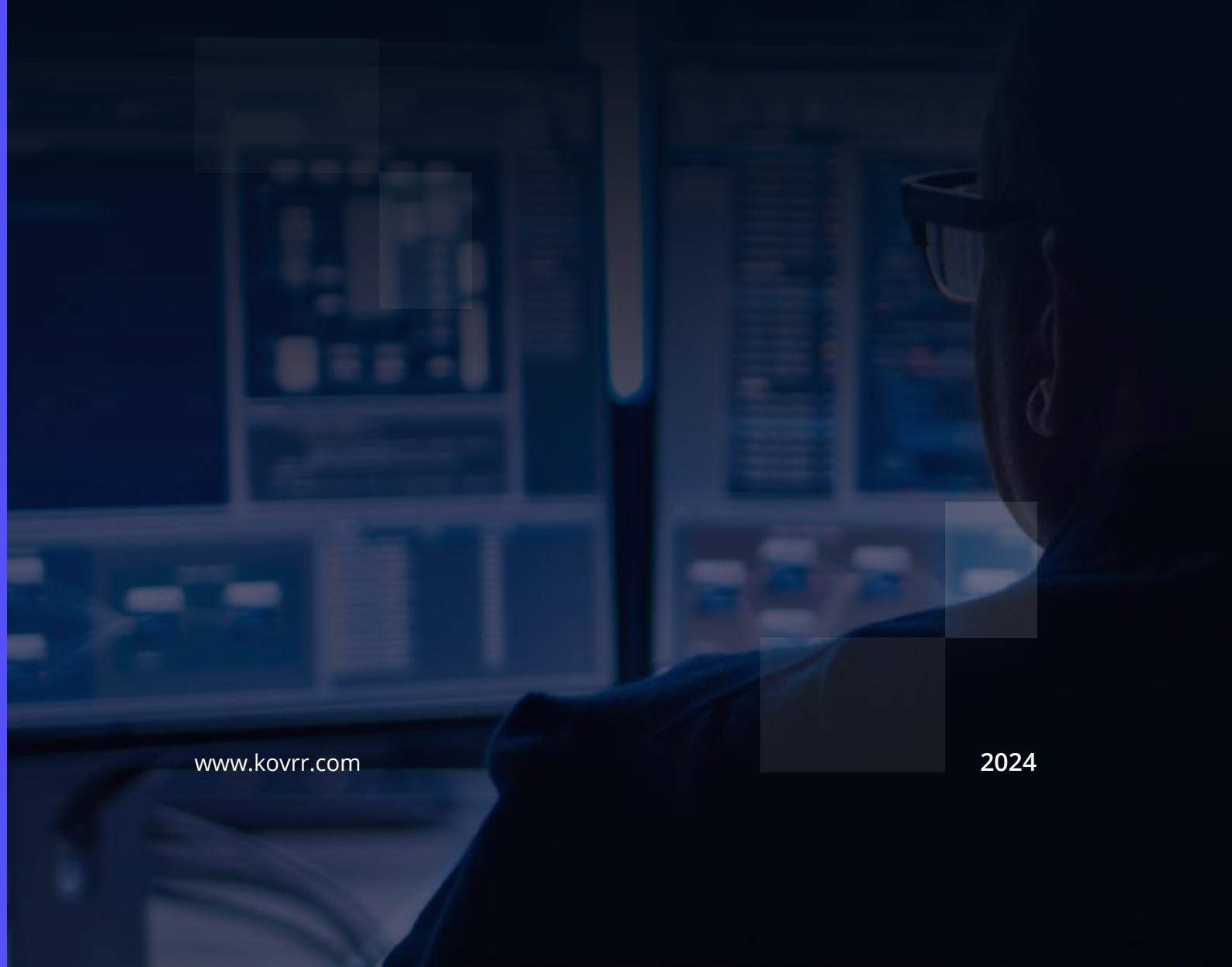
KOVRR
Cyber Decisions. Financially Quantified.

Complying With the New SEC Cybersecurity Regulations

A How-To Guide



www.kovrr.com

2024

Table of Contents

The Relationship Between Cyber Risk and the Marketplace

Since the SEC's latest cybersecurity regulations went into effect, thousands of companies have already been compelled to submit their annual Form 10-K with the novel Item 1C. Similarly, dozens of organizations have filed updated Form 8-Ks to disclose cybersecurity incidents. Slowly but surely, these public reports are helping investors become more aware of the intrinsic relationship between cyber risk and market value.

