# Signaler les cyber-risques aux conseils d'administration

Édition pour les conseils d'administration

Auteurs
Freddy Dezeure
George Webster
Lokke Moerel

Réviseurs
Alan Kessler
Jamie Hutchinson

Date : 14 mars 2022
Version : Finale

## Objectif

Le présent document fournit une vue d'ensemble de l'approche recommandée aux conseils d'administration en matière de cyber-risque, ainsi que de bons points de départ pour la mesure des cyber-risques par les conseils d'administration. Il s'agit d'un document complémentaire à celui adressé aux responsables de la sécurité de l'information (RSSI/CISO) sur la meilleure façon de contrôler, de mesurer et de rendre compte des cyber-risques à leurs conseils d'administration. Il doit être lu conjointement avec ce document.

## La plupart des conseils d'administration ne sont pas cyber-conscients

Les conseils d'administration ont l'obligation légale d'assurer une surveillance adéquate des risques. Le cyber-risque constitue désormais un risque d'entreprise critique, potentiellement matériel. Cependant, la plupart des conseils d'administration sont mal équipés pour faire face aux cyber-risques. Ils considèrent que la cybersécurité est un domaine trop technique, ils se contentent d'approuver les ressources et de déléguer le risque.

Pour les risques d'entreprise traditionnels, il existe une pratique établie sur la manière de signaler les informations et une répartition acceptée de la responsabilité/délégation. En ce qui concerne les cyber-risques, il n'existe actuellement pas de pratique établie. Les RSSI/CISO ont du mal à mesurer l'efficacité de leur programme de cybersécurité et à fournir une assurance raisonnable que le risque résiduel reste inférieur à l'appétit pour le risque de l'entreprise. De nombreux RSSI ne parlent pas le "langage du conseil d'administration" et ne sont pas invités à faire des rapports.

Dans les cas exceptionnels où des rapports sur les cyber-risques sont présentés au conseil d'administration, les méthodes, outils et processus utilisés sont très variés. Souvent, les rapports portent sur les progrès réalisés dans la mise en œuvre des mesures de cybersécurité (mesure des *efforts*, rapports où tous les indicateurs sont souvent au vert), plutôt que sur la *réduction des risques*.

## Tout est une question de risque

Notre cyber-environnement nous oblige à faire des choix quant à ce qu'il faut protéger et comment. La sécurité parfaite est une illusion et les ressources sont limitées. Les évaluations et les décisions concernant les priorités sont facilitées et objectivées par l'utilisation de l'évaluation des risques. Pour la cybersécurité, nous utilisons un modèle dans lequel le risque est composé de trois facteurs : **menace**, **vulnérabilité** et **impact**.

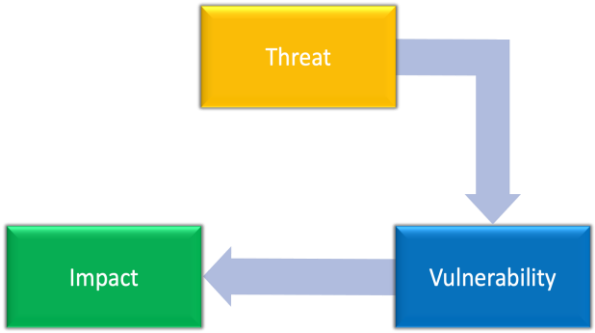



*Figure 1 Le risque est une combinaison de menace (threat), de vulnérabilité (vulnerability)et d'impact (imapct).*

**La menace** est principalement externe à notre organisation et est étroitement liée aux adversaires qui pourraient lui nuire. L'identification de nos **principaux adversaires** et de leurs motivations est importante pour la hiérarchisation de nos mesures d'atténuation. Nous pouvons observer les menaces actuelles et essayer de prédire les menaces futures.

Le deuxième facteur est la **vulnérabilité,** et c'est celui sur lequel nous pouvons avoir le plus d'influence en concevant et en mettant en œuvre des contrôles et des mesures d'atténuation. L'identification des **contrôles clés**, la prise en compte de nos principaux actifs, ainsi que de la motivation et des méthodes de nos principaux adversaires sont importantes pour établir des priorités.

En termes d'**impact**, nous pouvons penser au vol de propriété intellectuelle, à la fuite de données privées, à l'interruption de service, au préjudice personnel et à l'atteinte à la marque. L'impact est étroitement lié aux actifs. Il est important d'identifier nos **principaux actifs** pour établir des priorités.

## Approche recommandée aux conseils d'administration

### 1. Devenir cyber-conscient et obtenir une assurance raisonnable

Demandez des rapports réguliers et pas seulement en cas d'incident. Encouragez les rapports honnêtes et pas seulement les rapports indiquant que tout est bon. Insistez sur l'alignement interne et sur des canaux de communication clairs, le RSSI/CISO jouant un rôle central, garantissant une vision professionnelle et indépendante du cyber-risque[1] .

