Business executives routinely assess customer demand, resource availability, and other sources of market fluctuation, to keep their companies profitable. Significant time, effort and funding is spent on collecting the data needed for these assessments, as they are what ensures a company's continued growth. But the assessment typically only provides the information needed to make an informed choice. It is still the executives who make the final decisions, based on data that helps them to decide the risks associated on each potential path.

Security risk assessments are just as necessary to business profitability, and at times, survivability. They provide executives with the data they need to make informed decisions regarding security risk avoidance, risk acceptance, and risk mitigation. And although it is still the executive who makes the hard decisions, it's advantageous to have an external security professional provide what is and what is not relevant to a specific business, in terms of security related risks. A professional security assessment of each essential component of a business, to provide the information needed to ensure it can continue to function.

A security assessment begins with identifying those aspects of a business that are critical to its continued existence. Its brick and mortar resources, essential personnel, company branding, intellectual property, etc.; that have been built over time, and that have each played a part in its success.

Next is the identification of the possible threats to each of these components. What external (or internal) forces could jeopardize the continued success of each. And the treats run the gamut, from man-made…intentional and unintentional…to natural catastrophes.

And although there may be a variety of possible threats, the next hard question is what are the more probably threats. It's here that some of the more difficult decisions need to be made regarding what to spend your limited resources on, along the spectrum of the remotely possible to the highly likely threats to your specific business.

And if that call is not hard enough to make, you also need to evaluate the impact of each possible calamity. It may not make sense to spend large sums to protect yourself against a once in a lifetime possibility. But you may be willing to invest to mitigate a threat that is not likely, but would be catastrophic to your business, if the cost was right.

And there are a variety of ways to mitigate a threat to a successful business, from traditional security systems, to insurance, to a predefined recovery plan that accepts that some impacts to a business are just unforeseen, but still happen.

The bottom line is, all of this information needs to be compiled, specific to the business that's being assessed. It's a data driven exercise, guided by security professionals with a background in appropriately evaluating the threats, their likelihood, their impact, and the possible mitigation options. And then presenting the information to executives in a way that provides them with what they need to make the best informed business decisions.