However, the information provided on these disclosures varies significantly per registrant. Some 10-Ks are highly detailed, including thousands of words and mentioning how the organization's chief information security officer (CISO) plays a key role in cyber risk management. Other 10-Ks are conspicuously sparse, with some registrants not bothering to fill in Item 1C at all.

While a reasonable investor might correlate cybersecurity robustness with the amount of respective data included in these annual filings, the overall inconsistency obscures the true nature of the broader market-cyber relationship. Moreover, with a slew of corporations submitting Form 8-Ks disclosing non-material cyber events, it has become evident there is a disconnect between the SEC's expectations and what entities are actually disclosing.

To help close this gap, Kovrr has created an in-depth guide explaining the SEC's underlying intentions with these new regulations. This How-To Guide also offers expert advice on how organizations can better comply to keep their investors informed, providing a robust framework that streamlines the disclosure process.

What Are the Latest US SEC Cybersecurity Regulations?

The impact cyber attacks have on US businesses increases each year. Over the past decade alone, the average annual cost of a data breach has nearly doubled, reaching $9.48 million in 2023.

Recognizing cyber's immense power on market stability, the Security and Exchange Commission (SEC) passed its July 2023 cybersecurity regulations to ensure this risk was accurately reflected and accounted for. As of the regulation's enactment in December 2023, publicly traded US corporations now face two major fiduciary changes in their disclosure practices.

Form 8-K, New Item 1.05

New Item 1.05 requires registrants to disclose materially impactful cyber events, providing information such as when the event was discovered, its nature and scope (includ-

ing the financial and operational consequences), and whether it's still ongoing. The new regulation also mandates that such incidents be reported within four business days of being deemed material. Follow-ups must be submitted if any new, relevant details subsequently emerge.

Moreover, organizations are expected to make the materiality determination with unreasonable delay, giving investors ample opportunity to assess the potential effects of the incident and make informed decisions. If registrants believe that the disclosure of the details poses a risk to national or public security, they can request a filing extension from the US Attorney General.

Form 10-K, New Item 1C

The new SEC rulings likewise adopted Regulation S-K Item 106, whose details should ultimately be included in Form 10-K, Item 1C. The new regulation requires that organizations describe their processes, should they have, for assessing, identifying and managing "material risks from cybersecurity threats." US SEC registrants must also share if they expect any of these material risks to come to fruition and, if so, the overall impact it would have.

As a part of this updated annual disclosure, companies are also required to describe the role both board members and senior management play in overseeing, assessing, and managing these material risks. It should be noted that the SEC's final ruling does not insist that boards or key executives maintain specific cybersecurity expertise; rather, the organization merely needs to state whether such expertise is present.

Why Organizations Are Having Disclosure Challenges: A Material Issue

Adhering to a new set of rules after operating so long without them would initially prove challenging for any entity. In the case of the new cybersecurity regulations, this difficulty is exacerbated by the SEC's requirement that registrants specifically report "material" cyber risks and incidents.

The existence of a materiality differentiator is undeniably critical, as investors would become overwhelmed by the sheer number of cyber risks an average organization faces daily. However, by providing a definition of "material" that leaves ample room for interpretation, the SEC has essentially negated its own mission of standardizing cybersecurity reports.

The Ambiguous Nature and Definition of Materiality

Leveraging US Supreme Court case precedent, the SEC considers a cyber event or risk material if:

"...there is a substantial likelihood that a reasonable shareholder would consider it important in making an investment decision or disclosure of the information would have been viewed by the reasonable investor as having significantly altered the total mix of information made available."

According to this definition, what constitutes materiality is intrinsically contextual, varying per an organization's makeup, including but not limited to its size, location, industry, and data sensitivity. The SEC's decision not to define the term too sharply, therefore, not only expresses a recognition of this unavoidable subjectivity but also signals an intent to compel executives to invest time and thought into the determination process.

Still, as evidenced by the inconsistencies and lack of information in Form 10-K, Items 1C, and Form 8-K, Items 1.05, stakeholders need more specific guidance that will support them in compliance and ensure investors are provided with the details necessary to make sound decisions.

