Dix points clés pour une surveillance éclairée des risques cyber

Article · August 2023

CITATIONS
0

READS
573

8 authors, including:

Freddy Dezeure
Freddy Dezeure BV
26 PUBLICATIONS **3** CITATIONS
SEE PROFILE

João Pedro Gonçalves
EQT Group
14 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Eireann Leverett
Concinnity Risks
26 PUBLICATIONS **92** CITATIONS
SEE PROFILE

Lokke Moerel
Tilburg University
38 PUBLICATIONS **89** CITATIONS
SEE PROFILE

Signaler les risques cyber aux conseils d'administration

Dix points clés pour une surveillance éclairée des risques cyber

Auteurs
Freddy Dezeure
Peter Debasse
João Pedro Gonçalves
Tristan Guiheux
Éireann Leverett
Patrick Mana
Lokke Moerel
Bartosz Sygula

Réviseurs
Greg Bell
Paolo Borghesi
Philippe Coffyn
Chris Deverell
Tom Gilis
Kevin Holvoet
Angelos Keromytis
Ed Millington
Dimitri Rombaut
Sam Singer

Date : 30 août 2023
Version : Finale

Table des matières

Introduction

En mars 2022, nous avons publié le livre blanc Signaler les risques cyber aux conseils d'administration, qui fournit des conseils aux responsables de la sécurité des systèmes d'information (RSSI) pour concevoir et mettre en œuvre des mesures quantitatives de cybersécurité afin de rendre compte des risques cyber au niveau du conseil d'administration et de fournir une assurance raisonnable que ce dernier est maintenu dans les limites de l'appétence au risque de l'entreprise. Le livre blanc a reçu beaucoup d'attention et de crédit dans la communauté ou il a été largement diffusé. Il a également été publié dans une version condensée à l'intention des membres des conseils d'administration.

Depuis la publication du livre blanc, des exigences réglementaires supplémentaires dans l'UE (NIS2[1] , DORA[2]) et aux États-Unis (SEC[3] , NYDFS[4]) ont accru la responsabilité et l'obligation des membres des conseils d'administration d'exercer une surveillance prudente et éclairée des risques cyber dans leurs organisations. Le risque cyber joue également un rôle de plus en plus important dans les rapports ESG. Certaines exigences réglementaires font explicitement référence à des métriques du risque cyber (DORA, article 6). Il n'existe toutefois pas encore d'orientation officielle sur ce qui constituerait une surveillance appropriée de la part des conseils d'administration, et encore moins sur les paramètres stratégiques qui pourraient conduire à une surveillance *éclairée*.

Les commentaires de la communauté sur le livre blanc et des idées supplémentaires nous ont conduits à formuler des orientations additionnelles pour mettre en évidence les enseignements tirés et appuyer leur formulation. Le présent document vise à répondre à ce dernier objectif. Il fournit également des éléments pour répondre aux exigences réglementaires nouvelles en matière d'information et de contrôle pour le conseil d'administration.

Ce document repose sur la notion selon laquelle une bonne gestion des risques cyber doit être *fondée sur des preuves* plutôt que sur des intentions ou des hypothèses (souvent basées sur du déclaratif). Les métriques cyber stratégiques constituent une composante essentielle de l'effort bénéfique de hiérarchisation dans la mise en œuvre de la gestion des risques cyber.

Mesurer les risques cyber d'une manière *quantifiable*, en utilisant les données de l'infrastructure, n'est pas une pratique largement adoptée. Il n'est donc pas surprenant qu'il n'existe pas non plus de critères de comparaison entre pairs.

Le présent document vise à partager 10 points clés provenant d'organisations qui ont déployé des métriques cyber stratégiques afin que la communauté puisse s'appuyer sur ces enseignements et les adopter dans son propre environnement. Les idées sont formulées dans des résumés clairs, et suscitant la réflexion pour en faciliter la compréhension.

