KOVRR

Determining Cyber Materiality in a Post-SEC Cyber Rule World

BY JACK FREUND, ISSA DISTINGUISHED FELLOW, CHARLOTTE METRO CHAPTER AND NATALIE JORION

This article was originally published in the ISSA Journal, September 2023.

This article outlines the history of what constitutes a material event and its applicability to the cyber world and provides guidance on how firms can assess a material impact suitable for SEC disclosure.

The Securities and Exchange Commission (SEC) in the United States approved their cyber rules on July 2023, originally proposed in March 2022 for public comments (SEC, 2022; 2023). This has sparked many conversations about how the board of directors and executive management should think about cybersecurity and to what extent public disclosures should be made about cybersecurity incidents and risks. Most notable among them is the requirement that material cyber incidents be reported within four days. Under this new rule, affected companies have to file on Form 8-K the details of the potential effects of the incident.

This has brought significant focus to what constitutes a material incident. This paper will outline the history of what constitutes a material event and its applicability to the cyber world. We will end with specific, quantitative guidance on how firms can assess a material impact suitable for SEC disclosure. This approach to determining financial materiality may be helpful in responding to SEC cyber disclosure rules. Readers should keep in mind that there are also non-financial triggers for materiality that must be considered, which is outlined in the heuristic below.

Methods for Determining Materiality Thresholds

Governance consultants, auditors, and researchers define materiality as the degree to which a change in the information on financial statements could impact a user's decision-making (Normandin & Repetto, 2019; AICPA, 2021; SEC, 1999). Users could be shareholders, creditors, suppliers, customers, management, or regulating entities (Corporate Finance Institute, 2023). The Security Exchange Commission (SEC) has previously stated that companies must consider the materiality of risks when disclosing information on a cybersecurity incident (2011). The materiality depends on multiple factors, including the potential magnitude of a cybersecurity event, the range of harm it could cause, the nature of an organization's business, the type of data it handles, and the potential impact of a breach on its financial performance, reputation, and customers (Johnston et al., 2022).

To date, there are no universally agreed-upon standards for calculating materiality. Some governing bodies resist rules of thumb and prefer a complete analysis of the company's situation. The SEC states that reliance on

> any percentage or numerical threshold has no basis in the accounting literature or the law. Quantifying, in percentage terms, the magnitude of a misstatement is only the beginning of an analysis of materiality; it cannot appropriately be used as a substitute for a full analysis of all relevant considerations. (1999)

Likewise, the Financial Accounting Standards Board (FASB) states that

> [M]agnitude by itself, without regard to the nature of the item and the circumstances in which the judgment has to be made, will not generally be a sufficient basis for a materiality judgment. (1980)

The FASB suggests that auditors investigate additional factors, such as the expected standard error associated with a measurement or impact on earnings and regulatory requirements.

Indeed, companies often determine materiality based on various quantitative and qualitative factors (Normandin & Repetto, 2019). Company and auditor profiles also impact quantitative calculations. Auditor thresholds vary based on the auditor's experience, firm size, and industry specialization (Iseline & Iskandar, 2000; AICPA, 2021). For example, auditors working in larger firms with higher reputational risk tend to set more conservative thresholds (Iseline & Iskandar, 2000).

Early approaches to identifying quantified thresholds for materiality focused on straight percentages of financial benchmarks. McKee and Eilifsen (2000) discussed several

specific quantitative metrics for making a preliminary judgment on materiality. These include the following: 5% of pre-tax income, 0.5% of total assets, 1% of equity, or 0.5% of total revenues. Such rule-of-thumb calculations are helpful for quickly identifying transactions or events that could be material. Further contextualization and application of qualitative measures would further allow for an official material designation to be made.

