Dans de nombreux cas, les entreprises n'ont rien fait à cause de la nécessité perçue d'augmenter le budget et le personnel pour effectuer les tâches VRM. En effet, de nombreuses approches du VRM exigent des engagements importants de temps et de ressources - non seulement pour mettre en place le programme, mais aussi pour effectuer des audits, des évaluations et un suivi continu. En outre, de nombreuses organisations ont du mal à trouver des personnes possédant les compétences adéquates pour suivre les risques liés à la cybersécurité grâce à un système VRM. Par exemple, de nombreux gestionnaires des risques peuvent comprendre les risques juridiques et réglementaires, mais sont peu conscients du paysage des menaces liées à la cybersécurité.

Bien que certaines organisations disposent de programmes de gestion des risques pour les fournisseurs, les systèmes qu'elles utilisent reposent sur des questionnaires complexes. Beaucoup de temps est consacré à la configuration et à la gestion inefficaces du système, à l'envoi et à la réception de questionnaires et à la saisie d'informations - un processus lent et lourd qui expose les entreprises au risque.

Un système VRM moderne permet à une entreprise d'avoir une large visibilité en quasi temps réel, ce qui permet une utilisation efficace du personnel qualifié.

Les systèmes VRM traditionnels ont des faiblesses supplémentaires. Par exemple, les informations collectées peuvent être inexactes ou périmées, car elles représentent généralement la position de sécurité d'un fournisseur uniquement à un moment donné, ce qui rend une entreprise vulnérable jusqu'à la prochaine évaluation planifiée. Pour contrer cela, les organisations doivent être en mesure de surveiller en permanence les fournisseurs, mais les exigences en ressources peuvent être coûteuses et chronophages. Une autre lacune fréquente est de suivre uniquement un sous-ensemble de fournisseurs, généralement ceux du niveau le plus élevé, laissant ainsi un large éventail de fournisseurs non surveillés. Lorsque des lacunes sont constatées, les systèmes VRM traditionnels ne permettent souvent pas la collaboration entre l'entreprise et le fournisseur pour résoudre les problèmes.
Cependant, un système VRM moderne permet à une entreprise d'avoir une visibilité large, en temps quasi réel, en utilisant efficacement un personnel qualifié. Cela signifie également que l'entreprise peut évaluer et réduire les risques posés par ses fournisseurs et partenaires commerciaux tout en limitant les dépenses et les ressources pour le faire efficacement.

LES BESOINS DU VRM : VITESSE, EVOLUTIVITE, COLLABORATION

Une stratégie VRM moderne doit répondre à trois ensembles de besoins pour être efficace.

- **VITESSE**. Parce que des menaces graves et malveillantes peuvent apparaître rapidement et de manière inattendue, il est important d'identifier rapidement les risques. Une solution VRM efficace devrait aider les entreprises à gérer les risques en temps quasi réel. De plus, comme de nouveaux fournisseurs apparaissent fréquemment dans les écosystèmes des entreprises en croissance, une telle solution devrait permettre aux entreprises d'évaluer ces nouveaux fournisseurs à mesure qu'ils apparaissent. Une solution VRM qui identifie le risque sur une base mensuelle sera peu utile pour défendre une entreprise contre une épidémie de ransomware en évolution rapide telle que WannaCry.
- **EVOLUTIVITE**. Les entreprises ont besoin d'un système pouvant grandir d'un petit déploiement initial pour englober tous les fournisseurs au sein d'un écosystème d'entreprise, en particulier à mesure que les entreprises et leurs écosystèmes se développent. Le nombre de fournisseurs augmente régulièrement dans un large éventail de catégories, telles que le marketing numérique, la gestion des opérations et l'Internet des objets. Une solution VRM évolutive exploite l'automatisation pour ajouter des fournisseurs économiquement, sans nécessiter de ressources supplémentaires. Il a la capacité de suivre les fournisseurs à tous les niveaux, pas seulement le top.
- **COLLABORATION**. Une solution VRM devrait permettre la collaboration entre une entreprise et ses fournisseurs pour faire face aux risques et éviter les problèmes. Par exemple, une baisse du score de risque d'un fournisseur devrait entraîner une discussion entre une entreprise et le fournisseur pour identifier et corriger les faiblesses. Pour réduire les risques rapidement, une collaboration efficace et rapide entre une organisation et ses fournisseurs est cruciale.

