MARCH 2022

New regulation from the SEC to require companies to report how cyber risk could affect them financially.

The recent closure by Toyota of all of its Japanese factories was merely the most recent example of how paralyzing and damaging a cyber attack can be.

Against the backdrop of the growing frequency and severity of cyber attacks against enterprises; proposed new regulations from The Securities and Exchange Commission (SEC) are set to require publicly traded companies in the U.S. to analyze how cyber risk could affect financial statements.

Financial losses from cyberattacks are growing

A recent speech by SEC Chair Gary Gensler acknowledged just how financially damaging cyber risk has become, stating that "The economic cost of cyberattacks is estimated to be at least in the billions, and possibly in the trillions, of dollars".

The objective of the new rules are to strengthen the cyber security posture and resilience of businesses in general and the financial sector in particular.

The desire for enterprise decision makers to financially quantify cyber risk has long been strong internally, however the recent move by one of the most influential Wall St. regulators will give new impetus to invest in robust cyber risk management capabilities.

Learn more about how the Quantum Platform - Financially Quantify Enterprise Cyber Risk

The Importance of financially quantifying cyber risk

The regulations, which are still still open to public comment, would enable investors to have a faster way to identify and assess potential investment risks, They also push enterprise decision makers to ensure they have a robust approach to monitoring and mitigating their cyber risk exposure.

It's important to note that the SEC's new rules only apply to public companies. Private companies are not subject to these disclosure requirements, but they may want to consider voluntary disclosure as a way to improve their cyber security posture.

The spotlight being shone by the SEC on the financial impact is in line with a broader market evolution that elevates and views cyber risk as a critical business risk.

The benefits of understanding and communicating cyber risk in financial terms means that in addition to meeting regulatory requirements such as those proposed by the SEC and others, executives such as the CISO, CRO, CFO, board members and others can get the financially quantified answers they need around areas such as:

1 **Justifying Cybersecurity Investments** - Prioritize and justify cybersecurity investments that maximize risk reduction.

2 **Optimizing Cyber Insurance and Risk Transfer Placements** - Identifying gaps between risk mitigation options and cyber insurance spending to maximize your risk management decisions and strengthen business resilience.

3 **Measuring ROI of Cyber Security Programs** - Assessing the ROI of your cybersecurity program and stress test it based on potential risk mitigation actions, thereby supporting better resource allocation.

This approach is aligned with the overall intention from the SEC as is evidenced by Mr. Gensler's statement "I think companies and investors alike would benefit if this information were required in a consistent, comparable, and decision-useful manner." Platforms such as Kovrr's Quantum can deliver all these powerful data-driven insights on-demand with the click of a button.

Overview of the proposed regulations

The following is an overview of the three main areas the proposed new regulations will address:

* **Reporting Cyber Security Incidents:** Companies will be required to document and report the regulator if they suffer a material cybersecurity incident within 4 days of the event. They will also be required to periodically report the status of any cybersecurity incident that was previously reported.

* **Cyber Mitigation Strategies:** In addition to reporting when they have experienced a cybersecurity incident they will also be required to state which strategies they used to mitigate it.

* **Disclosing Cybersecurity Expertise:** The proposal will require annual reporting or certain proxy disclosure about the level of cybersecurity expertise represented on the board of directors. It will also seek to document what oversight the Board has on cyber security risk, and state the management's role and expertise is in assessing and managing cybersecurity risk and implementing cybersecurity policies and procedures.

Financially quantifying cyber risk in terms of dollars is an excellent way to demonstrate whether a cyber security event is material. Using our Quantum CRQ platform, organizations can do just that—evaluating the potential financial impact of a cyber attack and assessing if it is material or not.

Financially quantify, mitigate, and manage

The SEC's new rules are a step in the right direction for improving cybersecurity disclosure, however cybersecurity is a rapidly developing field, and organizations need to take a holistic and technology led approach to manage their risks.

This includes measures such as (1) Using a CRQ platform such as the Quantum to identify and financially quantify cyber risks, (2) assess and implement cyber risk mitigation strategies, and (3) monitoring ongoing and emerging risks.

To learn more about how Kovrr can help your organization comply with these new regulatory requirements, Book a demo with our experts.

The Author

Tom Boltman

VP Strategic Initiatives

About Kovrr

Kovrr's cyber risk modeling platform delivers global (re)insurers and enterprises transparent data-driven insights into their cyber risk exposures. The Kovrr platform is designed to help chief risk officers, chief information security officers, underwriters, exposure managers, risk professionals and catastrophe modelers understand, financially quantify and manage cyber risk by utilizing AI-powered risk models. To learn more please contact the Kovrr team: contact@kovrr.com