Guidepost

PREDICTIVE INTELLIGENCE AND INTELLIGENCE FUSION – MOVING FROM THE DEMO TO REALITY

Today's threat environment is evolving at an alarming rate. Global and domestic acts of terror are occurring on a more frequent basis with catastrophic outcomes that resonate at a very visceral level within the corporate fabric, from key executives to line employees.

Competing for headlines with these heinous acts are the continual data breaches that erode the financial integrity fabric and brand value of major enterprises.

The profile of the perpetrators of acts of terror and corporate security breaches continues to change, with self-radicalization topping the present day list of motivation for attacking innocent victims. In a similar fashion, the profile and motivation for the cyber-related offender has shifted from a shadowy figure simply looking to skim some easy money to sophisticated rings of hackers looking to not only obtain financial gain but to cause irreparable reputational harm in the process.

Security leaders tasked with the protection of the personnel and assets of leading corporate organizations are being assailed on a daily basis by providers of technology and operational solutions that are purported to address these threats.

The challenge lies in separating the true enterprise risk reduction value offered by these solutions from the slick presentations and exhaustive lists of generalized benefits being pitched by the solution sales teams.

There is no silver bullet, and no single solution will address the specific needs of a global organization. A pragmatic, integrated approach must be taken to identify the solutions that resonate with each company's unique risk profile, corporate culture and level of executive support for the security function. Once the optimum solutions are identified, they must be implemented in a cohesive, relevant and collaborative fashion (a process of "fusion") that delivers the maximum real-world value from the predictive intelligence and risk-reduction investment, and this value must be linked to key business functions that have a material and significant impact to the company's bottom line.

The key concept to grasp in this environment, where the security department's value has been tied to critical business functions that represent millions to billions of dollars in risk, is that you are reframing the entire financial discussion with your leadership from "how much money are we going to save" to "how much risk are we going to avoid". When you deliver on this monetary risk reduction the ROI received by the company and the perception of the security function as a cornerstone of corporate shareholder value will be significant and measurable.

Read Complete White Paper

MATTHEW WHARTON SR.

President, Strategic Accounts

Matthew Wharton serves as president for strategic accounts. Mr. Wharton is a career security professional with more than 35 years of experience leading security consulting and integration firms. He designs solutions from "The Owner's Perspective" with improved recommendations that meet regulatory and fiscal requirements and transform internal functions from cost centers to sources for corporate investment that deliver increased integrity to the enterprise and enhance shareholder value.