LA SOLUTION BITSIGHT

Les cotes de sécurité BitSight pour Vendor Risk Management offrent des informations précises sur les performances de sécurité de toute organisation en analysant et en surveillant continuellement les informations sur les systèmes compromis, la configuration de sécurité, le comportement des utilisateurs et les violations de données. Les cotes de sécurité BitSight sont observables de l'extérieur, ce qui signifie que BitSight n'effectue pas de tests de pénétration ou d'attaques malveillantes sur un réseau d'entreprises pour collecter des informations et produire une évaluation.

BitSight Security Ratings pour VRM permet aux entreprises de prendre le contrôle des risques de sécurité auxquels elles sont confrontées et de réagir de manière proactive aux menaces de sécurité émergentes en coopération avec les fournisseurs de leur écosystème.

Pour plus d'information, voir https://www.bitsighttech .com/security-ratings-vendor-risk-management. www.bitsighttech.com

Cybersel
Via Lessolo 3
10153 Torino Italie
www.cybersel.eu

A propos de Cybersel
Cybersel est un leader de solutions de cyber sécurité. Cybersel a supporté le projet Bitsight dès le
début et est maintenant l'un des partenaires de Bitsight Cyber Security Rating les plus expérimentés dans la zone EMEA.

Contact France :
Alain Melamed - Tel : 33 6 80 7 13 16
Email : alain.melamed cybersel.eu

Contact Italie :
tel: 39 011 2 81121
Davide Turina - Tel : 39 3 9 6038 6
davide.turina cybersel.eu

COMMENT BITSIGHT AIDE A FAIRE EVOLUER L'APPROCHE ACTUELLE DE L'EVALUATION DU RISQUE PARTENAIRE

PAR DAVE FACHETTI | JUIN 2017

Bien que votre programme actuel de gestion des risques fournisseurs (VRP) puisse avoir des points forts, il y a certainement place à l'amélioration. Les programmes de gestion des risques des fournisseurs constituent un important facteur de temps pour les conseillers internes et externes, extrêmement coûteux et d'envergure limitée.
Comment pouvez-vous exploiter avec plus de perspicacité, à l'échelle de votre programme, et vraiment comprendre en continu la cybersécurité de vos tiers ?
En utilisant BitSight Security Ratings, vous pourrez voir un impact positif sur votre programme VRM en tirant plus de valeur de ce que vous faites déjà.

Le nombre de fournisseurs et d'autres tiers dans votre écosystème continuera de croître. En fait, selon un récent rapport de Bomgar, «en moyenne, 181 vendeurs ont accès au réseau d'une entreprise au cours d'une même semaine, soit plus du double du nombre enregistré en 2016. En fait, pour 81% des entreprises », la popularité croissante du cloud, l'introduction de nouvelles technologies et les demandes croissantes de la part de l'entreprise font en sorte que votre travail ne cesse de gagner en importance.

Il y a trois domaines principaux où BitSight peut immédiatement améliorer l'efficacité et l'échelle de vos programmes VRM existants. Assurez-vous de vous poser les questions suivantes : Qui, quoi, quand ?

1. QUI : SUR QUELLES ENTREPRISES DEVRAIS-JE ME FOCALISER POUR DES EVALUATIONS OU DES AUDITS ?

Lorsque vous faites une évaluation de votre portefeuille de fournisseurs, il n'y a aucun moyen d'obtenir une image claire et continue de la cybersécurité pour toute une gamme d'entreprises avec des questionnaires annuels. Les questionnaires fonctionnent bien, mais les cotes de sécurité BitSight ajoutent plus de perspicacité et de données exploitables lors du choix des entreprises sur lesquelles se concentrer. En plus des considérations actuelles telles que la criticité de la relation, le type d'informations échangées (est-ce réglementé?) et les interactions passées, BitSight vous fournira une évaluation numérique facile à comprendre, 12 mois d'historique et une répartition des risques de chaque fournisseur.
Grâce aux cotes de sécurité BitSight, vous pouvez cibler les sociétés dont les notes sont faibles et examiner l'analyse sous-jacente. C'est un complément exceptionnel aux mesures d'évaluation déjà en place. Pour aller plus loin, des outils sont fournis pour collaborer avec vos fournisseurs sur les problèmes de sécurité, identifier les mesures de correction qu'ils prennent et déterminer comment cela affectera votre relation de travail.

