Third-party security assessments

Historical assessment process

The current model in assessing third-party security/ third-party risk is time consuming, resource intensive, and often not well correlated to actual risk. Even with an ever-changing cybersecurity landscape, companies often use static questionnaires that provide only a snapshot of the third party's cybersecurity posture. Resource constraints force difficult decisions and leave large portions of the third-party population unassessed. Companies are forced to rely on a triage process with little guarantee that it is followed, leaving them vulnerable. While this is the way things have been done, what if there was a better approach? What if we could assess all third parties using the existing time and resource limits? What if we included statistical analysis, current attack trends, and heuristics to rate a third party's security posture more accurately? Using machine learning and artificial intelligence has allowed a program to be developed centered around these principles. Now it is possible to assess an entire third-party population while keeping up with the fast-changing cybersecurity landscape.

Most third-party risk management programs require a due diligence questionnaire that can be quite lengthy and cumbersome. These questionnaires are often a one-size-fits-all approach and, in many cases, do not accurately or adequately assess the third party. The questionnaires are not well tailored to the specific third party's risk profile, include questions that are irrelevant, include inherently unreliable "attestation"-based questions, and are often completed by personnel who lack the needed subject matter knowledge.

Adding to the difficulty of these questionnaires is the time it takes to review and follow up with any items that are not in line with the company's expectations. Third parties fall through the cracks due to time limitations and the need to meet sales goals and project deadlines. Corners are cut and data is needlessly exposed using unencrypted files and unsecure email clients. But what if we could simplify the process? How do we make sure we have visibility into our entire third-party pool and that our data is protected?

Using a one-size-fits-all mentality for a questionnaire is not beneficial for anyone. These questionnaires contain questions that are unnecessary and, in many cases, rely on respondents who are not knowledgeable about the subject matter. The questions can be misconstrued, leading to inaccurate risk ratings. This increases the cost for all parties and can paralyze the assessment process.

In addition, the questionnaire process is static. It is nothing more than a point-in-time snapshot of a third-party's cybersecurity posture. Questionnaires are not well correlated with current cyber incidents because they are not updated frequently enough to keep up with the changing landscape. Often these questionnaires are simply a compliance measure and in the case of cyber insurance are rarely used by underwriters to determine premiums and coverages.

Modern thinking towards assessments

So, what's the fix? How do we design a risk-based approach that allows us to focus on the most critical third parties and not view every third party through the same lens? How do we develop a program that will give us more than a snapshot and will be intuitive enough to adapt to the changing cyber landscape?

Using a combination of expected business impact in the case of a cyber incident to define overall third-party cyber risk and the criticality of a supplier's role within your organization, it is possible to greatly decrease the number of third parties that receive a questionnaire. Additional information on third-party risk could be found using services that rate the cybersecurity posture of organizations. This increased knowledge would allow companies to better rate their existing third-party population and focus on those who have been classified as a high or critical risk.

This approach combines the real-time, high-scaling features of automated threat and vulnerability monitoring with the higher-fidelity details garnered from questionnaires and allows for the prioritization of the highest-risk third party. Creating a third-party cyber risk management program in this manner makes it possible to achieve 100 percent risk coverage visibility and allows prioritizing deeper-dive attention on those with the highest risk.

This increased visibility not only allows better visibility into third-party risks, but also makes it more possible to ensure compliance with the changes of data and privacy laws. For example, GDPR contains a specific requirement to perform an assessment of "the measures envisaged to address the risks, including safeguards, security measures, and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation," but does not specify how this assessment should be conducted. FDA regulations require adherence to GxP —but GxP is not defined for third-party security. FTC requires companies to "use reasonable information security practices to protect consumers' personal information." While none of the regulations dictate specifically how third-party cyber risk should be managed, the regulations do advocate that reasonable protective measures should be taken. Using this method will reduce risk due to the increased visibility on the third-party population and allow for more focused assessment where significant risk exists.

One thing to consider with this model is that continuous monitoring is built in using programs that are continuously rating the cybersecurity posture of third parties. If changes do occur, then the model can apply this new information and give visibility into the changes. If the new information changes the third party's risk score, then it can be quickly determined if the third party should be flagged for review. This additional knowledge will help a business owner to determine if any further action is necessary and if any additional due diligence, mitigation, and monitoring are needed to reduce the risk.

Simply relying on questionnaires to measure the risk of your third-party pool only provides a snapshot in time and does not truly give you visibility into the security posture of your third parties. A program that relies on analytics and data-driven decisions, powered by technology, will give you a much more accurate view of your third parties. This process provides a scalable and more relevant assessment solution that reduces the time and cost required to onboard a new third party and monitor the risk levels of existing third parties on a more frequent cadence, enabling companies to have a much more robust and effective program.

Contact us

Chetan Gavankar
Principal
Cyber Security Services
E: cgavankar@kpmg.com

Stephen Paradise
Senior Associate
Cyber Security Services
E: sparadise@kpmg.com

Christoph Henle
Associate
Cyber Security Services
E: chenle@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia