Top 3 Reasons Third-party Cyber Risk Validation Makes Sense for Your Enterprise

svtara.com | (866) 802-9405 | sales@securityvitals.com

TARA

Why use a third-party for ongoing cyber risk validation?

Despite all the media coverage that touts the importance of managing cyber risk, it is a surprisingly overlooked component in day-to-day business operations.

Any organization that is not actively looking for evolving risk is simply rolling the dice with the business. And it's not just big companies that are the target of cyberattacks. For small to mid-size companies, the threat is even more real as most do not have the resources to recover from a significant cyber event. On average, 60% of these companies go out of business within six months of falling victim to a cyberattack.

So, why do some organizations adopt a passive approach to managing cyber risk? The reasons are numerous ranging from a lack of knowledge and resources to a belief it could never happen to them. Surprisingly, some companies that have experienced a cyber incident continue with business-as-usual approach under the false belief that lightning will never strike twice in the same spot. The simple reality is, it's not a question of if…it's a question of when a cyber incident will occur; and an organization that has experienced an incident is no less likely to experience another. In fact, the disclosure of a cyber incident may increase the likelihood of being targeted by malicious players again.

TARA

Why a Risk Barometer Makes Sense

So, how do organizations identify and address areas of growing risk? The simple answer is it depends on a variety of variables ranging from company size to industries served. Some industries have mandated compliance requirements for identifying, managing, and mitigating cyber risk. In these cases, a blend of people, process, and technology resources are applied to address ongoing requirements and monitor performance.

Even in firms with established cyber programs, there are recurring questions most executives find themselves asking such as how do I know if we are still exposed, and how do I explain it to our customers when a cyberattack shuts down the company? These are difficult questions, and there are no simple answers. Organizations that have established teams face a difficult dilemma when it comes to understanding risk posture and the likelihood that a cyber event may impact the business. Trusting the team is doing what they need to do but verifying the level of coverage for the business requires an effective form measurement. Dedicated cyber security teams have finite skills and knowledge. In other words, they know what they know; conversely, they don't know what they don't know. Finding a risk barometer to consistently evaluate exposure is an effective way to solve this challenge.

Top 3 reasons why third-party cyber risk validation makes sense

The market offers many options for evaluating cyber risk. From a strategic standpoint, organizations should investigate solutions that address the specific concerns of executive leadership. Irrespective of the unique features a particular risk validation offering may provide, the value should be evident in three specific ways:

Cost Effective

Third-party risk validations are money well spent. With the average cost of a data breach hovering at $8 million, ongoing third-party risk validations are a fractional cost to the alternative. Beyond the financial implications, it's also important to consider the impact of reputational damage and how it will affect an organization.