---

[1] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32022L2555 (articles 20 et 21)
[2] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32022R2554 (articles 5 et 6)
[3] https://www.sec.gov/news/press-release/2023-139
[4] https://www.dfs.ny.gov/system/files/documents/2022/10/rp23a2_text_20221109_0.pdf

Cette approche peut apparaître comme une généralisation ou une simplification, mais elle permet de rationaliser et de concentrer l'attention des RSSI et des conseils d'administration pour, en fin de compte, obtenir de meilleurs résultats en matière de gestion et de surveillance des risques cyber.

Le présent document doit être considéré comme un complément au livre blanc de 2022 et il est vivement recommandé de les lire conjointement.

Dix points clés

1. Des preuves plutôt que de la conformité

De nombreuses organisations ont adopté un cadre de cybersécurité (NIST, ISO, CIS) ou ont suivi une réglementation et des normes spécifiques (PCI-DSS, Solvency/Basel II), associées à des audits externes ou à une certification. Il s'agit souvent d'une exigence dans leur activité, pour des raisons réglementaires ou commerciales (assurances, clients). Toutefois, cette approche doit être considérée comme une base de référence plutôt que comme une fin en soi. Elle fournit des normes et des politiques à respecter, mais ne reflète pas nécessairement l'adéquation réelle aux risques spécifiques de l'entreprise.

Les contrôles convenus, s'ils fonctionnent correctement, sont-ils suffisants pour conduire à une atténuation efficace des risques ? Sont-ils déployés dans leur intégralité ? Fonctionnent-ils comme prévu ?

Les organisations les plus matures utilisent des preuves (continues) provenant de données collectées dans leur infrastructure pour vérifier l'efficacité de leurs contrôles plutôt que de s'en remettre à une évaluation humaine, des systèmes déclaratifs et aux questionnaires remplis annuellement. La collecte et la conservation des données requises constituent, il est vrai, un défi important, mais ces organisations considèrent que le jeu en vaut la chandelle. Le jugement professionnel peut rester un élément de mise en contexte dans les rapports au conseil d'administration, mais s'il est étayé par des mesures dérivées de sources de données opérationnelles et d'outils de sécurité.

2. S’intéresser aux KCI en priorité sur le reste

Les conseils d'administration veulent être informés sur ce qui est important et tous les contrôles n'ont pas la même importance. La plupart des cadres de référence cyber indiquent qu'un nombre limité de contrôles engendre le plus grand impact sur l'atténuation des risques.

Il est donc logique de rendre compte au conseil d'administration des indicateurs clés de contrôle (KCI) et de leur évolution dans le temps plutôt que d'essayer de rendre compte de tous les contrôles. Cela ne signifie pas que le RSSI perde de vue tous les autres contrôles, mais plutôt qu'il mette en évidence ce qui a le plus d'impact sur l'atténuation des risques pour une organisation donnée à un moment donné.

Éviter de confondre le concept d'indicateurs clés de performance (KPI) avec les KCI. Un RSSI doit s'intéresser aux performances de son équipe, mais les KPI ne seront pas toujours pertinents pour déterminer dans quelle mesure le risque cyber est atténué. Les rapports au conseil d'administration nécessitent des indicateurs de nature stratégique, représentatifs de l'environnement de contrôle interne global et qui étayent l'appétence au risque. Le livre blanc de 2022 Signaler les risques cyber aux conseils d'administration contient des conseils détaillés sur les KCIs, leur efficacité et leur couverture.

