23 March 2022

Clarence Miller
Owner
Miller Cyber Security Consulting Services LLC

Hello,

My comment is regarding **S7-09-22** Cybersecurity Risk Management, Strategy, Governance (RSG), and Incident Disclosure. This seems to be an extension of the NIST Risk Management Framework (RMF) monitor step of security and privacy posture of systems and organization. Although NIST RMF is not a mandatory requirement for public trading companies to comply with, NIST's built in RMF monitoring procedures would seem the more logical approach to ensure disclosure of a company's true security posture and if incidents have or will occur based on the findings from ongoing monitoring.

Ongoing monitoring is the key to Risk Management, Strategy and Governance. In my humble opinion, there can be an extensive number of rules and regulations to require public trading companies to comply with. However, the critical piece to that compliance is through a form of ongoing monitoring, which means companies should have third-party assessor's/auditor's checking them on a bi-annual or annual bases, whichever is the more stringent for monitoring for a particular company.

To ensure that the companies risk management policies and procedures, Strategic principles and overall Governance are being followed and adhere to. Most companies are already doing this albeit most have tied this to their capital expenses. Since any new asset or add value to an existing asset is coupled with strategic value and risk management.

Would seem prudent to ensure any added risk is infused with the ability of the company to deduct those expenses through operational or tax purposes, as security and the reduction of risk to one's assets has a placed value, it should be part of your daily operating expense (e.g., remediation through operational expenses or insurance against the risk).

Having a company report on their Risk Management, Strategy and Governance through procedures both IS0 27001 and NIST SP 800-137 would allow for the granularity of seeing what risk is being overlook by the company and all disclosures that require reporting.

The key is identifying potential risk through Key Risk Indicators (KRI) and Key Performance Indicators (KPI) metrics in cyber and risk management. This can predicate if a company is trending in a particular trend would expose their risk.

Defining the particulars in what, when and how continuous monitoring should be conducted is the key. If it's left up to the individual companies, you will get different aspects of reporting of disclosure, based on what that company deems as important risk. For example, a whaling attack on high-profile employees' email, should this be report, - yes through the continuous monitoring of vulnerabilities of risk to a corporates email server and services how many and how often should be a metric collect and reported on through KRI. An assessor/auditor would have this data as part of their RSG

collected/correlated security data. Allowing for a comprehensive report too corporate board on the company's risk and compliance status.

Since this is ongoing, this would help the company trend it's progress over a given timeframe. This would also help the SEC in trending the potential incident of disclosure by looking back over time to see were the vulnerability/risk was overlooked that caused the disclosure.

In summation, yes, I agree this rule is needed, however, we should also add the benefit of outlining procedures to accomplish this rule which would help tremendously and not allow for disparage reporting. What I propose isn't new, just building on what sourced procedures already existing (e.g. ISO and NIST reporting) and utilizing it to better a company's reporting of Cyber Risk Management, Strategic and Governance.

Thank You,

Clarence T. Miller

Clarence T Miller
Miller Cyber Security Consulting Services LLC