board of cyber
Beyond Rating.

CESIN

OBSERVATOIRE 2024

Le risque cyber lié aux fournisseurs

Les attentes des entreprises face aux nouvelles réglementations et à la montée du risque

NOVEMBRE 2024

Sommaire

Introduction 3

Assurer une sécurité collective 4
par Frank Van Caenegem et Alain Bouillé (CESIN)

Faire face, ensemble 5
par Luc Declerck (Board of Cyber)

1. L'emprise de la régulation 6
2. Des modes de gestion des risques hétérogènes 8
3. De multiples dispositifs d'évaluation 10
4. Les obstacles majeurs 12
5. Si la méthode idéale existait… 14
6. Vers davantage de mutualisation ? 16

Remerciements 18

OBSERVATOIRE 2024
Le risque cyber lié aux fournisseurs

Introduction

En association avec le CESIN, Board of Cyber a réalisé une enquête sur la façon dont les entreprises gèrent le risque cyber lié aux fournisseurs. Cette étude porte sur plus de 100 entreprises de toutes tailles et de tous secteurs, et qui doivent gérer plusieurs centaines, voire des milliers de fournisseurs. Ses résultats montrent à la fois une réelle préoccupation des entreprises et une grande hétérogénéité dans la façon dont ce risque est pris en charge et géré.

La mise en œuvre des récentes réglementations (DORA, NIS2…) souligne, s'il en était besoin, l'urgence d'une prise en compte globale de ce risque et le besoin d'outils de mutualisation et d'automatisation pour l'évaluer dans sa globalité.

Le CESIN et Board of Cyber remercient les décideurs qui ont accepté de répondre à cette étude d'avoir contribué à une meilleure compréhension du risque fournisseurs et de ses enjeux.

ÉDITORIAL

Assurer une sécurité collective

Cet Observatoire des risques tiers est riche d'enseignements pour l'ensemble des parties prenantes de l'écosystème de la cybersécurité. Il révèle que les entreprises vont devoir franchir une étape décisive dans l'appréhension des risques fournisseurs afin d'acquérir une vraie maturité sur le sujet, dans la perspective de la mise en place progressive de la directive NIS2 et du réglement DORA. Il ne faut pas aborder la question des risques tiers comme un simple problème de mise en conformité, mais appréhender ce risque de façon globale. Il est également nécessaire d'avoir une démarche graduée, basée sur le risque, et ne pas se fonder uniquement sur des considérations financières pour déterminer la criticité d'un tiers. Pendant longtemps, cette approche a prévalu au sein des grandes organisations pour évaluer les partenaires. Cela n'est plus possible aujourd'hui. La philosophie à privilégier est l'instauration d'une sécurité collective entre les entreprises, leurs fournisseurs et leurs partenaires, reposant sur la confiance. Le CISO ne doit pas être perçu comme générateur de difficultés, mais comme un facilitateur de business dans un contexte où il va nous falloir, tous ensemble, apprendre ce nouveau métier de gestion du risque tiers.

Frank VAN CAENEGEM
CISO EMEA de Schneider Electric, administrateur du CESIN

Alain BOUILLÉ
Délégué général du CESIN

ÉDITORIAL

Faire face, ensemble

Les résultats de cet Observatoire, réalisé avec le CESIN, révèlent à quel point les entreprises françaises font face à un tsunami en matière de risque cyber lié aux tiers. Près de 90 % d'entre elles reconnaissent que ce risque est « très important » ou « important ». Mais les deux-tiers déclarent mener un processus d'évaluation du risque sur moins de 50 fournisseurs par an. Le risque lié aux tiers et l'application de NIS2 – ou DORA dans les prochains mois – commandent d'approcher ce risque de manière totalement nouvelle, alors que l'implication des fournisseurs dans cette démarche reste un défi bien identifié. Le moment est donc venu de changer de paradigme, en passant d'une attitude statique (administrer des questionnaires ou réaliser des audits annuels, par exemple…) à une attitude pro-active et efficiente qui engagerait les fournisseurs dans des processus vertueux, grâce à une massification et une automatisation de l'évaluation des systèmes d'évaluation. La création d'un écosystème de confiance auprès de nos organisations publiques comme privées est un défi majeur ; ce passage à l'échelle implique une collaboration de l'ensemble de l'écosystème.