It may be useful to consider general variances in risk profiles by industry to help determine materiality thresholds. Studies have been done to derive such general industry classifications. Businesses that store important sensitive data in highly regulated industries with a large customer base and high revenue are likelier to take cyber insurance. Financial services have the greatest uptake of cyber insurance compared to other industries, which may indicate how they perceive their risk exposure (Hiscox, 2022). Moody's Investors Service (2021) investigated which industries are at greatest risk for cyber threats. Banks, utilities, and government institutions had the highest systemic risk, given their role in the broader economy, while healthcare had highly attractive datasets with average mitigations in place. The Secure Controls Framework also defined attributes that signal risk tolerance and provided examples of industries by risk level (SCF, 2023). Low-risk industries have fewer cybersecurity regulations and store, process, or transmit a limited amount of sensitive data. Examples of low-risk industries include restaurants, hospitality, construction, manufacturing, and personal services.

Nonetheless, some still suggest using an absolute amount or percentage for comparison as a starting point for assessing materiality. Weaver (2017) provides a general rule of thumb stating that materiality is when a line item differs by more than $10,000 or 10% from the previous accounting period. More commonly, auditors calculate materiality as the percentage of a base amount. Auditors may use different input values for the financial benchmark: net income, gross profit, revenue, total assets, net asset value, total expenses, or total equity (AICPA, 2021). Jacoby & Levy (2016) recommend using relatively stable benchmarks for determining materiality, such as assets or revenues (whichever is larger) or measuring entity value for public companies. Net income is the most commonly used amount as the basis (MaterialityTracker, n.d.), however, Freund (2020) identified that a revenue benchmark is best for cyber materiality calculations.

The materiality ranges may also differ. MaterialityTracker (n.d.) defines a percentage under 5% as immaterial, more than 10% as material, and between 5% and 10% requires judgment (when speaking about transaction variance). The thresholds could vary depending on the chosen base amount. For example, some auditors base the calculation on capital with a 2% - 5% range. The thresholds might be 5% - 10% when they base it on net income. The Norweigan Research Council suggested two materiality thresholds (Eilifsen & Messier, 2015). The first is a single rule method with the following thresholds: 5% of pre-tax income, 0.5% of total assets, 1% of shareholders' equity, and 1% of total revenue. The second is a variable size rule method based on gross profit, with the following parameters:

- 2% to 5% of gross profit (if less than $20,000)
- 1% to 2% of gross profit (if gross profit is more than $20,000 but less than $1,000,000)
- 0.5% to 1% of gross profit (if gross profit is more than $1,000,000 but less than $100,000,000
- 0.5% of gross profit (if gross profit is more than $100,000,000)

Blending these methods and creating weighing for each element is also possible.

Plesser (1984) provides another set of suggested ranges for determining materiality, which uses different bases for the calculation:

- 0.5% to 1% of total revenue
- 1% to 2% of total assets
- 1% to 2% of gross profit
- 2% to 5% of shareholders' equity
- 5% to 10% of net income

Typically, auditors apply thresholds to the reported year, but they might look at earning trends over the last five years.

Qualitative factors also impact what auditors deem as material. Different company situations predicate which of these bases to choose:

- High-risk industries might have a lower percentage threshold, so finance tends to have a lower threshold than retail.
- If pre-tax profit is volatile, auditors may use total revenue.
- When operational profits are poor, using equity, assets, or revenue as the base might be more appropriate (Iskandar & Iseline, 1999).
- Even percentages falling below the designated threshold might be deemed material if they involve fraudulent behavior (CFI, 2023).

Many countries have tried to standardize materiality thresholds. Australian accounting standards state that below 5% is immaterial, whereas above 10% is material. Some auditors in Australia still report items below 5% (Iseline & Iskandar, 2000). In the US, the Financial Accounting Standards Board (FASB) published suggested guidelines in 1975, which they withdrew in 1980 and did not replace. Weaver (2017) states that one of the main bottlenecks for the FASB to establish materiality standards is enforcing them.

