By Timothy Hall

A Tailored Approach to Assessing Cyber Risk

To reduce problems, organizations need to align supplier assessment and third-party monitoring plans with cyber-risk criteria.

All organizations are dependent on their supply chain and third-party relationships. And in the drive for operational efficiency and competitive advantage, these relationships become more interdependent and interconnected, creating a host of potential cyber risks.

Some estimates claim that up to 80 percent of cyber breaches may occur in the supply chain; accordingly, organizations must rethink their traditional supplier assessments. The key is to identify cyber risks aligned to their business and incorporate this situational awareness into their strategies and tactics.

Standard Oversight Methods Insufficient

Organizations devote time, money and resources gathering third-party, cyber-risk data in an effort to better manage their overall enterprise cyber-risk position. But this data collection can be a drain on the organization — and a source of additional enterprise risk. For most companies, supplier monitoring and third-party oversight manifest as onsite assessments and system-testing. This results in those organizations dealing with a multitude of annual on-site assessments, penetration (pen) testing, self-assessments and questionnaires.

These monitoring and oversight programs are typically based on two best practices:

- Ranking suppliers based on inherent risks, such as access to networks and protected data, and the potential to impact the enterprise
- Using security standards or self-assessments to provide a holistic image of an organization's cyber-risk profile and highlight specific vulnerabilities or risks.

Most monitoring plans strive for some level of onsite assessment and system testing. Companies faced with the cost and logistics of assessing hundreds or thousands of suppliers are logically forced to align their monitoring methodology to the supplier's risk ranking. Suppliers are typically ranked based on their inherent risks and potential impact to the organization. For example, tier-one

suppliers likely undergo more detailed cyber-security oversight, such as formal onsite assessments and pen testing, while lower-ranked suppliers receive more cursory monitoring, such as self-assessments or questionnaires.

Build an Effective Assessment Program

However, these traditional ranking and assessment methods can be flawed. Tiered rankings miss specific cyber risks in lower-ranked suppliers, and many different types of supplier assessments generate mountains of data that is difficult to analyze and integrate into operational decision-making. Take, for example, Target's 2013 breach, which was initiated through a HVAC supplier's stolen credentials. It is unlikely that many organizations would have ranked that HVAC supplier as a tier-one supplier that required detailed cyber-security oversight.

Thus, an effective assessment program should be built around the cyber risks specifically related to your enterprise. To efficiently manage your supply chain partners, your monitoring strategy should be founded on two items:

- A supply chain cyber-risk criteria that is structured and aligned to your cyber-risk profile and your tactical and strategic business plans
- A methodology that efficiently ingests and presents monitoring data to shape current tactical and strategic business decisions.

Reshape Your Monitoring Strategy

Enterprise cyber-risk criteria is formed from a detailed understanding of your cyber-risk position and how your suppliers and partners impact your vulnerabilities and risks. The focus is on your cyber-risk characteristics, not the importance of the third party to your business. Mapping these risks to your suppliers and third-party partners should provide the foundation of your assessment strategy.

Most assessment methodologies provide a broad overview of an organization's security position. However, if your cyber-risk criteria include, for example, counterfeits and taints, completing a standard assessment or questionnaire will not provide the needed insight. Instead, lower-ranked suppliers with specific risk areas — for example, those susceptible to tainting or those using online billing — should be highlighted in the ranking process. By identifying these risk categories and suppliers, you can efficiently tailor your monitoring strategy across your supplier base.

Your monitoring strategy should also account for constant changes in the supplier landscape. Aligning your contracting structure to your monitoring strategy can help account for these inevitable changes.

Create an Effective Data Integration Strategy

Supply chain partners looking to reduce the cost and resource burdens of multiple assessments frequently seek to reuse already completed assessments or self-assessment questionnaires across their supply chain partners. But doing so can be daunting and unmanageable for those receiving the information. Depending on the method, each of these assessments can address 80 to 300 different security control areas. And while these assessments and questionnaires cover essentially the same key cyber-risk areas, they pose slightly different questions and require different evidence. The result is a complex maze of unmanageable data and reporting.

Shelves of assessments may keep regulators at bay, but they won't help your risk management or competitive position. The key is to get needed information into the organization so you can make better decisions. Your data integration strategy needs to enable information reporting at two levels:

1) Procurement and supplier management, to support contractual management oversight
2) Enterprise risk management, to support strategic, operational and risk-transfer decisions.

With a supplier assessment strategy that earmarks key data, framed by the cyber-risk criteria and supply management business drivers, organizations can quickly capture and allocate critical or bellwether trends for distribution and action. Depending on your desired level of integration and sophistication, the data can be integrated into regular business reporting, from stop-light charts to detailed and prioritized risk-mitigation plans.

Tailor Your Approach

While traditional approaches to supplier and third-party management may seem to answer requirements for third-party monitoring, the inherent complexity and resource burden often prevents meaningful absorption of the data.

Without the ability to efficiently identify and react to vulnerabilities identified in the monitoring process, a company may miss a risk-reduction opportunity or be held accountable for not taking corrective action after being informed of a material cyber risk.

Thus, to reduce potential problems in the supply chain, an organization should focus its supplier assessment and third-party monitoring plans around methodologies and tools that highlight risks aligned with its specific cyber-risk profile and support dialogue between corporate leaders and operational management teams. ISM

Timothy Hall is the president of Azorca Cyber Security, LLC in Mesa, Arizona.