Voici une liste d'exemples de KCIs utiles pour débuter :

KCI 1	Inventaire des actifs [5]	% d'actifs en stock dans le cadre de la politique
KCI 2	Comptes privilégiés	% de comptes privilégiés gérés dans le cadre d'une politique
KCI 3	Patching en temps voulu	% de correctifs à haut risque dans les N heures # sur les vulnérabilités exploitées détectées et connues
KCI 4	Sauvegarde	Délai maximal de récupération des actifs clés (% d'actifs critiques récupérables en N heures)
KCI 5	Protection des terminaux	% de terminaux conformément à la politique
KCI 6	Collecte des journaux	% de systèmes critiques intégrés à la collecte de données
KCI 7	Sécurité des réseaux	% de conformité des configurations de sécurité du réseau des équipements clés
KCI 8	Conformité des tiers	% de connexions conformes avec des tiers clés
KCI 9	Gestion de l'identité	% de couverture des systèmes avec l'AMF (Authentification Multi Facteurs)
KCI 10	Incidents majeurs	% d'incidents cyber majeurs ayant un impact métier sur les entreprises
KCI 11	Acceptation des risques	# écarts, sur les risques acceptés, par rapport à la politique
KCI 12	Couverture de sécurité des biens exposés à l'internet	Pourcentage des biens exposés à l'internet couverts par un contrôle de sécurité et une évaluation régulière de sécurité
KCI 13	Couverture des joyaux de la couronne	% de joyaux de la couronne couverts par une surveillance de la sécurité, une analyse de vulnérabilités et une évaluation régulière de sécurité
KCI 14	Origine des incidents de sécurité	Pourcentage d'incidents de sécurité liés à des défaillances d'au moins un indicateur de contrôle clé (KCI)

3. Informé des menaces actuelles et non passées

Le paysage des menaces évolue et nos contrôles et KCIs doivent en faire autant. Les adversaires adaptent leurs tactiques et techniques pour contourner nos défenses. Ils sont souvent mieux informés que nous des lacunes de notre infrastructure et de nos contrôles. Ils surveillent la divulgation des vulnérabilités par les fournisseurs et y réagissent dans des délais plus courts que nous. Certains disposent de ressources suffisantes pour acheter des exploits sophistiqués.

[5] Il est essentiel de disposer d'un inventaire précis et complet des actifs, car c'est le dénominateur d'un grand nombre d'indicateurs clés de performance.

Pour éviter tout impact négatif sur nos activités, nous devons adapter nos contrôles à la menace, en tenant compte de notre environnement et de nos actifs spécifiques. Il faut pour cela comprendre les tactiques, techniques et procédures de l'adversaire, hiérarchiser et réorienter les contrôles, et surveiller en permanence les indicateurs de comportement et de compromission. Les développements importants méritent d'être suivis et signalés au conseil d'administration. Et, bien sûr, ils nécessitent de se voir accorder la priorité qui s'impose au niveau technique.

4. Des priorités plus que des moyennes

Se concentrer sur ce qui est vraiment important signifie également qu'il faut être prudent avec les moyennes. En établissant des moyennes, les écarts par rapport aux contrôles critiques risquent de passer inaperçus. De même, les valeurs aberrantes peuvent ne pas être signalées. C'est pourquoi nous vous recommandons de ne pas faire une synthèse des résultats des centaines de contrôles que vous avez identifiés. Il peut être intéressant, d'un point de vue technique, d'identifier un pourcentage de couverture de l'ensemble du cadre, mais ce calcul de moyenne tend à masquer les principaux problèmes.

De même, l'établissement d'une moyenne au sein d'un contrôle spécifique peut masquer des risques importants. Si, par exemple, une organisation vise à corriger les vulnérabilités critiques dans un délai de trois jours, les vulnérabilités à risque moyen dans un délai d'un mois et toutes les autres dans un délai de trois mois, l'établissement d'une moyenne des performances en matière de correction pourrait masquer les vulnérabilités les plus critiques.

Ne déclarez les moyennes que lorsque cela se justifie pour un KCI spécifique. Le livre blanc de 2022 Signaler les risques cyber aux conseils d'administration contient des conseils plus détaillés sur les KCI et leur couverture.

5. Signaler les lacunes plutôt que de clamer "tout est vert"

Il est tout à fait normal de faire part de la situation réelle au conseil d'administration, y compris des manques à combler. Les membres du conseil d'administration ont besoin de l'entendre, si c'est la réalité. Cela aidera également l'organisation à se conformer à la surveillance réglementaire et à soutenir la priorisation des investissements.