A Data-Driven Framework to Assess Materiality and Ensure Compliance

Before pursuing any plan for developing a standard materiality determination framework, all key stakeholders should ensure they have a thorough understanding of what's newly required in the latest cybersecurity regulations. While the changes to Forms 8-K and 10-K are the primary ones, organizational leaders should familiarize themselves with other updates.

Click here to read the full, final ruling of the SEC's new Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure regulations.

After there is a shared understanding of what's required, the process of creating a framework can begin!

Step One: Establish Baseline Materiality Considerations

While CISOs are, for the most part, not the organization's cyber risk owners, they would still do well to assess the cyber risk landscape against various criteria. Cybersecurity leaders have the opportunity to step into greater leadership roles and demonstrate to upper management that their input is non-negotiable before signing off on any disclosures or legal reports.

Before meeting with these key stakeholders, CISOs should prepare a preliminary research report that takes into account the following metrics:

- Risk appetite and tolerance levels
- Potential financial impact, on average, of cyber events
- Insurance deductibles and likelihood of exceedance
- Potential brand consequences of a cyber event
- Data records quantities and sensitivity levels
- Operational interruptions and average event longevity

Once armed with this information, cybersecurity leaders are ready to communicate with the organization's risk owners and help develop a plan for assessing, identifying, managing, and (although hopefully not) reporting material risks and events.

Step Two: Collaborate With Executives, Board Members, and Risk Owners

While the materiality discussion should by now already be a top priority among business leaders throughout SEC-registered companies, CISOs can still take the initiative to ensure that these important decisions are being adequately invested in, offering their unique expertise. This cooperation helps parties align expectations with reality and ensure that the determination process has factored in all of the necessary business perspectives.

The core stakeholders that should be a part of this important exercise are:

- C-suite executives
- Boardroom members
- CISOs and security teams
- Internal compliance personnel
- Legal consultants

Step Three: Leverage CRQ to Calculate Basic Loss of Revenue Thresholds

After these crucial discussions have taken place, it's time to determine, on a practical level, whether the organization faces any material cyber risks. Harnessing all of the information ascertained during the collaboration process, in combination with the data gleaned from Kovrr's Cyber Materiality Report, CISOs and other key stakeholders can quickly identify material risks and take appropriate action to manage them.

Kovrr's Cyber Materiality Report

Recognizing the challenges many organizations face when generating a materiality determination framework, Kovrr's risk experts conducted extensive research to discover best practices, concluding that firms fare well when they begin this process with one basis point of revenue loss.

Consequently, the Cyber Materiality Report automatically plots this loss point, as well as several others, including a 10x (extreme) event point on a loss curve, to highlight an organization's most significant, most material risks, in combination with the likelihood of experiencing that type of event.

Our solution leverages these thresholds, along with the criteria agreed upon in Step Two, to compute the probability of an organization experiencing what it deems to be a material event. This feature provides further contextualization of potential losses, enabling organizational leaders to be better informed when selecting a threshold for reporting materiality.

Download a free sample materiality report from Kovrr today to learn more.

Step Four: Run Continuous Cyber Risk Assessments and Quantify the Risks

Considering how quickly the threat landscape evolves, managing cyber risk and remaining compliant with the SEC is an ongoing process. This continuous adaptation requires an on-demand cyber risk evaluation solution that automatically incorporates the latest cyber threat data and trends.

With this intelligence, CISOs and other cybersecurity leaders can be sure that they are accurately targeting material cyber risks, ensuring management processes are up-to-date, and, ultimately, keeping stakeholders informed.

Quantified Benchmarks for Material Determination: A Tried and True Method

Corporate use of quantified financial loss benchmarks is not a new phenomenon for devising a defensible process for materiality determination. Because the SEC similarly requires registrants to report other "material" business risks and incidents outside of cyber under the same definition (...a substantial likelihood that a reasonable shareholder...), there are many examples of executives using such thresholds as a starting point in their reporting frameworks.

In fact, every one of the Big Four accounting firms uses some form of quantified threshold when completing a preliminary determination of material impact. While what is considered to be a material accounting risk should not necessarily be applied to cybersecurity, the underlying approach of quantification has nevertheless proven historically useful for rationalizing materiality and remaining compliant with the SEC.