2. QUOI: SUR QUELLES QUESTIONS DEVRAIS-JE ME FOCALISER DANS MES ÉVALUATIONS QUAND JE M'ENGAGE AVEC CES SOCIÉTÉS?

Sur la base des données fournies par BitSight, vous pouvez adapter les questions dans les évaluations en fonction de leur notation. Vous pouvez également utiliser BitSight pour valider la plupart des réponses que vous recevez en retour.

Au lieu d'un questionnaire général destiné à une variété d'entreprises ayant des paysages de sécurité radicalement différents, BitSight vous aide à tirer le meilleur parti de votre processus existant en adaptant vos évaluations à des fournisseurs spécifiques en fonction de leur notation individuelle et historique. Par exemple, vous pouvez remarquer qu'un contrôle de sécurité est soit absent, soit inefficace dans la tierce partie que vous vous apprêtez à visiter. Lorsque vous êtes sur le site, vous concentrer d'abord sur ces domaines peut vous aider à comprendre leur approche de contrôle et de mise en œuvre de processus pour ce domaine spécifique, et pourquoi cela pourrait mener à ce que vous avez observé. Cela peut également vous donner un meilleur contexte pour l'équipe avec laquelle vous vous engagez et leur environnement lorsque vous examinez et évaluez les domaines restants de votre évaluation de leurs contrôles.

3. QUAND: QUAND DEVRAIS-JE M' ENGAGER AVEC CES ENTREPRISES?

Vous pouvez utiliser BitSight Security Ratings pour gérer votre rythme d'interaction avec vos fournisseurs. Au lieu de recourir à l'arrangement standard annuel, le calendrier des missions devrait être davantage axé sur les événements. Lorsque vous êtes averti de la modification de l'indice BitSight d'un fournisseur, utilisez-le comme pilote pour établir la connexion avec lui.
Les environnements sont dynamiques et le fait de synchroniser votre visite autour d'un changement significatif de cet environnement peut vous aider à mieux comprendre comment vos fournisseurs abordent de tels changements au plus près des événements qui se produisent. Cela peut ajouter un bon contexte à la façon dont vous pouvez penser à l'organisation et à sa gestion de tels risques.
L'utilisation de BitSight Ratings peut à la fois compléter et enrichir le processus d'évaluation déjà en place, vous permettant de vraiment intensifier votre programme VRM. En tant qu'entreprise ou conseiller, vous devriez poser de meilleures questions directement fondées sur un risque élevé dans un environnement ciblé, ce qui aura un impact positif sur les résultats de votre entreprise. BitSight peut vous aider à le faire.
Pour en savoir plus, téléchargez notre ebook "Creating efficiencies in Vendor Risk Management", pour obtenir des informations sur la manière de simplifier et d'optimiser le processus VRM.

RENDRE LA GESTION DU RISQUE FOURNISSEUR COLLABORATIVE,ET NON COMBATIVE

PAR NOAH SIMON | SEPTEMBRE 2017

Réduire le cyber risque qui découle des fournisseurs tierces et quartes parties n'est pas une tâche facile. Ceci exige que les organisations aient non seulement la capacité de surveiller et d'identifier continuellement les nouveaux risques, mais aussi la possibilité de travailler avec leurs fournisseurs pour résoudre rapidement les problèmes de sécurité. La réduction rapide des risques signifie que les deux organisations communiquent efficacement, en utilisant des données et des preuves plutôt que des conjectures pour progresser.

