An Introduction to the FAIR Materiality Assessment Model

(FAIR-MAM™)

Summary

The FAIR Institute is releasing a new standard to help organizations assess the materiality of cybersecurity risk and incidents, called FAIR Materiality Assessment Model (FAIR-MAM™). FAIR-MAM expands the loss magnitude factor of the FAIR model and provides a more detailed taxonomy and breakdown of loss categories driven by cybersecurity incidents.

New rules approved in 2023 by the U.S. Securities and Exchange Commission (SEC) elevated the requirements for disclosing and managing cybersecurity risk and set a standard for cyber risk management that extends beyond the public companies regulated by the SEC.

The new rules exposed a gap in cyber risk management practices as many organizations realized they have to meet the SEC's requirement to report on "material" risks from cybersecurity incidents in a timely, accurate, defensible, and comparable way.

The FAIR Materiality Assessment Model (FAIR-MAM) is an open, financial loss model that enables organizations to:

- *Quantify the impact of cyber incidents so they can quickly and reliably disclose legally defensible material risk on SEC Form 8-K*
- *Report financial risk internally to inform cybersecurity investment and management decisions for a full range of custom cyber risk scenarios*
- *Create a timeline of the multi-year lifecycle of the total cost of an incident*

FAIR-MAM is also a standard that allows companies to report 'comparable' material financial costs related to cybersecurity incidents, a critical requirement for institutional investors.

Request for Comments

We welcome comments to further improve the FAIR-MAM standard. Comments may be submitted via email to the FAIR Institute Director of Standards and Research at pankaj@fairinstitute.org and should be received on or before September 30, 2023.

The SEC Rules on Disclosure of Material Cyber Risk

The new SEC materiality disclosure rules call for reactive and proactive actions:

Reactive:

- Companies are required to disclose the material aspects of the nature, scope, and timing of a cyber incident, as well as the incident's material impact.
- Disclosure of a material incident must be within four business days from the time that a breach is determined to be "material" (not to be confused with four days from learning of the breach).
- Companies must also disclose previously undisclosed cyber incidents that become material for the company's financial condition in the aggregate, for instance, multiple attacks by the same threat actor.

Proactive

- Periodic disclosures (for instance on Form 10-K) are required to describe a company's processes if any for assessing, identifying, and managing material risks from cybersecurity threats, including the board of directors' oversight and management's role and expertise on those risks.

The SEC does not give a formula to calculate "material" other than defining it as information that a "reasonable investor" would consider as material and would need to know to assess the company's financial standing for an investment decision. SEC Chair Gary Gensler offered some clarification that disclosures should be "consistent, comparable, and decision useful." That leaves companies largely on their own to develop a standard for materiality. What is needed are the following:

- An architecture to build a financial materiality assessment model for cyber incidents
- Materiality assessments that are legally defensible
- Materiality assessment reporting on Form 8-K that is comparable to the security incident data included in future 10-Q and 10-K reports
- Materiality assessment reporting that is comparable across companies for optimal use by investors and the SEC
- Materiality assessments that identify where a particular cost occurs in the lifecycle of the total financial cost of an attack, not just a point in time cost

Introducing the FAIR Materiality Assessment Model

What Is FAIR-MAM?