Iseline and Iskandar (2000) surveyed Australian auditors and found that the average recognition threshold was 5.7%, and the average disclosure threshold was 8.7%. They also investigated how qualitative variables such as industry impacted materiality thresholds and found that the mean was 6.5% for financial specialists and 8.2% for retail specialists. This difference in percentage by industry corroborates the hypothesis that riskier industries have lower thresholds than more stable industries.

Testing Standard Materiality Thresholds with Cybersecurity Incident Loss Data

Based on the above guidance, applying those materiality thresholds to cybersecurity incidents may seem straightforward. Freund (2020) showed that such an approach to only one of the loss variables (fines and judgments) resulted in less than 10 of the top 50 most expensive fines being considered material. As of that writing, the fine would need to be over $2B to be considered material using the materiality thresholds reviewed above, exclusive of the other costs associated with a cybersecurity incident. We expanded on and updated that

research by conducting an empirical analysis of the total cost of top cybersecurity events and evaluating materiality using net income, revenue, and net income.

Our analysis leveraged the Advisen Cyber Loss dataset, which contains over ninety thousand publicly disclosed cyber incidents until February 2022. The data contains case types, affected count, accident date, source of loss, type of loss, actor, loss amount, company size, company type, number of employees, industry code, and geography. We filtered for the top 50 most expensive incidents for companies with available revenue data and checked that there were no duplicated events (which happens with variance in reporting). We extracted company revenue, net income, and equity from the year the event occurred from the Macrotrends website, which amounted to 39 unique companies with losses. Events ranged from $47 to $5B losses from 1999 to 2022.

Second, we selected benchmarks and thresholds based on the literature review and percentage ranges. We chose three benchmarks:

1. 4% of revenue and above
2. +/- 100% of net income
3. 5% of equity

None of the companies in the data had a negative revenue, so we could not implement a hybrid rule, where if a company had a loss, then use assets, otherwise use net profits. Third, we computed and plotted losses against benchmark percentages. Finally, we reverse-computed and plotted the material losses.

Case 1: 4% of Revenue

Fourteen incidents would have been material using this threshold with the revenue benchmark. Gawker Media had the most significant percentage. Their 2012 cyber incident cost $146M out of their annual $25M revenue, for a 570% loss to revenue.

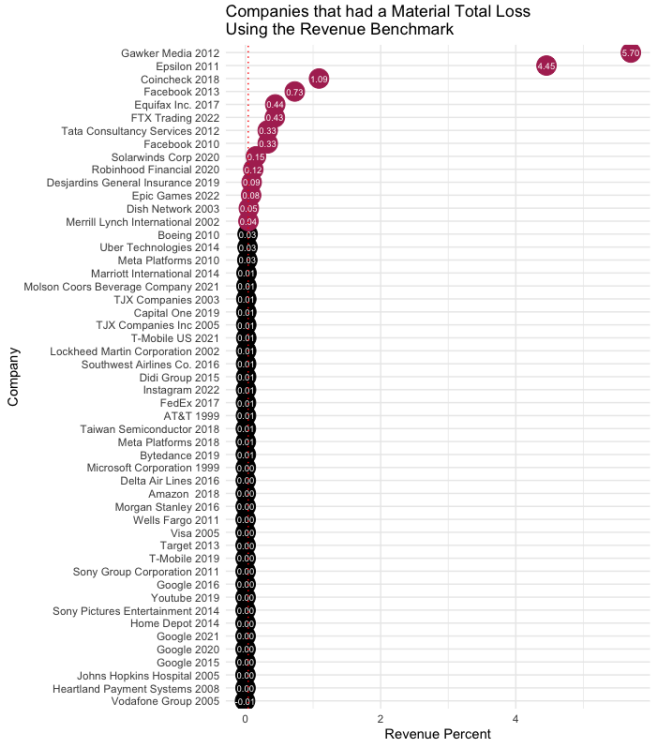


Figure 1: Analysis of top cyber losses and judgments with a 4% of revenue threshold

Case 2: +/- 100% of Net Income

Ten incidents would have been material using this threshold with the net income benchmark (four companies had a negative net income). Robinhood Financial had the most significant percentage. Their 2020 cyber incident cost $110M out of their annual $7M net income.

