ThreatConnect.

Addressing the SEC Requirements for Materiality Disclosure

The Need for A Cyber Risk Quantification Approach

Introduction

Cybersecurity is becoming an issue to the "health and safety" of a company. Most companies have demonstrated sufficient resilience to cyber attacks, with a few exceptions, like the attack against Code Spaces (who was put out of business after attackers wiped all their company data). They have successfully recovered from ransomware attacks, data breaches, insider threats, and even destructive attacks. However, the past is not a reliable predictor of what may happen in the future.

On July 26, 2023 the U.S. Securities and Exchange Commission (SEC) adopted new rules addressing the cybersecurity of publicly traded companies, and foreign private issuers. The new rules include a number of elements, such as annual reporting about a company's cybersecurity risk management, strategy, and governance, and the disclosure of material cybersecurity incidents.

These rules are poised to elevate the visibility of cybersecurity in public companies and make it a more common and consistent topic of discussion for company leaders and board members. The role of the Chief Information and Security Officer (CISO) is going to get more visibility and scrutiny too.

Given the newness of these rules, and their scope, company leaders and directors are facing a period of uncertainty as they seek to understand, learn, and react based on how the SEC responds to the information and level of detail provided by companies in their quarterly and annual filings. This is going to be an evolving situation for several years.

Overview of the SEC Cybersecurity Rules

The SEC Rules on Cybersecurity are aimed at improving the visibility of the impact of cybersecurity activities and events for investors. The new rules will require companies to:

- Describe their processes for assessing, identifying, and managing material risks from cybersecurity threats, as well as the material effects or reasonably likely material effects of risks from cybersecurity threats and previous cybersecurity incidents.
- Describe the board of directors' oversight of risks from cybersecurity threats and management's role and expertise in assessing and managing material risks from cybersecurity threats.
- Disclose within four business days any cybersecurity incident they determine to have a material impact on the company, and to describe the aspects of the incident's nature, scope, and timing, and the material impact or reasonably likely material impact to the company.

These rules are an evolution of previous SEC requirements. Publicly traded companies have been disclosing elements of cybersecurity in section 1. A Risk Factors of their annual reports (10-K) for several years. However, the level of consistency and detail varied widely from industry to industry, and between companies in the same industry.

> **“Most organizations' materiality analyses will include consideration of the financial impact of a cybersecurity incident ”**
>
> Source - SEC Final Rule: Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure[1]

[1] https://www.sec.gov/files/rules/final/2023/33-11216.pdf

The Challenges for Public Companies

The SEC rules are aiming to improve the consistency and transparency of a company's cybersecurity activities to investors, which creates, or exacerbates, a number of challenges.

Improving the Communication and Awareness of Cyber Risks

CISOs and cybersecurity leaders face a perennial challenge of communicating cybersecurity and cyber risk to executives and board members. This is due to several factors.

- Risks are commonly measured in qualitative terms, e.g., as an output of multiplying the likelihood of a risk happening by its impact using numerical representations for qualitative values like "high, medium, and low."
- Cybersecurity is perceived as being like an insurance policy, e.g., it doesn't generate revenue or value for the company.
- It has, and continues to maintain, a perception of being a technology-focused area.

The result is that many executives don't understand and appreciate the purpose and nuances of cybersecurity, and cybersecurity leaders do not have the language or units of measurement that are understood by the business. This results in a disconnect in how CISOs communicate cyber risk to executives, and impacts how executives and board members without a level of cybersecurity awareness perceive and react to the information provided by CISOs.

Defining Materiality

A common theme across the rules is the concept of materiality. Materiality is generally defined as the quality of being relevant or significant. The SEC Cybersecurity Rules do not have a definition of materiality, leaving it to companies to determine. This introduces an element of uncertainty for companies that they must address in order to comply with most aspects of the rules.

