerability, defined in FAIR as the "probability that a threat event will become a loss event." Here, FAIR users must estimate the capabilities of threat agents who might target them, and the capabilities of their defences to resist such an attack.

Threat Capability

Estimating the Threat Capability, the "level of force a threat agent is able to apply" typically requires FAIR users to conduct threat intelligence analysis, studying the tactics, techniques and procedures of various nation state actors, criminal gangs, and other threat groups. This research is used to attempt to assign a number to the level of skill those groups may have and how much time such agents may wish to spend attacking them specifically. Needless to say, this can be very challenging, time consuming, and difficult to explain.

Again, Squalify greatly simplifies the estimation of the concept of Vulnerability. Squalify users do not need to estimate directly the Threat Capability.

The skills and resources of threat agents are indirectly considered in the Squalify model's Exposure parameter described above. The more highly Exposed a firm is, the more attractive it is to attack, which brings with it more capable threat agents who may spend more time and resources planning and executing attacks.

Resistance Strength

Similarly, estimating the Resistance Strength in a FAIR quantification, "a measure of how difficult it is for a threat actor to inflict harm (a.k.a. difficulty)" is prone to inconsistency, and challenge in explaining the rationale of choices. Even using ranges for inputs, modellers can get bogged down guesstimating whether the probability that a password is vulnerable to brute force attempts is 0.2, 0.3 or indeed any value. Multiply this by the need to estimate these values for all relevant controls and a FAIR quantification quickly drowns in complexity.

The Squalify model does not require directly estimated on a per control or per system basis. Instead, Squalify addresses the Resistance Strength concept through Information Security Maturity.

A Squalify user must assign a maturity level to controls within an information security framework. We use the NIST Cyber Security Framework (CSF) v2 by default but can use others.

Squalify's top-down approach to cyber risk quantification looks at the maturity of controls across organizational level for the assessment being conducted. So, if you are quantifying scenarios across the whole company, you need to provide maturity levels for the whole company. Similarly, if you are performing a quantification for a regional subsidiary, or for a specific business unit, then the maturity assessment needs input at that level. This approach also means that it is not necessary to set up integrations with other security tools.

Squalify's maturity assessment framework is well documented and similar in approach to common maturity approaches such as CMMI.

Within the Squalify model, the information security controls are mapped to the pre-defined Consequence Scenarios, and their impact on the frequency and magnitude of losses for those scenarios is parametrized. This greatly simplifies modelling for Squalify users and also enables the control improvement simulation features of the Squalify platform.

Loss Magnitude

The Loss Magnitude is the "probable magnitude of primary and secondary loss resulting from an event." The Squalify model quantifies the magnitude of both primary losses and secondary losses.

We use the term Loss Component to group together categories of expenses arising from a loss event. For each Loss Component, the Squalify platform provides a structured set of questions to help you estimate what the potential costs are for your scenarios within your organization. This applies to both primary losses and secondary losses.

The Loss Components we use are derived from the Cambridge Cyber Taxonomy for loss coverages. The following seven selected Loss Components constitute the most significant loss figures and are covered in the Squalify Model:

- **Incident response costs**: Direct costs incurred to investigate and close the incident to minimize post-incident losses. Applies to all the other categories/events.
- **Breach of privacy event**: The costs of responding to an event involving the release of information that causes a privacy breach, including notification, compensation, credit-watch services, and other third-party liabilities to affected data subjects, IT forensics, external services, and internal response costs, legal costs.
- **Regulatory and defence coverage:** Covers the legal, technical, or forensic services necessary to assist the policyholder in responding to governmental inquiries relating to a cyber incident, and provides coverage for fines, penalties, defence costs, investigations, or other regulatory actions where in violation of privacy law, and other costs of compliance with regulators and industry associations.
- **Data and software loss**: The costs of reconstituting data or software that have been deleted or corrupted.

- **Cyber extortion**: The costs of expert handling for an extortion incident. Combined with the amount of ransom payment.
- **Business Interruption**: Lost profits or extra expenses incurred due to the unavailability of IT systems or data as a result of cyber incidents or other non-malicious IT failures.
- **Financial Theft and Fraud**: The direct financial loss suffered by an organization arising from the use of computers to commit fraud or theft of money.

The Squalify Loss Components address almost all of the cost categories included in the FAIR Materiality Assessment Model. A full comparison is shown in the Appendix.

