Guidepost

SECURITY MATTERS – ARE YOU DOING ENOUGH?

Regrettably, most security programs are judged on past performance. If an organization has not experienced a security incident, the conclusion is that the program must be effective. As a result, organizations become complacent and often reduce their security posture over time. The ubiquitous financial investment disclaimer, "past performance is not an indicator of future outcomes" is applicable to an organization's security program. Moreover, many companies only review and re-evaluate their security practices after a significant incident has occurred.

Organizations with forward-thinking security programs are constantly reassessing their practices. Their leadership understands how the threat environment can rapidly escalate. They challenge existing constructs because they anticipate today's assumptions are inadequate to predict tomorrow's challenges.

What are you and your organization doing to challenge existing security assumptions?

Today's threat environment is constantly changing. Performing frequent security risk assessments and embracing scenario planning to challenge existing assumptions and formulate strategic options are requisite functions if an organization is to maintain a successful security program.

SECURITY RISK ASSESSMENTS

Security risk assessments serve as foundational elements designed to identify vulnerabilities and gauge the organization's tolerance for risk. The risk assessment process can effectively reduce risk exposure if recommendations to reduce vulnerabilities are acted upon, and simultaneously identify operational efficiencies to enhance situational awareness across the organization.

SCENARIO PLANNING

Scenario planning enables decision makers within organizations to contemplate a future state – anticipating how the ever-shifting threat landscape may adversely impact the business, clients, guests, and loved ones. Exercising scenarios facilitates the collective practice of problem solving to enhance decision making while facing adversity. It creates a dialogue about what actions are to be taken and when, under various conditions. Such planning efforts can shape the response strategy, make individuals aware of and recognize the downstream impact that is created based

upon a decision, and align a cohesive recovery effort. At the line level, scenario planning empowers associates and front-line responders to proactively engage in the security program.

Regardless of how impressive the security program might appear on paper, despite the colorful and carefully diagrammed workflows indicating appropriate actions to a predetermined event, security comes down to people – organizational culture. The organization that treats security simply as another function, implementing it as a knee-jerk reaction without a strategic objective that is curated overtime, will ultimately fail when called upon.

Conversely, organizations that embed security into the very fabric of their cultural norms, consistently re-evaluate their practices, and incorporate scenario planning into their program, tend to have effective comprehensive security programs.

Engaging an independent third-party firm experienced in security risk management and scenario planning can benefit organizations in the assessment of their existing security program objectively. In today's dynamic threat environment an outside perspective free of the constraints of administrative heritage can provide unique expertise, while reducing the business impact upon the organization.