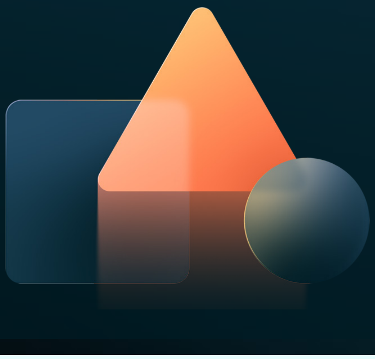
- How does the organization determine if a cyber attack or event is relevant or significant?
- How is an organization going to align its cybersecurity strategy to the most material cyber risks?
- How is the CISO going to prioritize cybersecurity investments across people, technologies, and services, and defend those decisions?
- How are executives and boards going to be assured that the most relevant cyber risks are being addressed?

Putting the Cybersecurity Strategy into Practice

Once a cybersecurity strategy is defined and agreed by the CISO, executives, and the board, it must be actioned and put into practice. Cybersecurity requires an investment proportional to the level of cyber risks acceptable to a company. It should cover the people, process, technologies, and services aspects required to execute and sustain the agreed strategy. The challenge for CISOs is ensuring and assuring that the investments are being applied appropriately, such that they are addressing and mitigating the most relevant risks. Without quantitative measures to know where to apply resources, and to what degrees, CISOs are left to make guesstimates. This makes assuring leaders, directors, and regulators that cybersecurity investments are appropriate and effective much more difficult.

Dealing with the Four Business Day Breach Notification

One of the most covered aspects of the SEC rules is the requirement that a company report a material breach within four business days. While the four-day rule has garnered much attention due its small number, the real challenge relates back to the challenge of defining materiality, as that is the trigger for the four day notification. Additional complexity introduced by the SEC rule is around cumulative incidents, that individually may not trigger a material event, but in aggregate may trigger the need to report. If an organization has not established their definition of materiality, then it creates a significant challenge, and risk, around determining whether or not to report.



Operationalizing Materiality with CRQ

In order to best position a company to address the SEC cybersecurity rules, they must be prepared to answer the question of how they define materiality. This is one of the most important actions a company must take. Organizations need to lay the scaffolding for how they define materiality and have a plan for ensuring that definition remains accurate by reviewing and refining the definition over time.

Once materiality is defined, i.e., a specific dollar financial impact to the company from a cyber event or events, the challenge is how to determine if the materiality value has been reached. This cannot be done effectively with a qualitative approach. Ordinal scales, stack ranking, etc. won't suffice. It requires quantification of the cyber risks facing a company and its business-critical assets. This is where applying cyber risk quantification (CRQ) is needed.

What is Cyber Risk Quantification?

Cyber risk quantification can be defined as a risk methodology that leverages data and analytics to compute the potential of a cyber event and its impact in financial terms. There are a variety of approaches used, such as FAIR, Hybrid FAIR, and proprietary ones. Regardless of the approach, the goals are the same - to provide a probability of a cyber risk occurring and magnitude of loss in financial terms if the event occurred.

How Does Cyber Risk Quantification Help with Materiality

Let's use temperature as an example. Everyone is familiar with qualitative means of describing temperature, like hot, warm, cool, and cold. The problem is that it varies by individual, and their perceptions, opinions, and biases. For example, someone living in Northern Canada is going to have a very different answer to what they think is "cold" compared to someone living in Arizona. A qualitative approach is too coarse when accuracy is needed.

How Does Cyber Risk Quantification Help with Materiality

But that's not enough. Not having the right measure can also impact the consistency of an output. Take cooking for example. Many recipes, like one for baking a cake, use volumetric measures like cups or ounces, but these are subject to variation based on the accuracy of the measuring cup and how a person uses it, e.g., is flour packed or sifted into the cup? Do you level the cup with a knife or eyeball it? The result is usually "good enough" but if a more accurate measure was used, like weight, it ensures an even higher degree of accuracy and a more refined and consistent output.