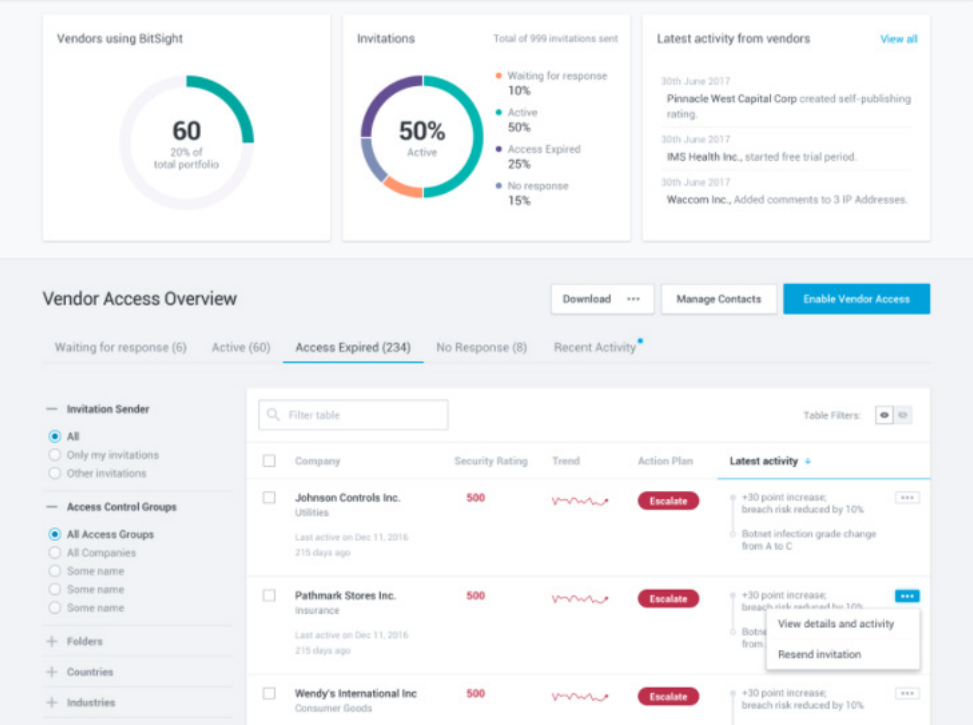
Les cotes de sécurité sont utilisées pour supporter ces conversations axées sur les données, ce qui permet aux entreprises de savoir pourquoi les performances de sécurité de leurs fournisseurs ont récemment changé ou pourquoi un problème particulier a émergé sur leur réseau. Cependant, les organisations ayant de grandes chaînes d'approvisionnement peuvent avoir des centaines de conversations avec des fournisseurs simultanés. Ils ne peuvent pas se permettre d'attendre plusieurs jours pour obtenir une réponse de chaque fournisseur : plus ils reçoivent des réponses rapidement, plus ils sont susceptibles de prendre une décision à temps pour éviter tout risque de transfert vers leur propre organisation.

Les clients BitSight permettent de plus en plus aux fournisseurs d'accéder au portail, pour leur permettre d'examiner gratuitement leur note et les détails qui s'y rapportent. À ce jour, près de la moitié des entreprises invitées à la plate-forme ont augmenté leur note de 37 points en moyenne, ce qui permet aux clients de réduire plus rapidement leurs risques et d'améliorer la sécurité de leur écosystème commercial.

Cette fonctionnalité a été renforcée, pour permettre aux clients d'avoir rapidement un aperçu des fournisseurs qu'ils ont invités et de mieux comprendre les problèmes qu'ils étudient.
La page Vendor Access Dashboard permet aux clients de voir qui ils ont invité sur la plate-forme BitSight pour répondre à des questions telles que:

- Quel est le statut de mon invitation? Le fournisseur à qui j'ai donné accès s'est-il connecté à la plate-forme BitSight ?
- Quelles actions mon fournisseur a-t-il entreprises pour améliorer leur note BitSight Security Ratings et leur posture de cybersécurité ?
- Est-ce que leurs ratings et/ou risk vector grades se sont améliorées depuis que je leur ai donné accès au portail BitSight ?

Les clients peuvent filtrer en fonction des dossiers de leur portefeuille pour suivre le statut d'un groupe de fournisseurs particuliers, ou même suivre le statut des fournisseurs qu'ils ont invités qui présentent un type particulier d'infection ou de vulnérabilité. Par exemple, une entreprise peut filtrer pour identifier les fournisseurs qui n'ont pas répondu à des niveaux spécifiques de criticité.



Les professionnels de la sécurité et du risque ne devraient plus avoir à surveiller chaque fournisseur avec lequel ils travaillent individuellement. Non seulement c'est un processus lourd mais il empêche également les organisations d'élargir leurs programmes de gestion des risques des fournisseurs.
BitSight permet d'atteindre les fournisseurs en masse et d'identifier instantanément les entreprises qui ont répondu à des problèmes potentiels et celles qui ne l'ont pas fait. La gestion des risques des fournisseurs doit être davantage une discussion collaborative que combative. Que vous soyez un client BitSight ou non, cette amélioration de la plateforme BitSight Security Rating aidera les professionnels du risque et de la sécurité à travailler ensemble.