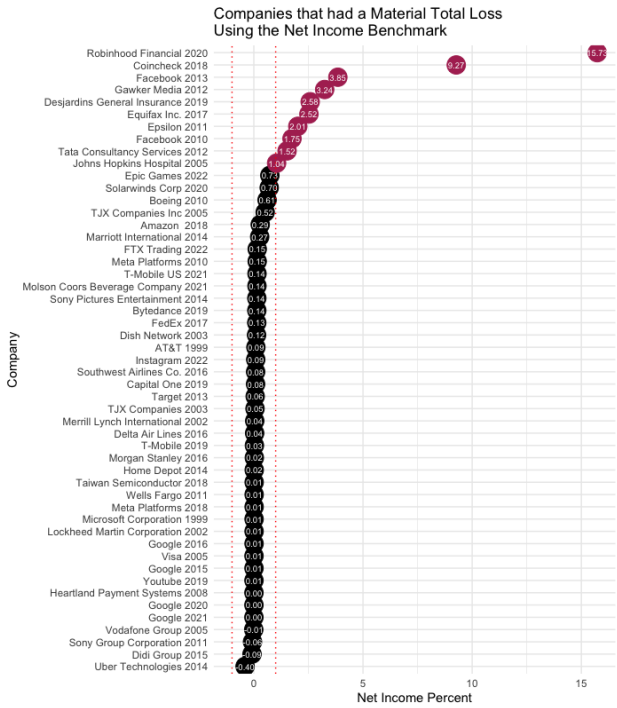


Figure 2: Analysis of top cyber losses with a +/- 100% of net income threshold

Case 3: 5% of Equity

Ten incidents would have been material using this threshold with the equity benchmark. Boeing's 2010 $2B breach had the highest ratio (70%).

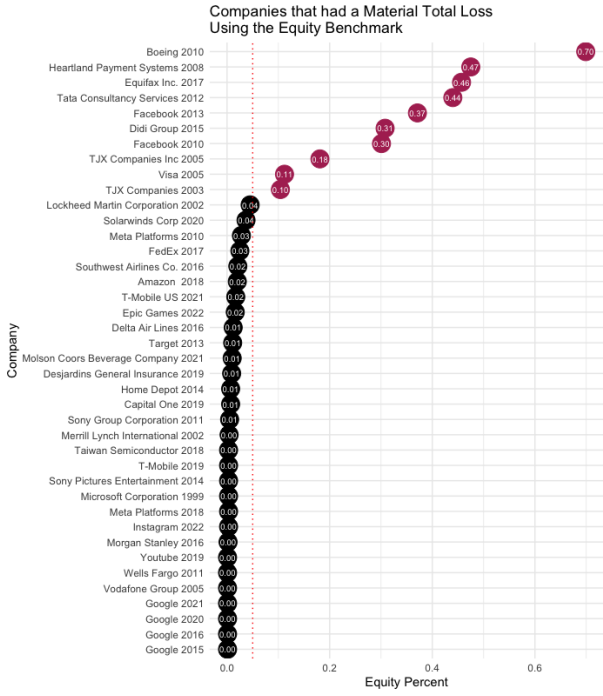


Figure 3: Analysis of top cyber losses with a 5% of equity threshold

Materiality by Size and Industry

We also analyzed the percentage of cases in the Advisen data that would be flagged as material based on various revenue materiality thresholds and company sizes. Companies with a revenue of 130M or more were classified as very large; those with revenues between 13M and 130M were considered large; companies with revenues between 1.3M and 13M were categorized as medium-sized; and those with less than 1.3M in revenue were classified as small. Notably, the larger the company, the more likely that even a small materiality threshold would result in the majority of losses being immaterial. For example, a 0.1% materiality threshold would mean that only 7% of cases involving a very large company resulted in a material loss.