Using CRQ allows companies to have a highly accurate, common unit of measurement, that ensures consistent and comparable outputs, which is vital when needing to make a decision on whether a cyber event is material or not.

When employing CRQ, one of the first steps is gathering the data necessary to quantify risk. One set of data is the assets most critical to an organization. This can be done by looking at business-critical processes and identifying the assets used to deliver that process, like applications.

Another data source is historical loss records for cyber events, like ransomware and data breaches. The challenge is how does an organization collect all this information such that they have sufficient data to perform analyses with a high degree of accuracy and confidence?

Taking data and getting to quantification requires analysis. The analysis of cyber risk is done using a variety of techniques ranging from basic statistical models, to doing Monte-Carlo simulations, to using supervised and unsupervised machine learning based on the type of cyber threats and risks.

Quantitative outputs in the form of financial impact, measured in dollars for example, result from the analyses. These outputs can then be vetted and critiqued to determine if they are inline with the expectations of the company, and refined as needed. These financial impact outputs can then be used to help determine what is material to an organization across a variety of activities.

Enabling Open and Effective Cyber Risk Conversations

CISOs are challenged to effectively communicate and reach agreements on risk tolerance and mitigations, and executives and directors face the challenge of understanding the complex space of cybersecurity. CRQ breaks down the walls between these parties. Going back to our examples around communicating temperature or how to make a cake, having a common and highly accurate measurement is critical when discussing cyber risk. CRQ puts cyber risk in financial terms, which is a unit of measurement that is common and understood across a company. It removes the trap of discussing cyber risk in generic, ordinal measures and cybersecurity in technical terms, which introduces opinions and emotions, and a lack of understanding between parties.

Using quantitative measures that are universally understood and enable consistent comparison enables the open and effective communication and conversations that are needed. When discussing which cyber risks may be material to a company, the outputs from using CRQ make that discussion easy. For example, if a material impact is defined as $10 million and a ransomware event that impacts a business critical application could potentially create $20 million of loss due to being attacked, determined using a sound, defensible method, that leads to a much more effective discussion than one based qualitative estimates of likelihood and impact, and swags for potential losses.

Allocating Resources and Defending Cybersecurity Investments

Determining how much investment in cybersecurity is required, and where those investments need to be allocated is critical to address the SEC rules. With only qualitative-level details, this leads to CISOs making decisions primarily based on their past experiences, inputs from subject matter experts, etc. Defending budget requests and how resources are applied primarily based on "gut feel" leaves CISOs exposed when needing to defend their decisions, whether to executives, directors, or regulators. Using the example above, if a ransomware attack could cause a $10 million gap between expected loss and the materiality threshold, then it makes the decision to invest in more security for that application defensible.

Knowing When a Cyber Event is Material

One of the biggest impacts the SEC rules will have on companies is the four business day notification requirement. The challenge CISOs, counsel, executives, boards, and investor relations face is being prepared to report an event, and then being able to move fast and decisively if an event materializes. CRQ facilitates the discussions and agreement when defining materiality, and because it's a quantitative approach, it makes the decision on when to report defensible to regulators and investors.