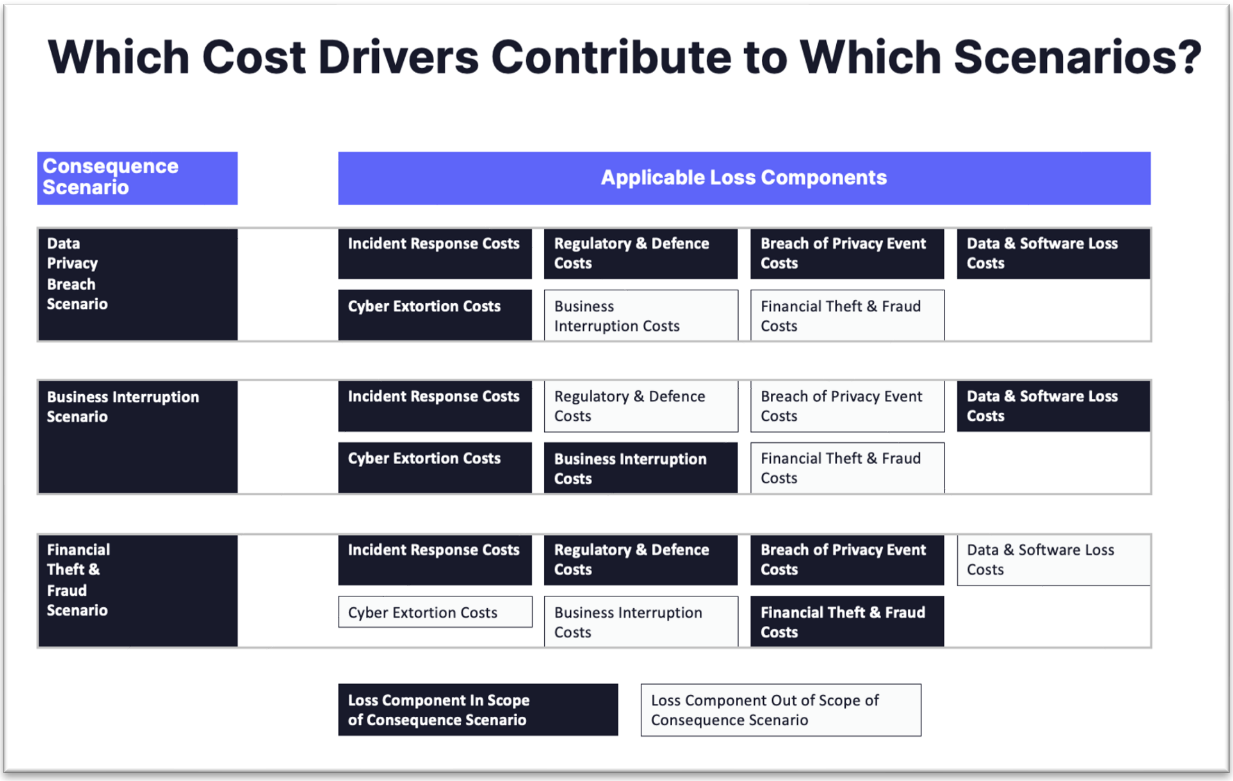
Secondary Loss Event Frequency and Magnitude

Within the FAIR methodology, a "Secondary Risk" is one that "exists due to the potential for secondary stakeholders' reactions to the primary event." This includes losses such as regulatory fines and judgements, legal liabilities, and expenses following an incident for public relations costs, credit monitoring and notification costs.

FAIR provides flexibility to estimate the frequency and magnitude parameters for the Secondary Risk. The Squalify model handles this in a different way: The Secondary Loss Event Frequency within the Squalify model is fixed, based on the type of Consequence Scenario. The Secondary Loss Magnitude is calculated based on other inputs.

For example, regulatory fines and judgements will always be considered for Consequence Scenarios that involve a data privacy breach. This is the equivalent of having a Secondary Loss Event Frequency equal to 100%. The magnitude of these fines and judgements is quantified based on parameters such as the overall information security maturity, the amount of personal data within the scope of the scenario, the sensitivity of that data, the company revenue, and the applicable regulatory jurisdictions.

The graphic below shows which Loss Components are applicable to which Consequence Scenario:



Which Cost Drivers Contribute to Which Scenarios?