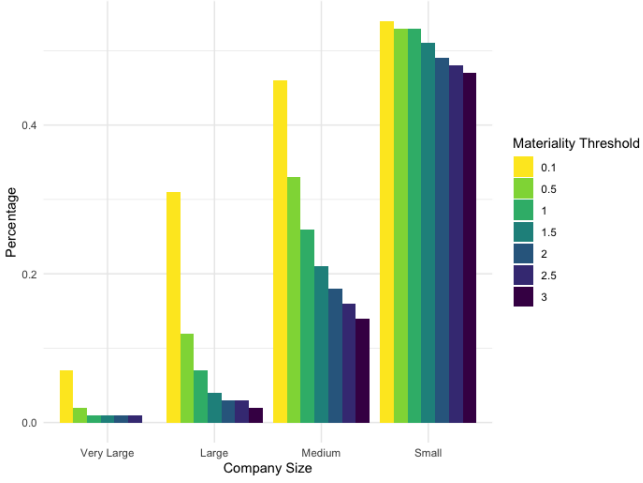


Figure 5: Analysis of materiality by firm size

We further analyzed the role that a firm's industry plays in determining its cyber materiality thresholds. The result of this analysis showed that there were no obvious trends for materiality based on industry. This suggests that setting industry-specific materiality thresholds based on revenue will not be a good strategy for determining cyber security materiality. One notable observation, however, was that public sector organizations had a larger percentage of material losses for all material thresholds.

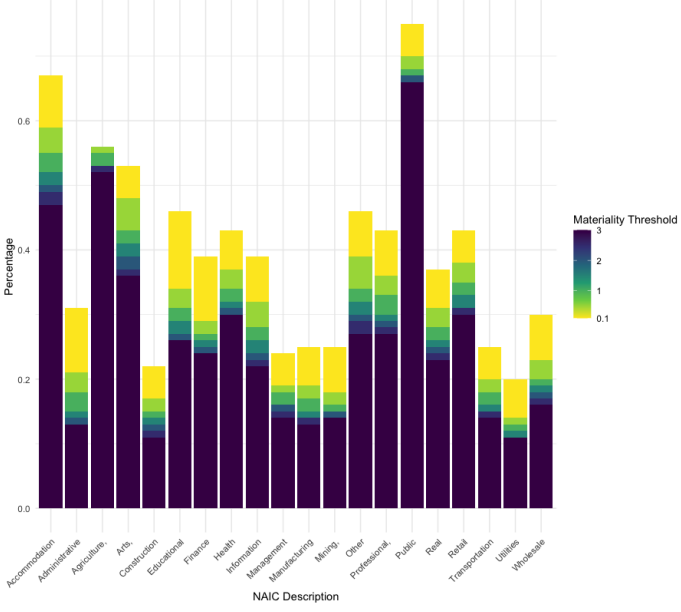


Figure 6: Analysis of materiality by industry

Discussion

There are two general use cases for applying cybersecurity materiality thresholds: cybersecurity risk report and cybersecurity incident reporting. Risk reporting generally has two versions: rate of change materiality (RoCM) and forecast accuracy materiality (FAM). The SEC's new guidance is the requirement to report on processes for assessing, identifying, and managing material risks from cybersecurity threats on Form 10-K. Namely, identifying material cybersecurity risks to enable one to report on the management process requires as a predicate an understanding of what a material cybersecurity risk is. Assessment approaches for quantitatively forecasting losses from cyber risks have been discussed by Freund and Jones (2014) and Freund (2021; 2022). Once cyber risk has been assessed quantitatively, values from those loss projections (such as a mode or max) can then be analyzed using the materiality thresholds discussed here.