Luc DECLERCK
Directeur général de Board of Cyber

1

L'emprise de la régulation

Les nouvelles réglementations vont aider les entreprises à faire accepter un certain niveau d'exigence à leurs fournisseurs et partenaires.

OBSERVATOIRE 2024
Le risque cyber lié aux fournisseurs

Depuis quelques années, les instances européennes ont créé de nouvelles règles en matière de cybersécurité, comme DORA, NIS2 ou le CRA.
L'Observatoire relève que près de 7 entreprises sur 10 sont concernées par NIS2, 32,6 % par DORA, 20,7 % par les règles PCI sur la sécurité des données de paiement, un nombre équivalent par les règles de cybersécurité de la Loi de programmation militaire. Et pour **53,4 %** des organisations, ces nouvelles réglementations vont les conduire à modifier dans les douze prochains mois leur approche de la gestion du risque fournisseurs.
Les entreprises interrogées affirment, notamment, que le nouveau cadre réglementaire induit un élargissement du périmètre de l'analyse des risques non seulement aux autres entités de leur groupe, mais aussi à la totalité de leurs fournisseurs.
Dans l'approche d'une « revue complète du dispositif », ce passage à l'échelle les conduit à industrialiser processus et outils, afin de « lancer des audits plus complets et plus fréquents ».
Certains RSSI estiment que les nouvelles réglementations vont les aider à faire accepter un certain niveau d'exigence aux fournisseurs et partenaires lors de la signature de contrats.

À SAVOIR

NIS2 et DORA, un changement de paradigme

La directive NIS2 a été publiée le 27 décembre 2022 et sa transposition dans le droit national français doit intervenir prochainement. Elle introduit de nouvelles obligations pour les entreprises en matière de cyber protection, d'audits réguliers et de signalement des incidents. Elle s'applique aux entreprises, mais aussi à leurs fournisseurs et concerne environ 15 000 entreprises en France et 200 000 dans l'UE.

Le règlement DORA (Digital Operational Resilience Act) qui s'appliquera aux 27 États membres à partir du 17 janvier 2025, vise particulièrement les acteurs de la finance. Il leur impose, notamment, de mettre en place des systèmes de gestion des risques cyber, de notifier les menaces et les attaques, d'opérer des tests de résilience, et surtout de garantir la gestion du risque cyber lié aux fournisseurs et prestataires de services TIC.

2

Des modes de gestion des risques hétérogènes

L'enquête montre d'assez grandes différences dans les approches et les méthodes sur la façon dont est pris en compte le risque fournisseurs.

OBSERVATOIRE 2024
Le risque cyber lié aux fournisseurs

L'Observatoire a interrogé les responsables de la cybersécurité sur la façon dont est pris en compte le risque fournisseurs et les résultats montrent d'assez grandes différences dans les approches et les méthodes.

En résumé :

➜ La prise de conscience des enjeux du risque fournisseurs fait l'objet d'un large consensus dans les entreprises interrogées : 88 % le considèrent comme « très important » ou « important ». Seules 11 % d'entre elles le considèrent comme « peu important » et une seule entreprise sur les 101 interrogées le qualifie de « pas du tout important ». Pour autant, dans 45 % des cas, ce risque n'est pas suivi par le Comex.

➜ Dans les entreprises considérant ce risque comme « très important », 76 % le font suivre par le Comex.

➜ Dans 55 % des entreprises, le pilotage du risque fournisseurs est centralisé (au niveau du siège par exemple), alors que 35 % d'entre elles ont mis en place un pilotage hybride et que 10 % privilégient une gestion décentralisée (au niveau de la business unit par exemple).