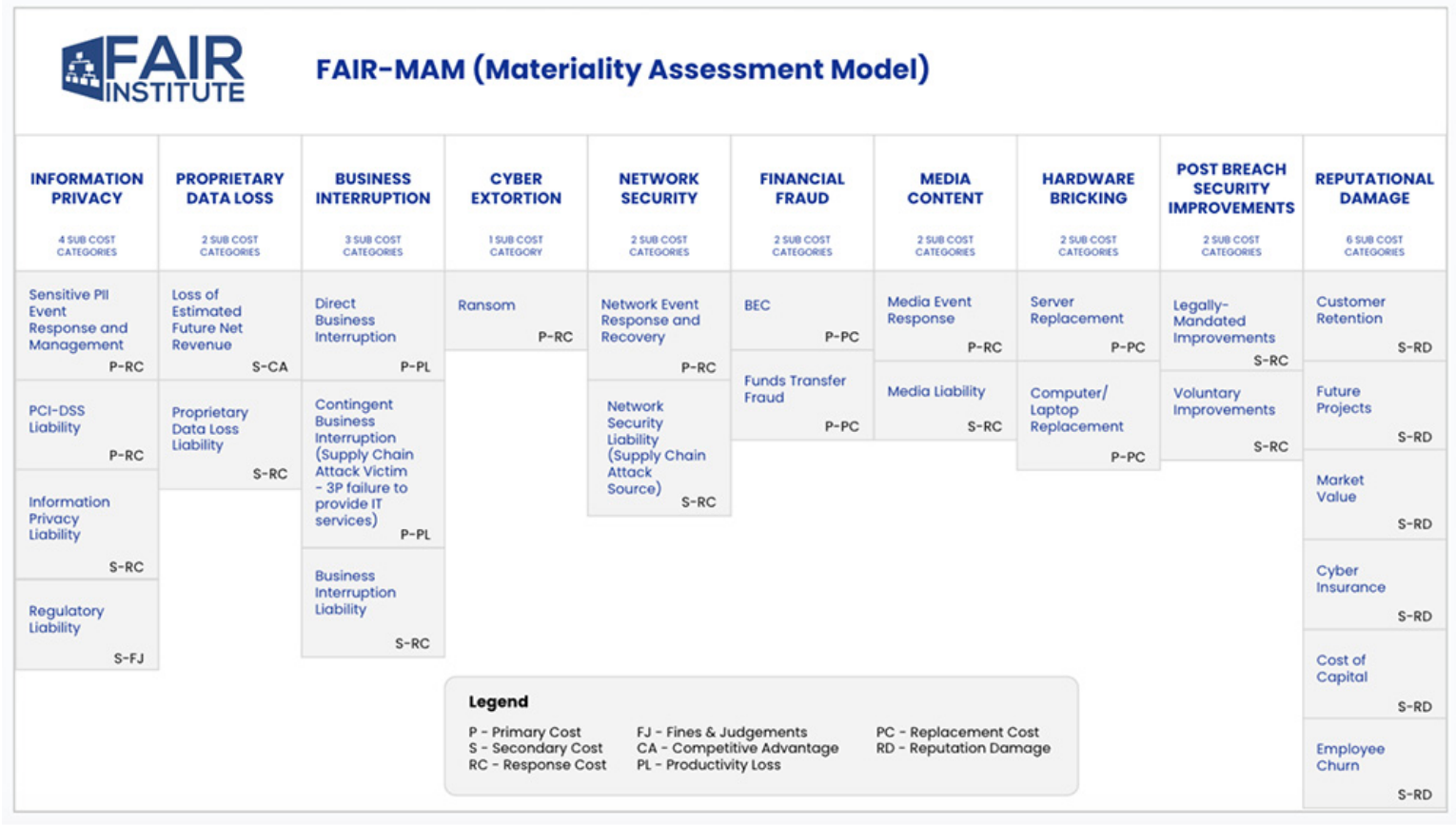
The FAIR Materiality Assessment Model (FAIR-MAM) is an open, financial loss model that can be used by organizations to help quantify the financial impact of cyber incidents, thereby enabling them to disclose material risk quickly and reliably or to report internally to inform security investment decisions. When used proactively and continuously, it allows management to manage estimated financial risk on an ongoing basis for any number of top risk scenarios custom to the organization. As an incident response tool, FAIR-MAM will help both SEC-registered and non-registered companies understand the potential financial impact of an incident as the magnitude of the attack is determined.

By translating the technical processes of cyber incident response and its consequences into the financial language of business, FAIR-MAM helps solve the materiality problem of cyber risk disclosure.

FAIR-MAM is released by the FAIR Institute, creators of Factor Analysis of Information Risk (FAIR™), the international standard for cyber risk quantification, recognized by the NIST CSF and other authorities.

FAIR-MAM is an open cyber-attack cost model, similar to the MITRE ATT&CK knowledge base for threat actor tactics and techniques. Like MITRE ATT&CK, FAIR-MAM, follows the MECE principle (Mutually Exclusive and Comprehensively Exhaustive) and is designed to include costs from any risk scenario against any corporate assets. It is open to any user.

FAIR-MAM can be used as a template for the creation of a complete, bottom-up cyber financial loss model that can easily be tuned - or customized - to reflect the unique asset profile and cost posture of any size company in any industry or geography. In-house teams proficient in the FAIR methodology that have done loss modeling can implement their own models within FAIR-MAM. Alternatively, they can leverage solutions that have implemented loss magnitude models based on FAIR-MAM.



