Quantifying Security Incidents

Annual loss expected (ALE) versus annual loss realized (ALR)

Executive Brief

Measuring the success and value of an information security organization is a perennial challenge. Companies in all industries have been struggling with how to consistently track the effectiveness of their Information Security Management Systems (ISMS) over time.

Adding to the challenge, security teams tasked with reporting to C-suites and boards require accurate metrics that are accessible and relevant to non-specialist audiences. Those audiences are used to judging value in dollars and cents… and Euros, Yen, and Yuan.

Thus the CISO is faced with the double challenge of quantifying the volume and impact of what didn't happen (the events their ISMS prevented), and attaching a monetary value to those non-events. Our experience in talking with our peers is that few have tried, and fewer still have persisted.

At Cisco, one way we're trying to quantify and communicate to leadership how well our ISMS is performing is through an innovative methodology for consistently quantifying security incidents against an established industry benchmark from the Ponemon Institute. We identified the benchmark, developed a process to consistently capture and quantify losses from our security incidents, and now compare actual to benchmark as a Board-level measure of operational effectiveness.

Annual loss realized (ALR) has given us a broadly accessible Board and C-level measure of security effectiveness. It has also supported decision-making in individual business units regarding security investments, and assisted in bringing visibility to the business impact of security incidents. The cost structure established for various types of incidents, combined with the historical data, supports leaders' investment decisions and the cost analysis of specific incidents. The data then drives targeted action.

This paper outlines the method by which we arrived at our ALR measure, and provides examples of how it is used. It is intended for all Information Security professionals, IT staff, and business people with an interest in security metrics.