board of cyber
Beyond Rating.

LIVRE BLANC

Risque cyber fournisseurs

Les entreprises en attente de solutions nouvelles

NOVEMBRE 2023

ÉDITORIAL

Une question stratégique

LIVRE BLANC
Risque cyber fournisseurs

Le contexte de recrudescence des cyberattaques portées contre la chaîne d'approvisionnement et de sous-traitance des entreprises et des organisations rend aujourd'hui urgent d'identifier de nouveaux moyens efficients pour gérer ce risque. C'est la raison pour laquelle Board of Cyber a décidé d'interroger un panel d'entreprises afin de mieux comprendre leurs attentes face à un risque, d'autant plus difficile à évaluer, qu'il émane souvent d'un grand nombre de partenaires de l'entreprise, de taille différente et dont la maturité en matière de risque cyber n'est pas toujours homogène.

Pourtant, traiter ce risque est une question stratégique, car un fournisseur peut fort bien être le « cheval de Troie » d'une attaque informatique.

Ce sujet est devenu tellement critique que l'Union Européenne, via le règlement DORA applicable au secteur financier et la directive NIS2, entend renforcer le pilotage du risque fournisseurs. Notre étude révèle qu'une entreprise sur deux va modifier son approche à la lumière de ces nouvelles réglementations.

L'étude souligne également à quel point les entreprises sont en attente de solutions nouvelles, au-delà des outils qu'elles utilisent déjà. La demande de rationalisation et d'automatisation est forte et les équipes de Board of Cyber sont mobilisées pour travailler à des réponses opérationnelles.

Luc DECLERCK
Directeur général de Board of Cyber

Un risque « très important » pour 1 entreprise sur 2

LIVRE BLANC
Risque cyber fournisseurs

Board of Cyber a interrogé les entreprises afin de mieux comprendre la façon dont elles apprécient le risque cyber lié aux fournisseurs et la manière dont elles le gèrent. Voici les principaux enseignements de cette étude.

49 %

Le risque cyber fournisseurs est jugé « très important » pour 49 % des entreprises interrogées et « important » pour 41 % d'entre elles. Le niveau de préoccupation est donc élevé pour 90 % des entreprises ! Pour autant, ce risque n'est suivi par le conseil d'administration que dans une entreprise sur deux (48 %)...

67 %

Le risque fournisseurs est analysé sur certains d'entre eux seulement (67 % des cas), dont les niveaux de risques sont évalués en grande majorité en fonction de la criticité des services, de la sensibilité des données traitées, du degré d'insertion du fournisseur dans le système d'information et de la nature de la relation commerciale.

60 %

Dans 60 % des entreprises interrogées, la fréquence d'analyse du risque cyber fournisseurs est annuelle. Le rythme est semestriel pour 10 % des entreprises, trimestriel pour 16 % d'entre elles, mensuel dans 10 % des cas. À noter qu'une seule entreprise conduit cette analyse à un rythme quotidien.

80 %

Dans la grande majorité des cas (80 %), le risque cyber fournisseurs est géré par le RSSI groupe et/ou des Business Units concernées. Dans 40 % des cas , la direction des achats est également impliquée.

À SAVOIR

Board of Cyber a mené cette étude auprès d'une trentaine d'entreprises de l'industrie et des services, dont 18 gèrent plus de 1 000 fournisseurs

Une multiplicité d'outils et de méthodes

LIVRE BLANC
Risque cyber fournisseurs

Plan d'assurance sécurité, certification, analyse des risques, audit, notation cyber... Une large majorité d'entreprises utilisent ces outils de façon combinée.

Comment les entreprises évaluent-elles le risque fournisseur ? Toutes les entreprises interrogées citent le plan d'assurance sécurité, la certification, le questionnaire d'analyse des risques, l'audit et la notation cyber, une large majorité d'entreprises utilisant ces outils de façon combinée. Il faut remarquer que la notation cyber est utilisée par 42 % des entreprises interrogées.

Les entreprises impliquent leurs fournisseurs dans la gestion du risque, sous de multiples formes, dont les plus citées sont des clauses contractuelles, des échanges réguliers, des comités de pilotage, des comités sécurité pour les fournisseurs les plus critiques, des prises de contact ponctuelles lors d'évènements particuliers et d'incidents, des réunions de revue des projets.

Il est à noter que 52 % des entreprises interrogées vont modifier leur approche du risque fournisseur dans le cadre des nouvelles réglementations NIS 2 et DORA. Cela prendra la forme d'un renforcement du suivi du risque, d'un effort de documentation, d'une augmentation du nombre d'audit sur davantage de fournisseurs ou de la mise en œuvre d'une méthode d'évaluation systématique, impliquant toutes les parties prenantes dont les achats.

À SAVOIR

42 %
des entreprises utilisent la notation cyber

52 %
des entreprises vont modifier leur approche du risque fournisseurs

80 %
des entreprises ont mis en place des procédures formalisées pour impliquer leurs fournisseurs dans la gestion de leur performance cybersécurité

Un manque de temps et de moyens

LIVRE BLANC
Risque cyber fournisseurs

Board of Cyber a cherché à identifier les difficultés des entreprises dans la gestion du risque tiers. Leurs réponses sont évidemment multiples, mais nous pouvons les classer en trois grandes catégories.

Le manque de temps, d'outillage et de process, pour assumer une charge de travail lourde et coûteuse, et qui implique parfois une revue, a posteriori, des contrats et la mise en place de KPI fiables. Ce manque de moyens empêche les entreprises de dégager une vision exhaustive des risques. En outre, dans les grandes entreprises, le nombre de fournisseurs est élevé, ce qui pose de réels problèmes en matière d'accès et de traitement des informations, ce dernier étant encore parfois manuel.

