SAFE MATERIALITY ASSESSMENT MODULE

Determine Your Organization's Potential Material Impact from a cyber attack with the Safe Materiality Assessment Module

With the new SEC cyber rules coming into effect, establishing "materiality" of cybersecurity incidents is the need of the hour. While the SEC refrains from defining "material", cyber risk quantification is the definitive solution to this "materiality" challenge.

The Safe Materiality Assessment Module is designed to enable security and risk leaders to present defensible, company-specific quantified cyber risk to stakeholders, C-Suite and Board of Directors. It is based on the Fair Institute's bottom-up, fully tunable FAIR™-MAM model.

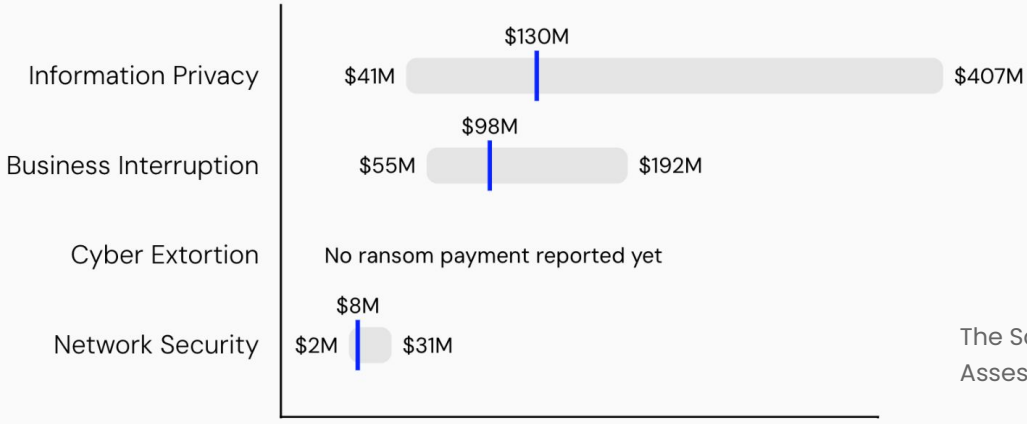
WHAT IS THE SAFE MATERIALITY ASSESSMENT MODULE?

Organizations use the Safe Materiality Assessment Module to quantify the probable frequency and potential loss magnitude of cyber events. This data equips leaders to tune their cybersecurity strategy, prioritize critical gaps, and reduce the business risk exposure from cyber events.

BENEFITS OF THE SAFE MATERIALITY ASSESSMENT MODULE

- ☑ Accurately assess the materiality of a cyber incident.
- ☑ Implement an open and customizable cost model that is defensible to the Board, investors, and regulators.
- ☑ Dynamically track incident impact identifying new inputs that could trigger a materiality threshold.
- ☑ Create a timeline of the multi-year life cycle of the total cost of an incident.
- ☑ Proactively calculate and track risk before an incident becomes material.
- ☑ Learn and disclose the material impact of previous cyber incidents with ease and simplicity.

Users of the Safe Materiality Assessment Module will find also an immediate application for FAIR™-MAM to quickly determine if a cyber incident will have the most serious material effect on the organization. This is a capability in high demand with the adoption by the U.S. Securities and Exchange Commission of new rules on speedy disclosure of material loss after a cyber event. **With the Safe Materiality Assessment Module, businesses will be able to instantly get a read on materiality, an outcome that typically takes weeks.**



The Safe Materiality Assessment Output

US Healthcare Case Study on using the Safe Materiality Assessment Module

US healthcare chain is hit by ransomware, halting critical revenue-generating medical procedures and triggering SEC disclosures. The healthcare chain had the foresight to build out an instance on the Safe Materiality Assessment Module.

- **Day 1:** Collected fresh and in-depth data from legal, finance, Incident Response, and other sources to perform detailed analysis on the cost inputs.
- **Day 2:** Started testing, inputting refined data such as the % of daily revenue interruptions
- **Day 3**: The Board is informed that the incident may not the predetermined materiality level since they could quickly revive revenue-generating systems and processes.
- **Day 6**: It's discovered that employee records were exfiltrated. Safe Materiality Assessment Module shows that the data breach exceeds the materiality threshold, prompting them to file an 8-K disclosure.

Beyond SEC Compliance: Use Cases for the Safe Materiality Assessment Module

While SEC rules on disclosure are the driver for publicly traded companies to implement materiality calculations, every company needs to set a risk appetite based on quantified targets – including a working definition of material risk levels – to manage cyber risk responsibly. **The other use cases of the Safe Materiality Assessment Module include:**

Proactively calculate and track risk before an incident becomes material. Model estimated financial losses from top risk scenarios with FAIR-MAM to cost-effectively target security or cyber insurance investments.

Assess materiality during an incident based on a comprehensive framework, tailored to the risk scenarios or business assets targeted. Leverage the insights to prepare for the probable financial impact to follow.

Track materiality post-incident. Forensic and legal discovery related to cyber loss events can continue for extended periods when assessing all immediate primary costs (quantitative in SEC language). Then, there are the secondary (or 'qualitative" in SEC language) cost considerations related to the likelihood that the company will be notified of regulatory investigation(s) and/or litigation filed in relation to the breach.

KNOW THE MATERIAL IMPACT OF A HACK WITH SAFE'S AI-DRIVEN APPROACH

It is clear that the determination of cyber risk materiality is non-negotiable and cyber risk quantification is key to solving the materiality challenge. The Safe Materiality Assessment Module, with the automated implementation of FAIR™-MAM, makes it simpler and scalable - all in a way that is standards-based, transparent, and defensible if challenged by regulators or investors.

Schedule a meeting with a cyber risk expert to address the materiality challenge of cyber risk disclosure.

RESEARCH SPONSOR
MITRE ATT&CK, TOP CONTRIBUTOR

PUBLISHER'S CHOICE AWARD
RISK MANAGEMENT
GLOBAL INFOSEC AWARDS - RSAC 2023

BEST NEXT GEN
CYBER INSURANCE PLATFORM
GLOBAL INFOSEC AWARDS - RSAC 2023

BEST RISK
MANAGEMENT SOLUTION
CISO CHOICE AWARDS 2022™