➜ Plusieurs fonctions dans l'entreprise sont impliquées dans la gestion du risque fournisseurs : la RSSI groupe (82 %), mais aussi la direction des achats (65,3 %), la RSSI de la business unit (36,6 %), le responsable conformité (33,6 %) et le risk manager (25,7 %). Dans 11 % des cas, la direction juridique est également impliquée.

➜ Seules 33,6 % des entreprises impliquent l'ensemble de leurs fournisseurs dans le processus d'évaluation.
Moins de 20 fournisseurs sont évalués au moins une fois par an dans 42,5 % des cas, entre 21 et 50 dans 23,7 % des entreprises, entre 51 et 100 dans 20,7 %. Dans près d'une entreprise sur dix, cette évaluation s'applique à plus de 251 fournisseurs.

➜ Dans 47,5 % des entreprises, ce processus d'évaluation adopte une fréquence annuelle, mais 12,8 % le mettent en place tous les deux ans et 30,6 % tous les trois ans. Seule une minorité d'entreprises a adopté une fréquence plus rapide.

À SAVOIR

88 %
des entreprises jugent le risque fournisseurs « très important » ou « important »

55 %
des entreprises centralisent le pilotage du risque fournisseurs

3

De multiples dispositifs d'évaluation

La plupart de ces dispositifs représente une charge de travail de plus en plus lourde pour les fournisseurs.

OBSERVATOIRE 2024
Le risque cyber lié aux fournisseurs

D'une manière générale, les entreprises ont mis en place des systèmes de classification de leurs fournisseurs (60 % des cas).

Quatre critères se démarquent:
➜ La criticité du service ou du produit délivré à l'entreprise (57,4 %)
➜ Leur niveau d'intégration dans le système d'information de l'entreprise (51,4 %)
➜ Leur accès à des données personnelles (48,5 %)
➜ Leur accès à des données stratégiques (44,5 %)

D'autres critères sont notés comme la nature de la relation commerciale (10,8 %) ou du produit faisant l'objet de la relation.

Quant aux dispositifs d'évaluation adoptés par les entreprises, ils sont majoritairement marqués par une approche « top-down » de type PAS ou questionnaire auto-déclaratif.
➜ Plan d'assurance sécurité (66,3 %)
➜ Questionnaire auto-déclaratif (66,3 %)
➜ Certification ISO SOCII (57,4 %)
➜ Questionnaire avec dépôt de preuves (41,5 %)
➜ Test d'intrusion (32,6 %)
➜ Audit GRC (29,7 %)
➜ Notation cyber (29,7 %)
➜ CTI (fuites de données, incidents récents de type rançongiciels...) (24,7 %)

La plupart de ces dispositifs accroissent considérablement le travail pour les fournisseurs.

La notation cyber et la CTI, seules solutions en continu, sont utilisées par près d'une entreprise sur trois, pratiquement au même niveau que les tests d'intrusion.

« Après contractualisation avec le fournisseur, s'il ne se produit pas d'incident, tout va bien jusqu'au renouvellement du contrat. En revanche, s'il y a un incident, nous demandons la réalisation d'un audit par un tiers. »
RSSI d'un **groupe de logistique**

« Nous impliquons nos fournisseurs grâce à l'appui de nos spécialistes métiers et de nos experts juridiques. Nous bénéficions aussi de la puissance de notre marque, qui induit des standards groupe très stricts auxquels nous ne pouvons pas déroger. »
CISO d'un **groupe d'assurance**

4

Les obstacles majeurs

Le manque de ressources et la complexité d'engager les fournisseurs représentent les difficultés les plus fréquentes auxquelles se heurtent les responsables de la cybersécurité.

OBSERVATOIRE 2024
Le risque cyber lié aux fournisseurs

L'Observatoire de Board of Cyber et du CESIN s'est également intéressé aux difficultés que rencontrent les responsables de la cybersécurité des entreprises dans la gestion du risque partenaires et/ou fournisseurs. Ils sont de nature différente et tiennent aussi bien aux ressources humaines et technologiques de l'entreprise, à la mobilisation de ses fournisseurs ou à la complexité des procédures d'évaluation.