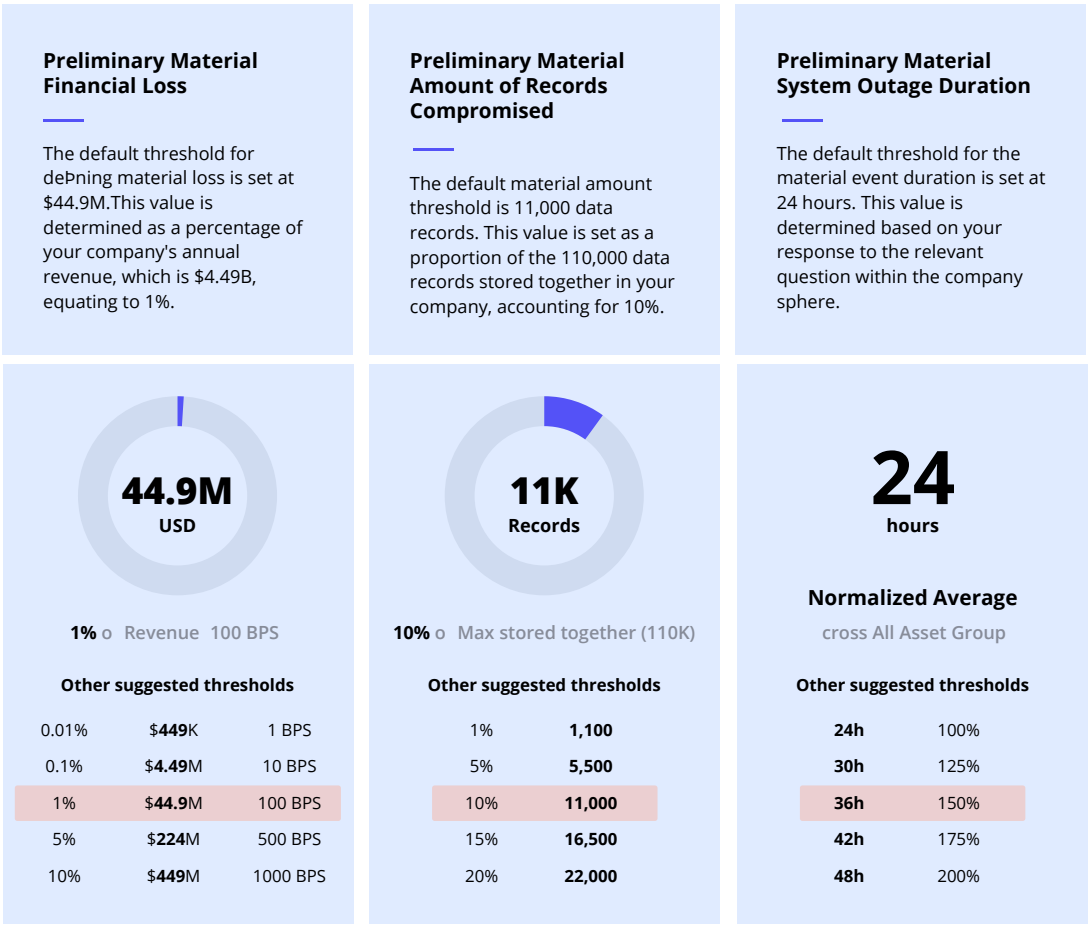
Moreover, the commission has also posited that an organization should specifically consider the "financial condition and results of operation (ROO)" when conducting materiality evaluations. Both of these factors are plainly cyber risk quantification (CRQ) outputs when applied to the new regulations, further demonstrating the value of quantifiable benchmarks in the material risk determination process.

How to Leverage Cyber Risk Quantification for Form 8-K Compliance

On-demand CRQ solutions, such as the one offered by Kovrr, can offer organizations quantified loss thresholds according to their specific revenue, data record amounts, and potential outage times. Using these metrics, CISOs, risk owners, and other key stakeholders should collectively decide the event consequences they would determine to be material.

For instance, for the organization evaluated in the figure below, the CRQ platform determined, based on industry standards and best practices, that based on its annual revenue of $44.9 billion, a loss of $44.9 million, equating to 1% of the total revenue, would be a solid indication that the event which precipitated the loss could be considered material.

Materiality Thresholds



With Kovrr's CRQ solution, organizations can quickly determine material loss thresholds.

Similarly, the quantification process has found that, given the organization's total number of stored data records, a loss or compromisation of 11,000 records, or 10% of the total, is a robust metric for determining if the incident should be reported to the SEC in Form 8-K. Finally, the CRQ solution found that an outage duration of 24 hours would likewise be grounds to file a disclosure.