FAIR-MAM is Comprised of 10 Primary Cost Modules

The 10 primary cost modules categorize costs according to cyber insurance claims categories. Each module has one or more additional categories that group costs as primary or secondary and classifies them by type. This comprehensive cost structure allows for customization of any asset mix on any attack surface for any risk scenario. The ten modules are defined as follows:

INFORMATION PRIVACY
All costs related specifically to compromise of sensitive personal data (including forensic discovery of records breached)

- PCI - Payment Card Information
- PFI - Personal Financial Information (e.g., bank account details, W-4 or 1099 data)
- PHI - Protected Health Information
- Sensitive PII - Personally Identifiable Information (including any government-issued ID information such as SSN, Driver's License, Passport, etc.)

PROPRIETARY DATA LOSS

- All costs related specifically to non-personal data such as Intellectual Property, Trade Secrets, Customer or Partner data, Internal Corporate information, etc.

BUSINESS INTERRUPTION

- The costs directly related to an interruption of business processes impacting revenue or operating expenses, or loss of third-party revenue-generating services

CYBER EXTORTION

- The cost of paying a ransom or preparing to pay a possible future ransom

NETWORK SECURITY

- All forensic and legal costs associated with the investigation of a security incident, notification to appropriate authorities, system and/or network remediation, data restoration, etc.

FINANCIAL FRAUD

- All costs related to the theft of cash or other monetary instruments

MEDIA CONTENT

- All costs related to the fraudulent use of media or advertising content (e.g., logos, trademarks, or other media content that uniquely identifies a company)

HARDWARE BRICKING

- The costs to replace IT systems or devices along with the operating systems and applications that were destroyed during a wiper type attack

POST BREACH SECURITY REQUIREMENTS

- Costs spent to improve cybersecurity after a breach, both voluntary improvements and those mandated by a regulatory body or court

REPUTATIONAL DAMAGE

- Costs that may reduce future revenues or increase costs after a breach due to breach-related damage to the reputation of the victim company

Key FAIR-MAM Use Cases

1. Proactively Calculate and Track Risk before an Incident Becomes Material
FAIR-MAM can be used proactively to model the estimated financial losses from a company's top cyber risk scenarios. Understanding and managing risk before an attack were to happen allows an organization to optimize the management of that risk: determining which mitigating controls offer the best return on investment based on financial risk reduction; evaluating whether existing cyber insurance coverages are aligned with the sources of costs from those risk scenarios; and defending the decision to accept any remaining risk.

2. Post Incident Materiality Assessment: All companies, not just those regulated by the SEC should know the financial impact of a security incident that occurred on their network or compromised their assets on a third-party network. FAIR-MAM's comprehensive framework allows for customizable models that can estimate the cost of an attack on any of the company's Business Resources from any type of risk scenario. This knowledge allows a company to begin planning immediately, if necessary, for both the inevitable and potential financial fallout from the incident.

3. Post Incident Materiality Tracker: Some incidents take longer than others to determine materiality for a number of reasons. It may not be immediately evident that data was stolen during a ransomware or DDoS attack. Or the forensic discovery process whereby the final list of deduped record holders and where they reside could take weeks or months to determine with a degree of certainty. Or there may have been a series of seemingly unrelated incidents that are later determined to have been parts of a staged attack by a single attacker. All of these situations could delay a determination of materiality for one or more cybersecurity incidents. By creating a dynamic model that automatically adapted to new forensic investigation inputs, one would know immediately when an incident triggered the predetermined materiality threshold, thereby placing the company in a defensible position to meet the SEC's 4-day Form 8-K reporting requirements, even if that reporting date was significantly later than the discovery of the incident.

Case Study

A publicly traded US healthcare center with numerous facilities in multiple states not only just discovered that several of their hospitals' networks were encrypted, but they are fairly certain that patient data was stolen before the encryption started. This company has 4 business days to file a Form 8-K from the point they determine the attack to have a material impact or reasonably likely material impact on the company, including its financial condition and results of operations. This filing with the SEC must not only describe the attack in general but must also provide investor guidance as to the potential materiality of the attack.

Given that the data potentially stolen is heavily regulated Protected Health Information (PHI), this could end up being a very expensive attack for the company, depending on whether customer data was in fact exfiltrated and how many individuals were compromised. If there was a significant data breach, there almost certainly would be litigation and given that this is a healthcare company, almost certainly regulatory investigations as well. On another front, several of the company's hospitals were unable to perform an unknown number of revenue-generating procedures from the time the encryption began until the systems were restored, or workarounds initiated to restore operations at some level of revenue generation. The business interruption may result in a material revenue loss, especially if the revenue-generating systems are down for an extended period of time.

Having previously adopted FAIR and now leveraging FAIR-MAM, this healthcare company would take the following steps to determine if and when a determination of materiality can be made for this security incident.