The RoCM framework presupposes the completion of a quantitative analysis of relevant risk scenarios coupled with regular reassessment intervals, such as on a monthly or quarterly basis. The rate of change forms the basis of a materiality disclosure assessment. This will allow investors to understand if the risks a firm faces are changing in an unacceptable way. For example, changes in the regulatory environment, inflation, or underlying business practices may adjust the risk of data loss and theft that an organization may incur. If an entity reports such a change of 9% as an example, an investor could make a determination of whether this change is meaningful to their investment decisions. Such disclosure determination should be judged using a sliding scale as indicated below. Values in the immaterial and potentially material categories should be subject to a second round of determination using qualitative factors discussed below.

FAM is closely related to RoCM but is conducted after an incident has occurred. This kind of materiality disclosure assesses the risk management capabilities of a firm by judging how well they could assess future losses accurately. Namely, it compares the actual loss of the cyber security incident to the range of estimates provided for such an incident in their risk assessments. The variance against a particular benchmark (likely the mode and max values) would form the foundation of the FAM. A similar sliding scale to the RoCM value should be used.

Value and Period	Determination
<5% change quarter over quarter	Immaterial
5% to 10% change quarter over quarter	Potentially Material
>9% change quarter over quarter	Material

Table 1: Materiality Determination for RoCM and FAM

The new SEC requirements also specifically mention the reporting of Incident materiality (IM) on Form 8-K. In the first set of analyses we conducted, applying common materiality heuristics flagged only a few top data breaches. However, these data breaches significantly impacted the organization and its customers. It would be questionable to assert that only a handful of companies should report the events and disclose this information in their SEC filings. Most, if not all, of these events, should count as material regarding cyber incidents.

The implication is that the standard accounting materiality thresholds are too high and inappropriate for analyzing cyber incidents. We suggest using the most sensitive of these three heuristics, the revenue benchmark. A 0.5% revenue materiality threshold would flag 37 of the 50 top incidents (including one company with a negative revenue), while a 0.01% threshold would flag 48.

In addition, it is of course appropriate to evaluate the qualitative nature of the incident. For example, the type of data breached could also impact whether the incident was material. A data breach that exposes sensitive company information would have more impact on a financial company and its clients than a small company. A financial company would have more sensitive information of greater value to cybersecurity criminals. Moreover, materiality thresholds for cyber incidents should also consider regulatory requirements and industry standards. Companies subject to data breach notification laws would have a lower materiality threshold than companies with no requirements.

The Freund-Jorion Cyber Materiality Heuristic

Below we propose the following heuristic for materiality determination for both risk- and incident-based materiality reporting. Note that in both cases, as supported by the literature, a quantitative and qualitative evaluation must be completed. However, reviewing potential and actual losses to the financial materiality thresholds shown here are useful determinants for evaluating preliminary materiality.

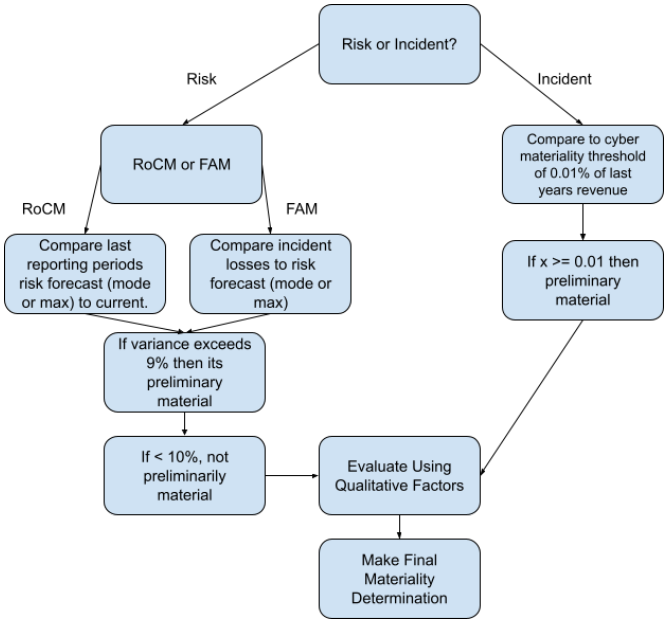


Figure 7: Freund-Jorion Materiality Heuristic

Generally, the process flow above follows the following steps for materiality determination.