Lorsque des déficiences sont signalées au conseil d'administration, il est nécessaire d'expliquer le risque qu'elles comportent et les mesures proposées pour y remédier dans un délai déterminé.

6. Intégrer et non exclure

L'impact du signalement des risques cyber au conseil d'administration sera renforcé si l'on donne accès à l'état des contrôles à ceux qui les gèrent (opérateurs, gestionnaires). C'est ce que nous appelons la "démocratisation des métriques".

La communication des risques cyber au conseil d'administration est un élément moteur de l'organisation. Ce qui est signalé comme important sera inévitablement (heureusement) perçu comme important par le conseil

d'administration et au sein de l'organisation. Les KCIs doivent donc avoir un sens du point de vue de la gestion des risques et révéler l'état réel du risque.

Les données sous-jacentes aux KCI devraient être collectées à partir des systèmes mettant en œuvre les contrôles. La mise en place de tableaux de bord connectés à tous les niveaux de l'organisation, avec la granularité requise pour fournir des informations aux gestionnaires des contrôles, crée de la transparence, renforce l'appropriation et permet d'affiner le système.

7. Transparence vis-à-vis des écarts (acceptés ou non)

Il serait utile de donner de la visibilité sur les écarts par rapport aux contrôles clés en les signalant au conseil d'administration. Ces écarts peuvent résulter de l'acceptation des risques ou de violations des politiques (délibérées ou involontaires).

La plupart des organisations ont mis en place un processus qui permet aux départements de s'écarter des politiques de sécurité en "acceptant le risque". Plutôt que de garder ces écarts sous le radar, il serait judicieux de les signaler. Donner de la visibilité aux écarts pourrait aider l'organisation à s'aligner sur les contrôles clés qui sont conçus pour atténuer le risque et rester dans les limites de l'appétence au risque.

Le suivi des écarts est particulièrement utile pour comprendre la maturité de l'organisation concernant les processus et la culture de gestion des risques. Les organisations les plus matures ont tendance à considérer l'acceptation des risques comme la dernière des options disponibles, et non comme la première.

Le processus même de documentation de ces écarts nous permet également d'identifier les seuils irréalistes, par exemple la correction de toutes les vulnérabilités avec un budget de 1 % de du chiffre d'affaires. En discutant des écarts, l'ensemble de l'organisation peut s'orienter vers des seuils d'acceptation des risques plus pratiques et plus réalistes.

8. L'appétence au risque plutôt que le risque zéro

On ne le répétera jamais assez, une organisation doit déterminer au niveau du conseil d'administration quel est le niveau acceptable de risque cyber. Le risque zéro est un objectif impossible à atteindre et probablement même indésirable. Il s'agit essentiellement d'éviter les risques plutôt que de les traiter efficacement. Dans de nombreuses organisations, cet appétit pour le risque a déjà été établi dans le cadre des processus généraux de gestion des risques.

Si ce n'est pas encore le cas pour le risque cyber, le RSSI doit inciter le conseil d'administration à définir cette appétence au risque :

- Combien sommes-nous prêts à perdre si le risque cyber se concrétise ? Pensez aux jours d'arrêt, au vol de propriété intellectuelle, à la perte d'informations confidentielles, à l'atteinte à la réputation...
- Dans quelle mesure voulons-nous que le risque soit atténué ? Le risque zéro est un objectif impossible à atteindre. L'appétit pour le cyber-risque devrait osciller entre élevé et moyen, compte tenu de l'évolution du paysage des menaces et de la technologie disponible.

- Quelles ressources sommes-nous prêts à mettre à disposition pour l'atténuation ?
- Voulons-nous assurer ou prendre à notre charge le risque résiduel ?