Parmi les motifs les plus souvent évoqués figurent :
➜ Le manque de ressources (73,2 %)
➜ La complexité d'engager les fournisseurs (64,3 %)
➜ La difficulté d'embarquer les métiers (51,4 %)
➜ L'incapacité de certains fournisseurs à atteindre le niveau de sécurité demandé (48,5 %)
➜ Le passage à l'échelle (42,5 %)
➜ Des process non clairs de gestion de ce risque (24,7 %)
➜ La complexité des processus (20,8 %)
➜ Des outils non efficients (16,8 %)

À SAVOIR

73,2 %
des entreprises citent le « manque de ressources » comme premier obstacle

48,5 %
des entreprises citent « l'incapacité de certains fournisseurs à atteindre le niveau de sécurité demandé »

« La dimension juridique reste très (trop ?) présente dans les discussions avec nos partenaires. Il faut noter aussi que les échanges sont plus complexes avec certains partenaires lorsqu'ils sont dans une situation quasi-monopolistique. »
CISO d'un **groupe bancaire**

« La difficulté, c'est l'absence d'un véritable référentiel de tous les tiers. L'outil groupe ne concerne que les sous-traitants au sens de Solvability 2, mais ce n'est pas l'ensemble des tiers. L'autre difficulté réside dans la supervision régulière et la capacité à réaliser des audits. »
Responsable cyber contrôle d'un **groupe d'assurance**

5

Si la méthode idéale existait...

On retrouve un certain consensus en faveur de la création d'une méthodologie d'évaluation standardisée et reconnue par les autorités de régulation.

OBSERVATOIRE 2024
Le risque cyber lié aux fournisseurs

Et si par un coup de baguette magique, les responsables cyber pouvaient créer le contexte le plus favorable pour gérer le risque fournisseurs et partenaires, que suggéreraient-ils ?

Leurs réponses sont assez diverses, mais il existe un certain consensus en faveur de la création d'une méthodologie d'évaluation standardisée et reconnue par les autorités de régulation. S'exprime également le désir de bénéficier de budgets et de ressources humaines, pour réaliser une fois par an un audit très poussé ou pour imposer des audits plus fréquents et obligatoires.

Certains suggèrent la mise en place d'une plateforme unique et commune en Europe, voire de réduire le nombre de fournisseurs, quitte à créer une dépendance.

« Il faudrait mettre en place un "cyber score fournisseur" régulièrement mis à jour et/ou une certification obligatoire type ISO 27001 garantissant la mise en place des bonnes pratiques et leur suivi dans le temps. Cela pourrait apporter plus de confiance dans les relations clients/fournisseurs. »

RSSI département Gouvernance et Réglementation
d'un groupe de services

« Je chercherais à convaincre tous les fournisseurs (même les petites structures) qu'une bonne gestion des risques cybersécurité est pour eux un avantage concurrentiel et commercial, et qu'ils devraient mieux se préparer et démontrer qu'ils ont un bon niveau de maturité ou qu'ils sont prêts à atteindre ce niveau en collaboration avec leurs clients. »

Security Risk Manager
d'un groupe d'assurance

6

Vers davantage de mutualisation ?

Une majorité d'entreprises accepteraient de se rallier à des évaluations autres que les leurs. Encore faut-il s'accorder sur la méthode.

OBSERVATOIRE 2024
Le risque cyber lié aux fournisseurs

Pour surmonter les obstacles listés par les responsables interrogés dans le cadre de cet Observatoire 2024, la mutualisation pourrait-elle être une arme décisive ?

En apparence, oui. En effet, **71 %** des entreprises accepteraient de réduire leurs demandes aux partenaires et fournisseurs si leurs services avaient déjà été évalués positivement par plusieurs entreprises.

