Measuring Security Posture

To understand how stock price can be affected following a data breach, we bifurcated the companies according to their security posture, which is measured by the Security Effectiveness Score (SES). This proprietary methodology was developed by Ponemon Institute for its annual encryption trends survey to define the security posture of responding organizations. The SES is derived from the rating of numerous security features or practices.

This method has been validated from more than 50 independent studies conducted for more than a decade. The SES provides a range of +2 (most favorable) to -2 (least favorable) with a theoretical mean of zero. Hence, a score greater than zero is viewed as net favorable and a score less than zero is net unfavorable.

A high favorable score (such as +1 or above) indicates that the organization's investment in people and technologies is both effective in achieving its security mission and is efficient.

Data breaches are pervasive and companies with both a positive and negative security posture can experience the loss or theft of sensitive and confidential information. However, it is our belief that companies with a strong security posture are more resilient, and therefore will have a less detrimental impact on stock price than those with a weak security posture. Of the 113 companies, 57 had an average favorable score of +.67 and 56 had an average unfavorable score of -.71. Following are attributes of both a high and low SES.

Security Effectiveness Score Attributes

High SES

- Fully dedicated CISO
- Adequate budget for staffing and investment in enabling security technologies
- Strategic investment in appropriate security enabling technologies, especially enterprise-wide encryption
- Training and awareness programs designed to reduce employee negligence
- Regular audits and assessments of security vulnerabilities
- A comprehensive program with policies and assessment to manage third-party risk
- Participation in threat sharing programs

Low SES

- Lack of incident response plans
- Inadequate funding for staffing and investment in enabling security technologies
- Frequent turnover of IT security personnel
- Poor data retention practices
- The C-Suite values productivity of workforce over security
- Lack of collaboration between lines of business and IT security in determining IT security priorities