While the 1% of revenue loss, 10% of data record loss, and 24-hour outage windows are benchmarks this particular organization has chosen to leverage for its materiality determination process, this CRQ solution also offers other calculations for companies to leverage should they want to adjust accordingly. For instance, stakeholders may decide that, in their case, it's better to consider a 5% revenue loss as their guideline for rationalizing materiality.

Regardless of the specific loss threshold organizations decide upon, these calculations can then be used to comply with the extremely short reporting deadline of the 8-K. Instead of scrambling around and wasting time examining all of the far-reaching consequences of the incident that took place, organizational leaders can use these metrics to assess the situation. They can ask themselves, "Did the event result in our agreed-upon revenue loss benchmark?"

In combination, risk owners should also evaluate the criteria assessed in Step Three. A situation could arise in which a preliminary loss threshold was surpassed, but after eval-

uating the other consequential criteria, executives determined the cyber attack ultimately not to be material. Vice versa, after examining the qualitative consequences, business leaders may decide that the event was, indeed, material, although it did not surpass the quantitative loss levels.

Even in such situations, the quick availability of these benchmarks and established criteria renders compliance a more straightforward, efficient process. Moreover, by having these clearly defined metrics in place, organizations can more easily defend their disclosure choices to the SEC and include the appropriate scope of information, highlighting their robust, data-driven determination framework.

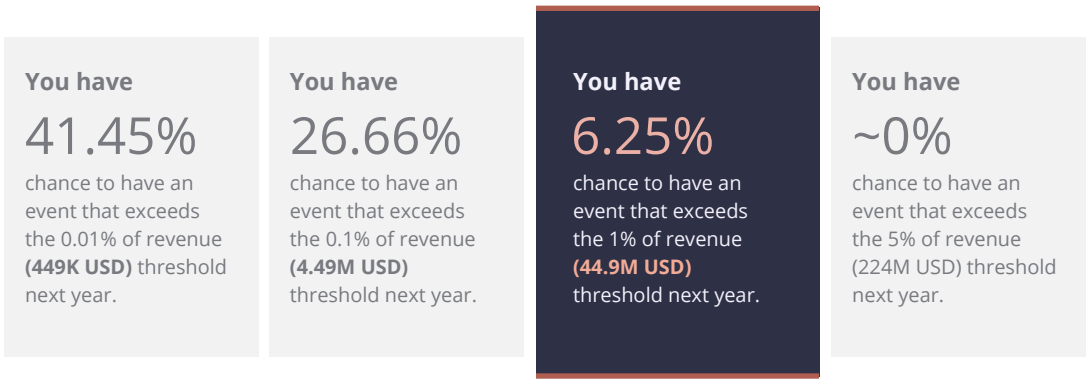
How to Leverage Cyber Risk Quantification for Form 10-K Compliance

With the loss thresholds, which can be adjusted according to organizational context, set in place, a CRQ platform with a materiality feature can then calculate the likelihood of experiencing that level of loss within the upcoming year, along with the type of cyber events most likely to lead to such a material event. When equipped with this capability and the ensuring outputs, CISOs and stakeholders are in a strong position to comply with Form 10-K, Item 1C.

For example, a CRQ solution such as Kovrr's can highlight how likely it is that an organization will experience a material revenue loss within the upcoming year. As seen in the figure below, the company has a 6.25% chance that, within the next year, it will be the victim of an attack that results in a loss of more than $44.9 million. This information alone proves valuable to a reasonable investor, primarily concerned with the safety of their returns.