Mais encore faut-il s'accorder sur la méthode. Parmi les entreprises qui se rallieraient à des évaluations autres que les leurs, 62% souhaitent qu'il s'agisse d'un tiers de confiance (agence de notation, certification, label) ou d'avoir communication du détail de l'évaluation et souvent les deux…

Dans tous les cas, les responsables cyber interrogés insistent sur le fait qu'une évaluation réalisée par un tiers devrait « fournir des preuves », « s'appuyer sur des KPIs standards » et « une définition précise du périmètre ».

« Cela pourrait se faire seulement si l'évaluation a été effectuée sur un périmètre pertinent et dans un contexte lié spécifiquement au service fourni à mon entreprise par ce partenaire. Car un fournisseur donné peut fournir différents services à mon entreprise et une évaluation se fait par rapport au contexte du service fourni. »

3rd Party Security Risk Manager d'un **groupe d'assurance**

« Il est de ma responsabilité d'analyser le niveau de risque introduit par une collaboration avec un fournisseur et/ou un partenaire. En revanche, une base commune où trouver des éléments récurrents, type PAS, certifications, rapport de PenTest, processus de gestion de crise ou autre aiderait sûrement à moins solliciter les fournisseurs et partenaires. »

CIO d'un **groupe de distribution**

merci

Cette étude a été rendue possible grâce à la participation de :

- Agrial
- Autorité des Marchés Financiers
- Butagaz
- CCI de Corse
- Christian Dior Couture
- CHU de Lille
- Capgemini
- Conseil départemental des Hauts-de-Seine
- E-attestation.com
- Fibus Group
- Generix Group
- Groupe Arcade
- Groupe Rocher
- Groupe VYV
- GRTgaz
- HelloAsso
- Hub One
- Institut Curie
- La Poste Groupe
- Lagardère
- MGDIS
- MGEN
- Moët-Hennessy
- Motul
- Mutex
- Nantes Métropole
- Orange
- OVHcloud
- Petit Forestier Group
- Sogécap (Société Générale Assurances)
- Sysmex France
- Schneider Electric
- Saint-Gobain Distribution Bâtiment France
- Transat

OBSERVATOIRE 2024
Le risque cyber lié aux fournisseurs

aux plus de 100 décideurs qui ont répondu à cette enquête

Remerciements particuliers à :

- Antoine Ancel
- Ralph Arnaud
- Jean-François Audenard
- Thierry Auger
- Elise Babelaere
- Fabrice Bardey
- Herve Baudry
- Pierre Belin
- Dominique Berti
- Vincent Bohy
- Matthieu Blin
- Cédric Chausson
- Patrick Chauvin
- Charles Chollet
- David-Alexandre Correia
- Katia Derache
- Florence Devambez
- Guillaume Devoyon
- Djalil Djouadi
- Noémie Douénat
- Jérôme Etienne
- Joakim Gautier
- Jean-Géraud Greze
- David Giorgis
- Olivier Gleyze
- Christophe Hugot
- Stéphane Jourdain
- Timothée Laumann
- Alexandre Le Bihan
- Frédéric Leblond
- Paul Lemesle
- Julien Levrard
- Jean-François Louapre
- Ramzi Lounissi
- Guillaume Ly Van Manh
- Christophe Maira
- Magali Matelot
- Sébastien Mauptit
- Joris Michallon
- Thibault Millant
- Sébastien Olaïzola
- Olivier Pallany
- Vivian Pelissou
- Frédéric Pillefert
- Cédrick Pipitone
- Pierre-Luc Réfalo
- Benoît Grangé
- Patrice Renaudineau
- Stéphane Riffard
- Emmanuel Roux
- Richard Sangaré
- Jérémy Schwalb
- Olivier Stassi
- Bonny Sounthone
- Tommy Vayron
- Frank Van Caenegem
- Nicolas Van Tieghem
- Stéphane Vasselon
- Estelle Tchigique-Boyer
- Grégoire Turcat

board of cyber

Beyond Rating.

CESIN

boardofcyber.io

contact@boardofcyber.io

7, avenue de la Cristallerie, 92310 Sèvres

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

cesin.fr

contact@cesin.fr

115, rue Saint-Dominique, 75007 Paris

Contact Presse :
vloquet@alx-communication.com