Consequence Scenario	Applicable Loss Components			
Data Privacy Breach Scenario	**Incident Response Costs**	**Regulatory & Defence Costs**	**Breach of Privacy Event Costs**	**Data & Software Loss Costs**
	Cyber Extortion Costs	Business Interruption Costs	Financial Theft & Fraud Costs	
Business Interruption Scenario	**Incident Response Costs**	Regulatory & Defence Costs	Breach of Privacy Event Costs	**Data & Software Loss Costs**
	Cyber Extortion Costs	**Business Interruption Costs**	Financial Theft & Fraud Costs	
Financial Theft & Fraud Scenario	**Incident Response Costs**	**Regulatory & Defence Costs**	**Breach of Privacy Event Costs**	Data & Software Loss Costs
	Cyber Extortion Costs	Business Interruption Costs	**Financial Theft & Fraud Costs**	

Loss Component In Scope of Consequence Scenario

Loss Component Out of Scope of Consequence Scenario

Summary

To summarise, let's compare the respective strengths and weaknesses of the Squalify and FAIR methodologies.

Element	Squalify	FAIR
Purpose	For assessing and managing cyber risk at the strategic level.	For assessing and managing cyber risk at the operational level.
Risk Aggregation	Focuses on risks aggregated to company level by design.	Asset-centric focus means that aggregation to company level requires additional analysis and complexity.
Data	Frequency estimates largely provided based on historic data and simple company information.	User estimation required for all frequency and severity parameters.
Customisability	Pre-defined threat model is built in. Threat analysis is customised based on business level inputs (not estimating frequencies). User customisation focuses on the consequences and business impacts.	All aspects of model can be customised, but user is responsible for building and maintaining this complexity and bringing the necessary data.
Setup, Effort & Maintenance	Model implementation and maintenance is provided by Squalify. Typically 1-4 weeks to get CRQ results.	Can purchase tools that have models implemented and maintained. Can also do-it-yourself but need to resource this yourself. Typically 3-9 months to get CRQ results.

In short, Squalify is an excellent choice for quantifying your cyber risk, whether you are a CRQ beginner or a current FAIR user. We offer a simple methodology, we take care of the setup and maintenance of the model, and our historic dataset removes the need to make subjective threat analysis estimates.

About Squalify: Cyber Risk Quantification for the Boardroom

Squalify is a cyber risk quantification platform for the Boardroom. Our risk insights support information security and risk executives to answer the Board's toughest cybersecurity questions and steer group-wide risk reduction effectively from one platform. Fast. Data-backed. Scalable.

We are a corporate venture of Munich Re, one of the world's largest cyber reinsurers. Our proven risk model is built on a decade of cyber insurance expertise and powered by exclusive access to Munich Re's industry-leading cyber loss database; covering over 100,000 companies across 130+ industries and 80 countries. More than 4,500 companies have already been assessed using our quantification methodology.

- Want to see how this works in practice? Book a meeting
- Learn more on www.squalify.io
- Follow us on Linkedin
- See what Forbes is saying about us

AS SEEN IN

Forbes yahoo!finance CYBER DEFENSE MAGAZINE Cybersecurity INSIDERS

Appendix: Comparison of FAIR Materiality Assessment Model (FAIR-MAM) Cost Categories and Squalify Loss Components

- ✅ Included in Squalify core model
- ✏️ Can be added to quantification as "other costs"

FAIR-MAM Cost Category	Included in Squalify Model?	Comments
Information Privacy		
Sensitive PII Event Response and Management	✅	
PCI-DSS Liability	✅	
Information Privacy Liability	✅	
Regulatory Liability	✅	
Proprietary Data Loss		
Loss of Estimated Future Net Revenue		Scenario not included within Squalify model
Proprietary Data Loss Liability		
Business Interruption		
Direct Business Interruption	✅	
Contingent Business Interruption (Supply Chain Attack Victim – 3P failure to provide IT services)	✅	
Business Interruption Liability	✅	
Cyber Extortion		
Ransom	✅	
Network Security		
Network Event Response and Recovery	✅	
Network Security Liability (Supply Chain Attack Source)	✏️	
Financial Fraud		
Business Email Compromise	✅	
Funds Transfer Fraud	✅	
Media Content		
Media Event Response		Scenario not included within Squalify model
Media Liability		
Hardware Bricking		
Server Replacement	✅	
Computer / Laptop Replacement	✅	
Post Breach Security Improvements		
Legally Mandated Improvements	✏️	
Voluntary Improvements	✏️	
Reputational Damage		

Customer Retention, Future Projects, Market Value, Cyber Insurance, Cost of Capital, Employee Churn		Reputational damage addressed in part through loss of revenue but not broken down this way.