Step 1 The Risk team needs to build or use a commercially available materiality model using FAIR-MAM. If the team is composed of FAIR practitioners, then it is likely that they already have loss magnitude values with which they can begin to populate the model.

Step 2 The Risk team then solicits subject matter expertise from other teams within the company: cybersecurity incident response; legal; finance; etc. The information the Risk team is looking for pertains to costs of various external services and the estimated duration of business interruption and the activities performed by external service providers according to the FAIR-MAM cost categories. These additional cost parameters are added to the higher-level loss magnitude values already in the model to provide the specificity needed to perform detailed analysis of the inputs.

Step 3 The Risk team then begins to test the model, inputting data from the incident response team such as the percent of daily revenue interrupted from each impacted hospital, whether PHI records were compromised and, if so, how many. With this input, they can then see whether the company has reached the estimated materiality determination or how far away they are in terms of record count or days/hours of revenue interruption.

Frequently Asked Questions about FAIR-MAM

Q: What is FAIR-MAM?
A: FAIR-MAM is a standard taxonomy and analysis model for assessing the financial materiality of cyber incidents that is legally defensible and comparable across companies, as required by regulators.

Q: What is the need for FAIR-MAM?
A: Rules approved by the Securities and Exchange Commission in 2023 exposed the problem that many companies are not equipped to assess and disclose material risks from cybersecurity incidents in a timely, accurate and comparable way.

Q: How does FAIR-MAM differ from FAIR?
A: FAIR-MAM extends FAIR risk measurement of Loss Magnitude, providing a more detailed breakdown and description of the categories that contribute to Loss Magnitude. Similarly, to FAIR-CAM™, FAIR-MAM is an ancillary standard to the FAIR ontology and deepens the description of a main factor of the ontology.

Q: How does FAIR-MAM help companies with disclosing material cyber risks?
A: FAIR-MAM offers solutions for each of the proactive and reactive reporting requirements of the SEC. 1) Determining if a cybersecurity event has had material impact. 2) Materiality reporting generated within 4 days. 3) Aggregating materiality of multiple events over time. 4) Satisfying regulators that processes are in place for assessing and managing material risks on an ongoing basis.

Q: How is this different from and better than existing models or frameworks?
A: No comparable standard models exist specifically to quantify material risk from cyber incidents a) in financial terms, b) legally defensible and c) in a timeframe of 4 days or less.

Q: Can I use FAIR-MAM with MITRE ATT&CK or similar kill chain models or frameworks?
A: Yes, one can directly map 'Action on Objective' Tactics or Techniques in MITRE ATT&CK to loss categories. For example, losses associated with ransomware would map to Data Encrypted for Impact (T1486) and Inhibit System Recovery (T1490). For Data Compromise risk scenarios, one would map to the Exfiltration Tactic (TA0010) because it would not be possible to know exactly which technique was used from the loss magnitude perspective. Similarly, for a simple social engineering Business Email Compromise attack, where an employee was fooled into sending a vendor wire transfer payment to a fraudulent account, one would map to the Initial Access Tactic Phishing Technique (T1566).

Q: Can I use FAIR-MAM without a product?
A: Yes, users can build their own models to implement FAIR-MAM. For organizations that require enterprise-scalable use of FAIR-MAM, there are commercial solution providers such as Safe Security (Technical Advisor of the FAIR Institute) that have begun incorporating FAIR-MAM in their cyber risk management platform.

Q: What rights do I have to use the FAIR-MAM materials and related content and what are the restrictions on use?
A: FAIR-MAM™ is a copyrighted work owned by the FAIR Institute. The final version will be available to you under Creative Commons Attribution-Non Commercial-No Derivatives 4.0 International Public License (the link can be found at **https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode).**

You may use the FAIR-MAM™ standard for non-commercial purposes only. Additionally, if you remix, transform, create derivative works of, or otherwise change and/or build upon FAIR-MAM™, you may not distribute the modified materials. Users of FAIR-MAM™ are also required to refer to (https://www.fairinstitute.org/resources/FAIR-MAM) when referring to the model in order to ensure that users are employing the most up-to-date guidance. You may not remove the trademark FAIR-MAM™ from any content provided by the FAIR Institute as part of the work and any use of the trademark FAIR-MAM™ other than on exact reproductions of documents provided to you by the FAIR Institute is prohibited.

Commercial use of FAIR-MAM and related materials is prohibited without the prior approval, in writing, of the FAIR Institute. Please direct questions and inquiries to info@fairinstitute.org.