Step 1: Quantitative Preliminary Materiality Judgement

IM: Compare the cost of the incident to 0.01% of the organization's revenue as reported on the last annual report.

If X > 0.01% * Revenue then the incident could be preliminarily material

RoCM and FAM: Compare the cost of the risk to the sliding scale. Variances in excess of 9% can be considered preliminarily material.

Step 2: Qualitative Preliminary Materiality Judgement

Assess the impact that the risk/incident may have on the organization's primary value proposition. This includes evaluating risks/incidents that were not determined to be preliminarily material using the above quantitative analysis. Such categories for consideration may include the type of data, the criticality of the risk/incident, issues of actual or perceived negligence, the particular nature of the event, regulatory oversight and requirements (more highly regulated industries may err on the side of over-disclosure), industry, and size. Generally, if most senior executives feel an incident would impact an investor's decision-making, the risk/incident should be considered preliminarily material.

Step 3: Finalize Materiality Disclosures

Once preliminary assessments have been completed, an internal review of the results should ensue. At this point, it may also be valuable for organizations to request review by their external auditors and legal counsel. The appropriate SEC forms can then be filed once all the proper consents and approvals have been obtained.

Conclusion

Determining the materiality threshold for cyber incidents is a complex process dependent on many factors, including the type of data involved, the company's industry, regulatory requirements, and the potential impact a data breach could have on its business, reputation, and clients. However, a 0.01% loss to revenue threshold could be a reasonable starting point for some organizations. Anything less than a 0.01% loss of the company's annual revenue would be considered immaterial, and companies may not need to report losses to regulators or shareholders. The 0.01% threshold should only be a rule of thumb; each organization should consider its unique circumstances to determine the appropriate threshold. Moreover, this threshold should be reviewed periodically and updated as the organization's business and the risk landscape change.

References

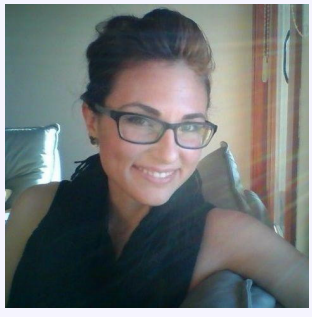
1. https://www.macrotrends.net/
2. American Institute of Certified Public Accountants (AICPA). (2021). Materiality in Planning and Performing an Audit. AU-C Section 320. Retrieved from https://us.aicpa.org/content/dam/aicpa/research/standards/auditattest/downloadabledocuments/au-c-00320.pdf
3. Corporate Financial Institute. (2023). Materiality Thresholds in Audits. Retrieved from https://corporatefinanceinstitute.com/resources/knowledge/accounting/materiality-threshold-in-audits/
4. Eilifsen, A., & Messier Jr, W. F. (2015). Materiality guidance of the major public accounting firms. Auditing: A Journal of Practice & Theory, 34(2), 3-26.
5. Freund, J. (2020). Engineering Economic Externalities: Methods for determining material cyber security fines [Paper presentation]. SIRACon 2020.
6. Freund, J. (2021). Cyberrisk Quantification, ISACA, https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpcrq