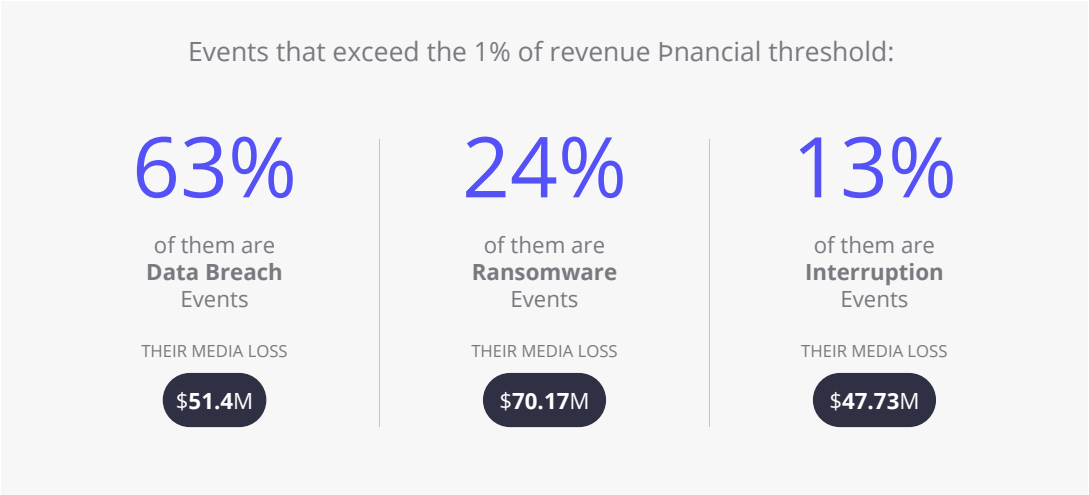
Likelihood Analysis

01 Preliminary Material Financial Loss



Kovrr's CRQ illuminates how likely an organization is to experience a material revenue loss.

By further drilling down this insight, CISOs can also make data-driven decisions, investing in mitigation efforts that reduce the overall likelihood of experiencing a specific incident with that severity level. For example, a cyber risk quantification analysis may illuminate, as in the case of the image below, that of those forecasted events that lead to a material revenue loss, 63% of them are data breaches, 24% ransomware events, and 13% business interruptions.



CRQ breaks down materially impactful events (based on revenue loss) according to type.

With these objective forecasts, stakeholders may decide to allocate more resources to security control upgrades that specifically decrease the likelihood of experiencing a data breach. Consequently, organizations can explain to investors and regulators in their 10-Ks that, by using CRQ, they've adopted a defensible framework for assessing, identifying, and managing their material risk of cyber threats.

The more information companies have regarding the material events they face and the ensuing consequences, the more proactive they can be with mitigation efforts and better protect investors. Download Kovrr's sample Cyber Materiality Report today to view the full range of metrics and insights CRQ can offer organizations to better comply with materiality reporting requirements.

Moreover, by translating cyber risk and its potential materiality into broader business terms such as financial loss, data record amounts, and outage times, CRQ enables non-technical executives and board members to actively engage in the determination process. One of the SEC's intentions with its new regulations was to ensure cybersecurity risk management was elevated to the highest organizational levels, and with this common language, it can be.

Incorporating Qualitative Factors When Defining Material Loss and Risk

In its new cybersecurity regulations, the SEC explicitly states that disclosures of material incidents and risks need to consider "all relevant facts and circumstances, which may involve consideration of both **quantitative** and **qualitative** factors." Therefore, while the **quantitative** loss thresholds provide a solid, data-driven starting point for the determination and subsequent disclosure of these events and risks, qualitative factors are just as crucial to assess.

Indeed, a disclosure that only included numerical thresholds would unequivocally be deemed non-compliant. The SEC's motivation behind leaving the definition of materiality

ambiguous was carefully calculated. The governing body wants to ensure that organizations invest the time and resources into exploring all of the potential contextual factors that may cause an event or risk to be deemed material. Only when combining both **quantitative** and qualitative implications can stakeholders credibly determine materiality.

The more **qualitative** components of a potential material incident or risk were those criteria examined in Step Three. Additional qualitative factors that can help stakeholders determine materiality in the cybersecurity realm include, but are not limited to:

- The organization's industry
- The nature of the business operations
- The type of data records it handles
- The potential reputational damage
- The ensuing effect on customers

Consulting With the Experts: A Fundamental Component for SEC Compliance

This How-To Guide offers CISOs, executives, and board members a data-driven approach to determining cyber materiality and complying with the latest SEC regulations. Nevertheless, these stakeholders must consult with other parties, such as legal counsel and auditors, to ensure the disclosures include the necessary information and meet the SEC's standards.

The materiality determination process is complex and requires significant investment, for which this How-To Guide cannot substitute. Still, preliminary quantified thresholds can be leveraged as the starting point in this process, offering a standardized methodology for organizational leaders who find complying with the new regulations challenging.

To learn more about how cyber risk quantification can aid organizations under the new SEC cybersecurity regulations, contact one of Kovrr's risk management experts today.