Une approche quantitative de l'appétence au risque cyber est actuellement difficile à mettre en œuvre et constitue l'exception plutôt que la norme. La déclaration d'appétence au risque (DAR) est généralement fondée sur une approche qualitative combinant des éléments qualitatifs et quantitatifs sous-jacents. Le niveau de la DAR est fixé par le conseil d'administration en termes de faible, moyen ou élevé. Souvent, il est fixé en comparant différents domaines de risque et en les classant par ordre de priorité. Il s'agit plutôt d'un étalonnage des différents domaines. L'étayage du DAR est un véritable défi. Il nécessite une cascade d'indicateurs partant du niveau technique/opérationnel jusqu'au niveau managérial et stratégique.

Bien que cela soit difficile, il est utile de discuter des risque cyber en termes d'impact sur l'activité en chiffres, et l'objectif n'est pas la perfection. Il faut d'abord se tromper sur les chiffres, puis laisser les dirigeants s'efforcer de répondre à ces questions de manière reproductible. Ils devraient prendre conscience que le risque cyber est un risque pour l'entreprise et l'aborder de la même manière que les autres risques.

9. Raconter l'histoire - le lien entre les risques et les services

Pour que le message soit reçu, le RSSI doit raconter l'histoire cyber dans le contexte de l'entreprise. Pour cela, il doit comprendre l'état des contrôles et leur impact sur le profil de risque qui est déterminé par les services de l'entreprise.

Un objectif important pour les organisations qui visent une véritable maturité de leur environnement de risque et de contrôle est la capacité à comprendre :

- la manière dont leurs services commerciaux (par exemple, l'octroi d'un prêt ou la réalisation d'opérations commerciales) ont une incidence sur le profil de risque cyber inhérent (par exemple, la nécessité de stocker en toute sécurité des données confidentielles sur les clients)
- comment le risque cyber inhérent peut avoir une incidence sur ces services (par exemple, l'absence de stockage sécurisé des données confidentielles des clients peut entraîner la divulgation involontaire de données ou faciliter l'accès aux données pour les acteurs malveillants).

L'organisation doit s'assurer qu'elle comprend quels actifs et processus informatiques soutiennent ses services commerciaux (par exemple, quels systèmes sont nécessaires à l'octroi d'un prêt). Cela permet d'établir le profil et de mesurer le risque cyber inhérent.

L'étape suivante consiste à s'assurer que les contrôles cyber sont appliqués et mis en œuvre sur les actifs et processus informatiques par le biais de méthodes automatisées (par exemple, "contrôles en tant que code"), de sorte que l'efficacité puisse être mesurée clairement au moyen d'indicateurs de contrôle clés (par exemple, comme mentionné précédemment, KCI5 % de terminaux configurés conformément à la politique).

Cette approche permet au RSSI de fournir au conseil d'administration une description claire de la manière dont le statut actuel du risque résiduel et les lacunes connues en matière de contrôle peuvent avoir un impact sur l'entreprise et de fournir un contexte permettant de gérer avec succès l'appétit pour le risque et de prendre des décisions d'investissement pertinentes.

10. Unifier les réglementations - appliquer un « gold plating » sélectif

La plupart des réglementations contemporaines et émergentes en matière de risque cyber ont des exigences qui se superposent et s'entremêlent. Un RSSI doit mettre en œuvre toutes les réglementations pertinentes pour son organisation dans les différents lieux géographiques et secteurs en utilisant des ajustements pour unifier leur mise en œuvre.

Cette approche permet d'appliquer la même logique et le même raisonnement pour traiter des risques et des contrôles similaires, quel que soit le règlement concerné, avec une réduction significative des efforts pour le RSSI et les équipes techniques.

Cependant, il existe toujours des exceptions. Certaines réglementations peuvent stipuler des contrôles spécifiques qui sont propres à une entité donnée et potentiellement difficiles à maintenir. Dans ce cas, il est possible d'opter pour une stratégie de "gold-plating", en isolant ces contrôles, exclusivement pour cette entité. Cette application sélective minimise le travail superflu pour les autres entités de l'organisation et permet de maintenir une stratégie et un reporting de cybersécurité complets à l'échelle mondiale.

