1

Introduction

Les entreprises actuelles se focalisent fortement sur les compétences fondamentales et sur les facteurs clés de la réussite. Couplée à une croissance rapide de l'activité SaaS (Software as a Service), cette approche conduit à une externalisation accrue de certaines fonctions métier au profit de fournisseurs qui les mettent en œuvre de manière plus efficace, plus rapide ou plus économique. Aussi, les relations avec des tiers se multiplient ; une situation qui n'est pas sans avantages… ni conséquences.

Par exemple, une grande entreprise peut entretenir de 50 000 à 100 000 relations fournisseurs. Elle peut ainsi croître plus rapidement que si elle tentait de tout faire en interne. **Mais, si le nombre de relations fournisseurs se multiplie,** le risque concomitant augmente également. Et dans un environnement actuel de plus en plus interconnecté, lorsqu'il s'agit du risque lié aux fournisseurs, le cyber-risque est sous les feux de la rampe.

Dans cet e-book, nous allons examiner la manière traditionnelle d'appréhender la gestion des risques liés aux fournisseurs, ou VRM (Vendor Risk Management), déterminer pourquoi les stratégies traditionnelles seules sont inadaptées, et prodiguer aux responsables VRM des conseils sur la manière de réduire efficacement le cyber-risque.

2 Suivant
Tactiques VRM traditionnelles

2

Tactiques VRM traditionnelles

Pour comprendre parfaitement le mode de gestion traditionnel du risque lié aux fournisseurs, vous devez prendre en compte ses deux facettes : d'une part, le consommateur des services tiers (c'est-à-dire, le client), et d'autre part le prestataire des services tiers (c'est-à-dire, le fournisseur). En outre, dans des contextes différents, nombre d'entreprises sont à la fois clients et fournisseurs. Le problème survient lorsque le client ne connaît pas réellement tous ses fournisseurs, et encore moins le risque qu'ils font courir à leur clientèle, à leur fonctionnement, à leurs informations sensibles et à leur activité dans son ensemble.

Pour répondre à cette situation, les entreprises doivent réaliser un inventaire exhaustif de toutes leurs relations fournisseurs, déterminer et catégoriser le risque posé par chaque fournisseur, déléguer la prise en main de ce risque aux différentes composantes de leur organisation, instituer une protection contractuelle contre ce risque, et mettre en place un programme d'évaluation continue visant à surveiller, contrôler ou passer en revue le degré de conformité du fournisseur. Enfin, en cas de problème, elles devront identifier un responsable pour remédier à la situation.
Il va sans dire que ce processus n'est pas une mince affaire. Habituellement, à ce stade, les entreprises font appel à des méthodes de gestion des risques, telles que des évaluations, questionnaires, audits, tests de pénétration et analyses de vulnérabilité, pour les appliquer à leurs fournisseurs.

Si ces méthodes sont d'un réel secours pour déterminer les risques posés par chaque fournisseur, elles ne sont pas sans failles.

Défis liés aux tactiques VRM traditionnelles

Elles sont extrêmement chronophages.

Les organisations possèdent différents degrés de tolérance au risque et réalisent un certain nombre de contrôles de cyber-sécurité. A ce titre, elles élaborent des questionnaires qu'elles adressent à leurs fournisseurs afin de déterminer si ces derniers sont en mesure de gérer les risques dont elles se préoccupent. Tant pour l'entreprise que pour le fournisseur, répondre à ces questionnaires et vérifier les pratiques de cyber-sécurité prend du temps. Or, si en matière de questionnaires, il existe des normes qui facilitent le processus, ces derniers n'en restent pas moins laborieux.

Elles brossent un tableau incomplet du risque.

Les méthodes VRM traditionnelles sont particulièrement délicates à manier. En effet, elles ne sont valables et représentatives de la sécurité d'un fournisseur qu'**à un instant T**. Par exemple, si votre entreprise examine les contrôles de sécurité des données d'un tiers et les trouve satisfaisants, sitôt franchie la porte de sortie, cette bonne impression n'est déjà plus valable. En effet, sur une période de six mois, la plupart des fournisseurs sont susceptibles de modifier leur infrastructure informatique des dizaines, des centaines, voire des milliers de fois. En d'autres termes, la conformité d'un fournisseur aujourd'hui n'est pas identique à celle de demain.