7. Freund, J. (2022). Cyber Risk Quantification (CRQ) Accelerators, ISSA Journal, June 2022.
8. Freund, J., Jones, J. (2014). Measuring and Managing Information Risk: A FAIR Approach. Portsmouth, NH: Butterworth-Heinemann.
9. Financial Accounting Standards Board. (1975). An Analysis of Issues Related to Criteria for Determining Materiality. Financial Accounting Standards Board.
10. Financial Accounting Standards Board. (1980). Statement of financial accounting concepts no.2: Qualitative characteristics of accounting information. Financial Accounting Standards Board.
11. HISCOX. (2022). Hiscox Cyber Readiness Report. Retrieved from https://www.hiscox.com/documents/Hiscox-Cyber-Readiness-Report-2022.pdf
12. Iskandar, T. M., & Iselin, E. R. (1999, September). A review of materiality research. In Accounting Forum (Vol. 23, No. 3, pp. 209-239). Taylor & Francis.
13. Iselin, E. R., & Iskandar, T. M. (2000). Auditors' Recognition and Disclosure of Materiality Thresholds: Their Magnitude and the Effects of Industry. The British Accounting Review, 32(3), 289-309.
14. Jacoby, J., & Levy, H. B. (2016). The materiality mystery. The CPA Journal, 86(7), 14. Johnston, J., Falcon, B., Natenson, M., & Garcia, Angie. (2022, April 21). What makes a cyberSECurity risk or incident material? A look at the SEC's proposed rules on cyberSECurity. Vinson & Elkins LLP. https://www.velaw.com/insights/what-makes-a-cybersecurity-risk-or-incident-material-a-lok-at-the-secs-proposed-rules-on-cybersecurity/
15. KPMG. (2008). Understanding and articulating risk appetite. Retrieved from https://www.kpmg.com.au/Portals/0/ias_erm-riskappetite200806.pdf
16. McKee, T. R., & Eilifsen, A. (2000). Current Materiality Guidance for Auditors.
17. MaterialityTracker. (n.d.). Financial Thresholds. Retrieved from http://www.materialitytracker.net/standards/financial-thresholds/
18. Moody's Investors Service. (2022). Industries boost cyber defenses against growing number of attacks. Retrieved from https://www.moodys.com/web/en/us/about/insights/data-stories/cyber-risks-are-rising.html
19. Normandin, E. & Repetto, M. (2019, March). SEC Disclosure Requirements for Cybersecurity Breaches are Murky. Directors & Boards. Retrieved from https://www.directorsandboards.com/news/sec-disclosure-requirements-cybersecurity-breaches-are-murky
20. Plesser, D. (1984). Audit risk and materiality. The CPA Journal (pre-1986), 54(000007), p. 83.
21. Secure Controls Framework. (2023). Cybersecurity materiality. https://securecontrolsframework.com/cybersecurity-materiality/
21. Securities and Exchange Commission. (2018). Commission Statement and Guidance on Public Company Cybersecurity Disclosures. Retrieved from https://www.sec.gov/rules/interp/2018/33-10459.pdf
23. Securities and Exchange Commission. (2022). Proposed Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure. Retrieved from https://www.sec.gov/files/rules/proposed/2022/33-11038.pdf
24. Securities and Exchange Commission. (2023). Final Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure. Retrieved from https://www.sec.gov/files/rules/proposed/2022/33-11038.pdf
25. Weaver. (2017, December). FASB Abandons Proposed Changes to Definition of Materiality. Retrieved from https://weaver.com/blog/fasb-abandons-proposed-changes-definition-materiality

About the Authors

Jack Freund, Ph.D., CISA, CRISC, CISM, CGEIT, CDPSE, NACD.DC

As Chief Risk Officer for Kovrr, Jack oversees the risk and compliance function and governance of the firm's cyber risk products. He is also the co-author of the foundational cyber risk quantification (CRQ) book using the FAIR standard, which was inducted into the Cybersecurity Canon in 2016. Jack was awarded a Ph.D. in Information Systems after his research in disaster informatics and cyber resilience at Nova Southeastern University. He holds multiple security and risk certifications and was named Distinguished Fellow of the ISSA. Jack also serves on the board of the ISSA Education Foundation.



Natalie Jorion, Ph.D.

Is a principal data scientist at BitSight, a cybersecurity ratings enterprise. She has been involved in validating and refining algorithms used for financial quantification and risk vector models.