Le(s) rattachement(s) hiérarchique(s) du RSSI

Le RSSI est chargé de définir et de maintenir la vision, la stratégie et le programme de l'organisation en vue de protéger les informations et les actifs technologiques. Le RSSI doit être capable d'agir de manière autonome et indépendante (par exemple, l'article 6.4 de DORA[6]). Traditionnellement, le RSSI rend compte à un cadre dirigeant de l'entreprise, tel que le directeur des systèmes d'information (DSI), le directeur des opérations (DOO), le directeur financier (DAF) ou même le PDG. Bien que cette structure soit largement adoptée, les RSSI peuvent se trouver dans une position conflictuelle lorsque le cadre supérieur concerné est également responsable d'autres fonctions qui impliquent des décisions sur les compromis entre le respect des normes de sécurité et l'efficacité opérationnelle, etc.

Pour éviter que le RSSI n'agisse de manière isolée, nous devons maintenir un équilibre entre les intérêts des parties prenantes internes et l'atténuation du risque cyber. Une organisation peut souhaiter mettre en place un comité de pilotage de la sécurité de l'information (SteerCo) chargé de prendre des décisions opérationnelles, de surveiller les risques de sécurité et les contrôles clés, de convenir de mesures, d'arbitrer les budgets, de valider la stratégie de sécurité et de surveiller sa mise en œuvre effective.

[6] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32022R2554 (article 6)

L'efficacité du SteerCo dépend de la participation des membres concernés de la direction, tels que le Chief Risk Officer (CRO), le Chief Operating Officer (COO), le Chief Compliance Officer (CCO), le Chief Information Officer (CIO), le Chief Financial Officer (CFO), le Legal Counsel et, bien sûr, le RSSI. Un SteerCo moins fréquent mais doté de pouvoirs est préférable à des réunions fréquentes du SteerCo avec un pouvoir de décision limité.

La communication des risques cyber au conseil d'administration relèverait de la compétence du RSSI, idéalement en accord, ou au moins en toute transparence, avec le SteerCo. Le RSSI devrait disposer d'une ligne de reporting indépendante vers le conseil d'administration ou l'un de ses sous-comités, comme le comité d'audit. La fréquence des rapports sur le risque cyber au conseil d'administration doit être proportionnelle à l'importance du risque pour l'organisation, mais un rapport trimestriel serait une bonne pratique, à condition qu'il soit associé à un processus d'escalade en cas de besoin.

Ce modèle combine un pouvoir de décision effectif et une gouvernance solide et efficace.

Risque cyber lié aux produits, aux portefeuilles et à la chaîne d'approvisionnement

Les principes décrits dans nos livres blancs sur la communication au conseil d'administration des risques cyber de l'entreprise peuvent facilement être transposés et étendus au *risques cyber des produits* (dans quelle mesure vos produits sont-ils protégés?), au *risques cyber du portefeuille* (quels sont les contrôles clés que vous souhaiteriez imposer aux entreprises de votre portefeuille et comment voulez-vous mesurer le respect de ces contrôles clés?), ainsi que les risques cyber liés à la chaîne d'approvisionnement (actifs clés, dépendance, contrôles clés et moyens de mesurer et de signaler l'adhésion). Les KCIs peuvent différer dans ces domaines, tout en utilisant des principes similaires.

Comparaison avec les pairs

Nous avons constaté un niveau substantiel d'alignement sur les principes décrits dans ce livre blanc au sein d'une communauté intersectorielle de quarante organisations qui se sont réunies au sein d'un groupe de travail RSSI sur une base trimestrielle pendant une période de deux ans.

Nous espérons que le partage de ces pratiques au sein de la communauté élargie permettra de comparer les expériences (et les résultats) avec les pairs et même d'utiliser ces principes dans l'interaction avec les régulateurs.