Cyber Risk Report

Prior to becoming the Chairman of the SEC, Jay Clayton wrote, "cyber-threats are among the most urgent risk to America's economic and national security and the personal safety of its citizens." As recently as October 2017, the Co-Director of SEC Division of Enforcement identified cybersecurity disclosure as a priority and subject of potential enforcement "where there may be a cyber-related disclosure failure by a public company."

In 2017, the Healthcare Industry Cybersecurity Task Force noted the industry experienced more cyber incidents resulting in data breaches than any of the other 15 critical infrastructure sectors. According to a 2016 report by the Ponemon Institute, data breaches in healthcare are increasingly costly and frequent, and continue to put patient data at risk. The report estimates that data breaches could be costing the healthcare industry $6.2 billion.

In 2008, the Express Scripts Holding Company ("Company") disclosed a data breach affecting personal and medical information of over 700,000 customers.

The Company recognized in its 2017 10-K that:

[The Company's] ability to conduct operations depends on the security and stability of our technology infrastructure as well as the effectiveness of, and our ability to execute, business continuity plans across our operations. A failure in the security of our technology infrastructure or a significant disruption in service within our operations could materially adversely affect our business and results of operations.

However, the Company has not provided shareholders with a full report regarding this risk and its policies, procedures or other information concerning how it mitigates this risk.

RESOLVED: The Company's shareholders ask the Board to review and publicly report (at reasonable cost, in a reasonable timeframe, and omitting proprietary and confidential information) on its cyber risk and actions taken to mitigate that risk. A report adequate for investors to assess practices should include:

aspects of business or operations that give rise to material cyber risk;

the extent to which the Company outsources functions that have material cyber risks, descriptions of those functions and how the Company addresses those risks;

descriptions of cyber incidents experienced by the Company that individually or in the aggregate are material, including a description of costs and consequences;

risks related to cyber incidents that remain undetected for an extended period;

description of relevant insurance coverage;

compliance, regulatory or contractual obligations related to cyber risk;

certification to widely recognized standards; and

how cyber risks and cyber incidents are reflected in financial statements.

The report should also discuss the scope and frequency of the Board's oversight of cyber risks which may include review of relevant systems, policies, and procedures, related to:

- determining critical assets (e.g., customer information);
- employee training on data security and privacy-related risks;
- due diligence for third party vendors and potential acquisitions;
- data breach and incident response plans;
- minimization of data collection and retention; and
- security policies and audit frequency