En outre, les tactiques VRM traditionnelles sont souvent **subjectives** par nature. Si un client demande à un fournisseur s'il dispose d'un programme de gestion des changements efficace, la réponse va dépendre de la définition du mot « efficacité » chez le fournisseur, ainsi que de sa connaissance du programme de gestion des changements. L'approche devient donc inutile, à moins que le client ne soit en mesure de tester et de contrôler les informations obtenues.

Elles ne sont pas entièrement exploitables.

Certes, après avoir appliqué des tactiques VRM traditionnelles, telles qu'une évaluation méticuleuse, vous pouvez en retirer un sentiment général sur le positionnement d'un fournisseur en matière de cyber-sécurité. Toutefois, le destinataire de l'évaluation du fournisseur peut avoir du mal à comprendre pleinement les informations reçues et à les utiliser pour protéger son entreprise et ses données. Ainsi, si nous consacrons beaucoup de temps à *identifier* les risques potentiels liés à un fournisseur, nous n'en consacrons pas assez au *traitement* de ces risques.

Conformité n'est pas synonyme de sécurité.

Vous assurer que vos fournisseurs font ce que vous leur demandez constitue une mesure adéquate. Et comme nous l'avons mentionné auparavant, ce point est important. Mais vous devez également comprendre qu'il ne suffit pas que le fournisseur coche une case pour que cela signifie qu'il protège correctement vos données. Autrement dit, même si vos fournisseurs sont en conformité avec vos politiques de risque, des incidents de sécurité sont toujours susceptibles de se produire sur leurs réseaux, et peuvent avoir une incidence sur vos données. Vous devez donc vous focaliser essentiellement sur la gestion des risques liés aux fournisseurs, et non pas simplement sur la conformité de ces derniers. Si la conformité constitue un objectif solide à court terme, la gestion des risques liés aux fournisseurs est une pratique continue à ne pas négliger.

Par exemple, en matière de cyber-sécurité, il peut s'avérer difficile d'évaluer le « facteur humain ». Imaginons qu'un fournisseur ait mis en place une politique globale relative aux pare-feu, stipulant quels ports peuvent et ne peuvent pas être ouverts ; une règle préalablement imposée dans le cadre de leur contrat avec le client. D'un point de vue extérieur, la politique de pare-feu est parfaitement fondée. L'entreprise la met en œuvre et la gère correctement, et tout le monde semble satisfait de son efficacité. Toutefois, le « facteur humain » intervient lorsqu'un utilisateur se trompe

et met le pare-feu hors service. Le fournisseur lui-même peut ne pas savoir qu'il n'est plus en conformité, et le client encore moins.

Aussi, il reste une question à se poser : comment vous protégez-vous dans cette situation ? Les stratégies d'identification et de protection en amont constituent deux méthodes disponibles. Nous allons examiner ci-après quelques-unes de ces nouvelles stratégies et technologies dédiées à la VRM, et déterminer en quoi elles sont essentielles.

3 Suivant
Stratégies VRM émergentes

3

Stratégies et technologies VRM émergentes

Pour faire court, les tactiques traditionnelles de VRM sont parfois justifiées, mais ont tendance à se montrer chronophages, à effectuer un tableau incomplet du risque associé à un fournisseur et à se révéler inexploitables. Toutefois, un certain nombre de technologies et stratégies émergentes peuvent aider les responsables VRM dans leurs tâches quotidiennes.

Applications de surveillance continue.

En matière de VRM, l'une des plus grandes incertitudes réside dans les moyens de s'assurer réellement que les tiers avec lesquels vous êtes en relation respectent leurs obligations de sécurité. Certaines solutions de surveillance continue aident les clients à contrôler la cyber-sécurité de leurs fournisseurs au quotidien, et non pas seulement le jour de leur évaluation. Ces solutions permettent de visualiser facilement et rapidement de nouveaux risques et vulnérabilités susceptibles de menacer vos données via votre fournisseur. Disposer d'un outil accessible et facile à utiliser pour surveiller les fournisseurs en temps réel aura un impact durable sur les capacités de cyber-sécurité actuelles et futures.

Processus normalisés.