La difficulté pour un certain nombre de fournisseurs (en particulier des PME) **d'appréhender les enjeux de la cybersécurité** ou de se mettre en capacité d'y répondre avec un certain niveau de maturité. Les investissements nécessaires à une prévention du risque cyber peuvent se révéler onéreux pour des entreprises petites ou moyennes. La disparité des niveaux de préparation des fournisseurs représente donc, pour les donneurs d'ordre, une difficulté supplémentaire à traiter.

Un manque de réactivité, de compréhension et d'intérêt de la part de certains fournisseurs. Cela implique de la part des donneurs d'ordre un effort de pédagogie et de conviction vis-à-vis de leurs fournisseurs, en soulignant notamment qu'au sein de la supply chain, la faiblesse d'un maillon, c'est la faiblesse de la chaîne tout entière.

À SAVOIR

Seules 13 % des entreprises interrogées sont accompagnées par un cabinet de conseil en cybersécurité pour la gestion de ce risque

Ce qu'en pensent les RSSI et CISO

Extraits des propos de dirigeants interrogés par Board of Cyber

LIVRE BLANC
Risque cyber fournisseurs

Pour parvenir à une gestion optimale du risque cyber fournisseur, il faudrait mettre en place une automatisation complète du processus d'évaluation du risque, avec un workflow d'informations et la mise en lumière de l'ensemble des différentes actions à réaliser par le fournisseur.

CISO Groupe d'une **grande entreprise industrielle**

Il serait utile de mettre en place un outil capable de collecter, de centraliser et de vérifier l'état de conformité de l'ensemble des fournisseurs. Un tel outil permettrait, en quelques clics, d'avoir une image globale de notre risque fournisseur avec un maximum de flexibilité sur les outils de requête.

Directeur cybersécurité d'un **groupe financier**

L'idéal serait de disposer d'une certification et d'un audit systématique de tout l'écosystème fournisseurs pour disposer d'un certificat émanant d'un tiers de confiance.

CISO Groupe d'une **grande entreprise industrielle**

Il faudrait impliquer davantage les régulateurs dans l'obligation de certification pour les fournisseurs représentant un risque systémique.

CISO d'un **grand établissement financier**

En réalité, nous manquons de temps pour traiter l'ensemble des informations, apprécier correctement toutes les interactions entre notre entreprise et l'ensemble de ses fournisseurs.

CISO Groupe d'une **entreprise du BTP**

Une forte demande de rationalisation et d'automatisation

LIVRE BLANC
Risque cyber fournisseurs

Que faudrait-il changer pour que les entreprises améliorent leur efficacité dans le traitement du risque fournisseurs ? Les réponses à cette question valent d'être presque toutes citées, tant elles expriment les insatisfactions et les attentes des entreprises en demande de davantage de rationalisation.

Une certification et un audit systématique de tout l'écosystème pour disposer d'un certificat provenant d'un tiers de confiance ;

Une automatisation complète du processus d'évaluation du risque fournisseur, avec un flux de collecte du questionnaire ou des documents indiquant les actions à réaliser par fournisseur, et avec un tri des priorités ;

Une combinaison d'outils entre le « Cybersecurity framework » NIST, les agences de notation, les outils de test de pénétration et des KPI techniques ;

Une rationalisation des questionnaires d'analyse des risques ;

Des évaluations journalières automatiques ;

Le recours à une notation cyber indépendante basée sur les critères de l'entreprise en matière de relation avec ses fournisseurs ;

La réalisation d'une cartographie exhaustive et claire des liens et interactions de l'entreprise avec ses fournisseurs ;

La délégation du pilotage du risque auprès d'entreprises tiers, certifiées ANSSI ;

Une direction des achats centralisée et une gouvernance opérationnelle des acteurs locaux ;

Un questionnaire d'analyse des risques à l'état de l'art et une revue de preuves acceptée par l'ensemble des fournisseurs ;

La mise en place d'un schéma de certification nationale.

CONCLUSION

Des attentes à satisfaire

LIVRE BLANC
Risque cyber fournisseurs

Il suffit de considérer la montée en puissance des risques géopolitiques et leurs conséquences économiques pour prendre conscience que le risque cyber est à traiter en priorité par les entreprises. La difficulté est que la menace est protéiforme, difficile à prévenir et à traiter. Son panorama se complexifie en permanence, qu'il s'agisse des cibles, des motivations ou des technologies d'attaque. Pour faire face à ce risque, il faut donc adopter une approche globale, presque holistique.

Paradoxalement, l'accélération de la transformation numérique des entreprises les expose encore davantage au risque cyber. D'autant que les cyberattaques se multiplient contre la supply chain, ce qui provoque une inflation du risque lié aux tiers.
Les groupes gèrent des chaînes d'approvisionnement de plusieurs milliers de fournisseurs et de sous-traitants et doivent donc traiter un nombre croissant de données chaque jour.
L'étude de Board of Cyber illustre cette réalité d'un jour nouveau.

À SAVOIR

TYPOLOGIE DES ENTREPRISES INTERROGÉES

- Assurances
- Beauté & Cosmétique
- BTP
- Chimie
- Distribution
- Électronique
- Énergie
- Finance
- Industrie
- Luxe
- Services à l'industrie
- Services publics
- Transports

board of cyber

Beyond Rating .

boardofcyber.io
contact@boardofcyber.io

7, avenue de la Cristallerie, 92310 Sèvres

Contact presse : pierre-edouard.builly@lesroismages.fr