Broad Experience

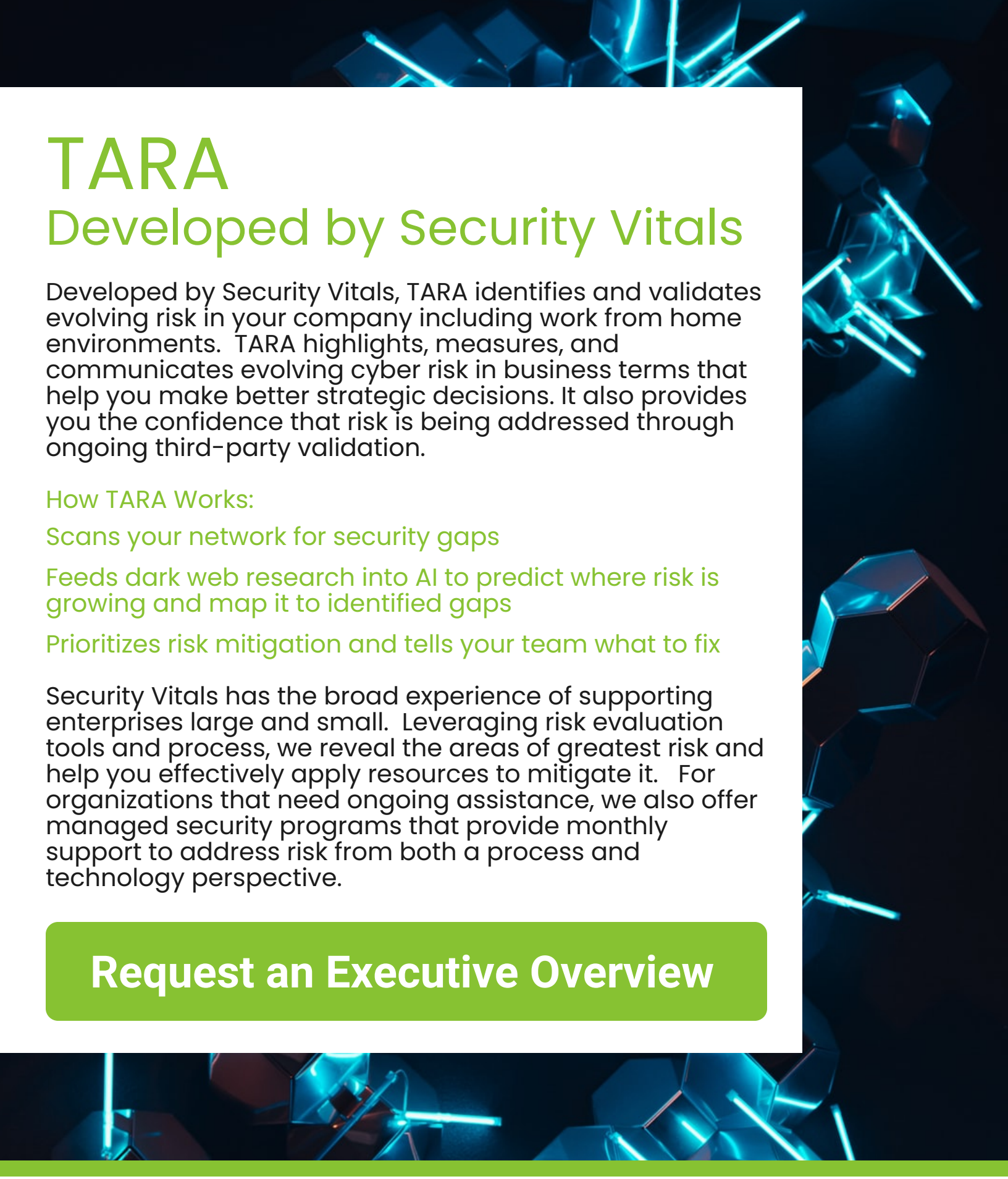
Any reputable risk validation offering includes access to resources that can answer questions and provide specific guidance on how to address areas of concern. This depth and breadth of experience will augment internal team capabilities and help drive improvements across the board.

Improved Insights

Knowledge is power and having a firm grip on evolving risk improves both strategic and tactical initiatives. Effectively managing cyber risk requires an ongoing blend of internal and external perspectives. Third-party risk validations improve visibility and inject unbiased feedback into the organization. This detail supports decision making across the enterprise.

Effectively managing any business requires actionable data to make informed decisions. From a cyber risk perspective, executives want to know their organization is protected. Third-party risk validations are an important component for any organization looking for sustained performance.

TARA



TARA

Developed by Security Vitals

Developed by Security Vitals, TARA identifies and validates evolving risk in your company including work from home environments. TARA highlights, measures, and communicates evolving cyber risk in business terms that help you make better strategic decisions. It also provides you the confidence that risk is being addressed through ongoing third-party validation.

How TARA Works:

Scans your network for security gaps

Feeds dark web research into AI to predict where risk is growing and map it to identified gaps

Prioritizes risk mitigation and tells your team what to fix

Security Vitals has the broad experience of supporting enterprises large and small. Leveraging risk evaluation tools and process, we reveal the areas of greatest risk and help you effectively apply resources to mitigate it. For organizations that need ongoing assistance, we also offer managed security programs that provide monthly support to address risk from both a process and technology perspective.

Request an Executive Overview

svtara.com | (866) 802-9405 | sales@securityvitals.com

TARA