Cyber Security as a Differentiator

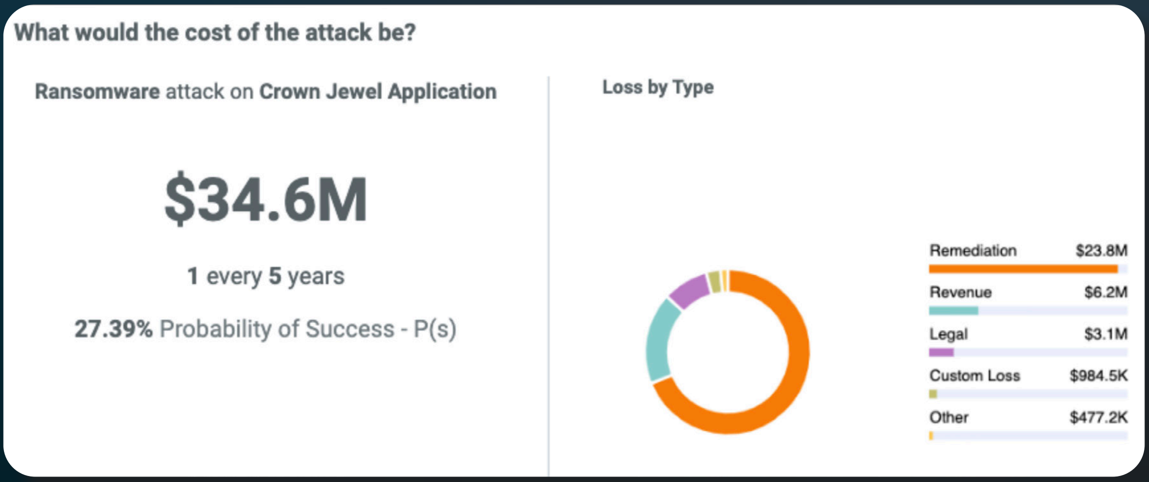
The SEC rules are meant to give investors more insights into how companies are addressing cybersecurity challenges, and reacting when events occur. A company that uses CRQ could be viewed as being a better investment opportunity compared to other companies. CRQ helps companies take a more holistic approach to cyber risk, demonstrating a commitment from the board on down to addressing cyber risk as a critical concern, in an efficient and optimized way.

ThreatConnect Risk Quantifier Democratizes Cyber Risk Quantification

Applying and using CRQ to help address the SEC cybersecurity rules does not need to be a painful journey of hiring cyber risk quantification experts and data scientists, then locating, aggregating and preparing the necessary data, letting the experts figure out the right models to analyze the data, and then validating outputs and refining the inputs to get to a number that can be believed and trusted.

ThreatConnect Risk Quantifier (RQ) enables CISOs and cyber risk managers to establish a CRQ capability in days, not months, by

- Automating the CRQ process. RQ brings the right data and applicable models, leaving users to critique the outputs
- Enabling CISOs to have meaningful, effective discussions and make wise, business-aligned, and defensible cyber risk and cybersecurity decisions
- Letting the CISO go from saying "no" to saying "yes with an IF" - changing cyber security decisions into a risk and business conversation



What would the cost of the attack be?

Ransomware attack on **Crown Jewel Application**

$34.6M

1 every **5** years

27.39% Probability of Success - P(s)

Loss by Type

Remediation	$23.8M
Revenue	$6.2M
Legal	$3.1M
Custom Loss	$984.5K
Other	$477.2K

Conclusion

The SEC Cybersecurity rules are going to force all public companies to address the impact of cybersecurity on their businesses, whether they want to or not. While it's still very new for many organizations, creating new areas of uncertainty for them, it cannot be ignored. The question is how does a CISO prepare for complying with these rules, especially the challenges with defining materiality. The answer is to adopt a cyber risk quantification approach now, before it becomes the norm, and reap the benefits in improved communications, awareness, and alignment with executives and directors, optimize cybersecurity investments to maximize risk reduction, and ensure meeting the SEC rules is done in an effective and defensible approach.

ThreatConnect.

ThreatConnect enables threat intelligence operations, security operations, and cyber risk management teams to work together for more effective, efficient, and collaborative cyber defense and protection. With ThreatConnect, organizations infuse ML and AI-powered threat intel and cyber risk quantification into their work, allowing them to orchestrate and automate processes to get the necessary insights and respond faster and more confidently than ever before. Over 200 enterprises and thousands of security professionals rely on ThreatConnect every day to protect their organizations' most critical assets.
Learn more at www.threatconnect.com.

ThreatConnect.com

3865 Wilson Blvd.,
Suite 550
Arlington, VA 22203

sales@threatconnect.com
1.800.965.2708