Si vous êtes un fournisseur tiers travaillant avec 100 000 clients qui veulent tous connaître le degré d'efficacité de votre programme VRM, un processus de certification normalisé prouvera que vous prenez beaucoup de mesures adéquates pour sécuriser votre entreprise et vos données. Par exemple, décrocher la certification ISO 27001 (une certification de gestion de la sécurité des informations émise par l'Organisation internationale de normalisation) exige beaucoup de temps et d'efforts. En tant que

client, si vos fournisseurs clés sont conformes ISO-27001, vous savez qu'ils attachent de l'importance à leurs programmes de cyber-sécurité.

Comme nous l'avons vu précédemment, conformité n'est pas synonyme de sécurité. Il n'en demeure pas moins qu'elle garantit un réel niveau de rigueur et de détail.

Surveillance des risques liés à plusieurs niveaux de fournisseurs

La surveillance des risques liés à plusieurs niveaux de fournisseurs constitue une stratégie VRM émergente qui modifie la manière d'aborder les risques liés aux fournisseurs. Cette approche prend en compte les fournisseurs de votre fournisseur. En d'autres termes, en tant que client, vous devez comprendre que votre fournisseur a lui-même des fournisseurs, et ainsi de suite. Cette réalité implique que si la sécurité du fournisseur de votre fournisseur est compromise, et qu'elle impacte votre fournisseur, vos données sont susceptibles d'être menacées.

Aussi, les fournisseurs de fournisseurs doivent être examinés avec le même degré d'attention et de diligence. Les solutions automatisées d'exploration des risques liés aux fournisseurs d'une entreprise constituent une avancée et vous aident à identifier les vulnérabilités dont vous n'aviez peut-être pas conscience jusqu'à présent.

4 Suivant
Faciliter la VRM

4

Trois manières de faciliter la VRM

1. **Continuer de se tourner vers des solutions plus automatisées.**

   Intégrer les solutions et mises en œuvre VRM qui arrivent sur le marché contribue à assurer une certaine cohérence. Par exemple, si vous avez établi une relation fournisseur avec une structure verticale avec laquelle vous n'aviez encore jamais travaillé, vous devrez probablement examiner toute une nouvelle série d'exigences de cyber-sécurité spécifiques à cette structure verticale. Le recours à des solutions automatisées telles que celles décrites ci-dessus contribuera à la cohérence de ces nouveaux processus.

2. **Mettre un processus en place et s'y tenir.**

   Pour gérer correctement les risques liés aux fournisseurs, vous devez savoir qui est chargé de cette gestion. Lorsque vous entamez votre processus VRM, identifiez dès le début les responsables clés. Cette approche éliminera toute confusion initiale.

3. **Faire de votre positionnement en cyber-sécurité un avantage.**

   En tant que client, vous connaissez tout le temps, l'énergie et les efforts nécessaires pour déployer un programme complet de gestion des risques liés aux fournisseurs. Mais quoi que vous entrepreniez, n'envisagez pas ce processus comme une corvée chronophage. Différenciez plutôt votre programme de cyber-sécurité par la qualité de sa gestion, de son contrôle et de sa maintenance, particulièrement en matière de risque lié aux fournisseurs.

   En tant que fournisseur, montrez que vous gérez activement votre cyber-sécurité et que vous avez mis en place des contrôles appropriés. Cette approche jouera certainement en votre faveur dans vos relations clientèle. Les fournisseurs qui présentent des programmes robustes doivent les « vendre » comme un atout et les utiliser comme facteur de différenciation face à la concurrence.

Pour savoir comment la plateforme de notations de sécurité BitSight peut contribuer à alléger vos responsabilités en matière de risques liés aux fournisseurs, demandez une démonstration gratuite dès aujourd'hui.

DEMANDER UNE DEMONSTRATION GRATUITE

A propos de ersel

erselest un leader de solutions de Cyber Sécurité. Cybersel a supporté le projet BitSight dès le début et est actuellement un des partaires de BitSight Security Ratings les plus expérimentés dans la zone EMEA.

Contact France :
Alain Melamed - Tel : +33 6 80 74 13 16
Email : alain.melamed@cybersel.eu

Contact Italie :
Eurosel MoMa Srl
Via Lessolo 3
10153 TORINO - ITALY
tel: +39 011 2481121
Davide Turina Tel :+39 3494603846
davide.turina@c ersel.eu