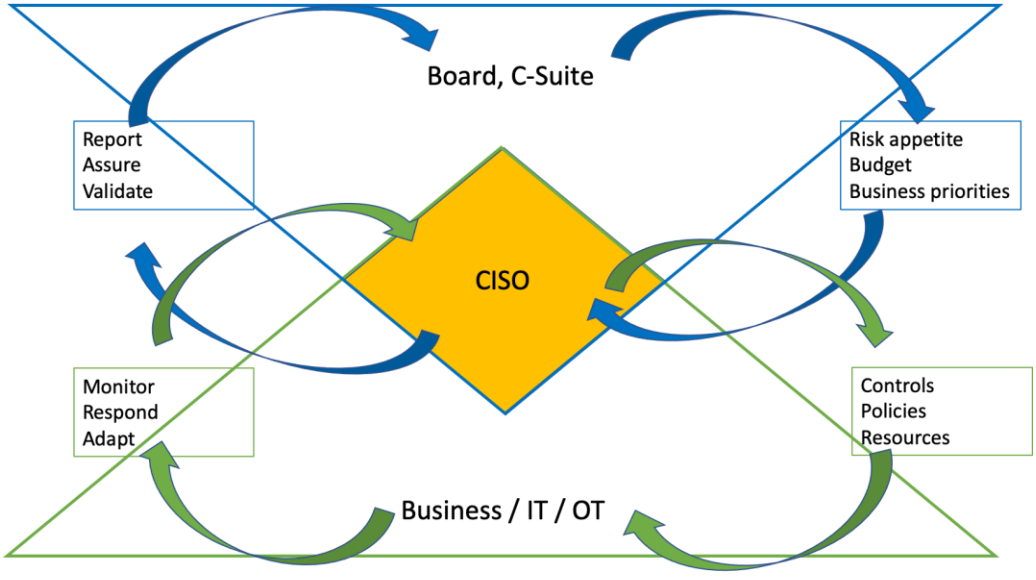



*Figure 2 Flux d'informations et rôle de coordination du CISO.*

L'établissement de rapports sur le cyber-risque doit servir à (r)assurer le conseil d'administration qu'il se situe dans les limites de l'appétit pour le risque :

- Sommes-nous assez bons ?
- Les ressources allouées sont-elles appropriées et efficaces ?
- Comment nous situons-nous par rapport à nos pairs et à notre secteur ?

[1] Flux d'informations, inspiré du cadre de cybersécurité du NIST https://www.nist.gov/cyberframework

Les indicateurs rapportés pourraient être combinés avec le contexte des incidents importants à l'intérieur et à l'extérieur de l'entreprise, des menaces et des évolutions réglementaires. Le RSSI/CISO devrait signaler toute évolution qui modifie sensiblement la situation, en bien ou en mal, et proposer des actions et des ressources appropriées en conséquence.

Un exemple de rapport est joint en annexe.

## 2. Posez les bonnes questions situationnelles

Les questions que les conseils d'administration doivent poser à leur RSSI/CISO sont étroitement liées aux facteurs de risque.

- Avons-nous un inventaire des principaux actifs ?
- Quels types d'adversaires nous ciblent et pourquoi ?
- Quels sont nos contrôles clés et quel est leur état ?
- Où sont les lacunes et comment comptons-nous les combler ?
- Avons-nous un plan de réponse aux incidents / de continuité des activités / de résilience ?
- Quel est le montant à risque ?
- Comment nous comparons-nous à nos pairs ?

## 3. Maîtrisez vos risques

Les cadres de cybersécurité sont un outil permettant de gérer les risques de cybersécurité de manière cohérente et de mettre en œuvre une stratégie de cybersécurité d'entreprise. Les cadres les plus utilisés sont la norme ISO/IEC 27001[2] et le cadre de cybersécurité du NIST.[3] Le cadre choisi par une organisation n'a pas beaucoup d'importance car il existe des correspondances entre eux. Pour les conseils d'administration, il est toutefois important de s'assurer qu'il existe un alignement interne complet (entre le RSSI/CISO, la gestion de l'infrastructure IT et opérationnelle et la gestion des risques) sur le cadre utilisé par l'organisation.

Les cadres comportent généralement des centaines de contrôles dont il est impossible de rendre compte au niveau du conseil d'administration. Il faut donc identifier les contrôles clés. Les orientations publiées par les autorités nationales chargées de la cybersécurité constituent un bon point de départ.

Il existe un large degré de chevauchement entre ces différents ensembles d'orientations de base et ils constituent un excellent point de départ, succinct et pratique. Vous trouverez ci-dessous quelques-uns des contrôles clés qui sont invariablement inclus :

- K1: Maintenir un inventaire à jour de tous les actifs (clés) et dépendances;
- K2: Produire des sauvegardes fiables, valides, sûres et sécurisées des actifs clés;
- K3: Appliquer l'authentification multifactorielle partout où cela est possible;
- K4: Limiter les autorisations d'accès des utilisateurs au strict nécessaire ;

[2] https://www.iso.org/isoiec-27001-information-security.html
[3] https://www.nist.gov/cyberframework

- K5: Identifier les vulnérabilités importantes et y apporter des correctifs en temps utile;
- K6: Collecter et analyser les journaux de tous les actifs clés;
- K7: Segmenter le réseau pour protéger les actifs clés;
- K8: Renforcer les systèmes d'accès à Internet;
- K9: Mettre en œuvre un processus de réponse aux incidents et de récupération;
- K10: Sensibiliser les utilisateurs (y compris les membres du conseil d'administration).

L'impact de chaque contrôle pourrait être mesuré et faire l'objet d'un reporting sous la forme d'un "score de couverture", combinant le déploiement, le fonctionnement et l'efficacité d'un contrôle.

# Annexe : Exemple de rapport

## Développement du paysage des menaces

| Who? | Group / Malware? | Why? | Trend |
|---|---|---|---|
| Adversary 1 | APTX | Adversary known to steal intellectual property in high tech industry. | → |
| Adversary 2 | APTY | State sponsored actor known targeting critical infrastructure | ↗ |
| Adversary 3 | FINX | Ransomware actor increasingly prevalent and sophisticated | ↗ |

## Incidents notables et évolution des menaces

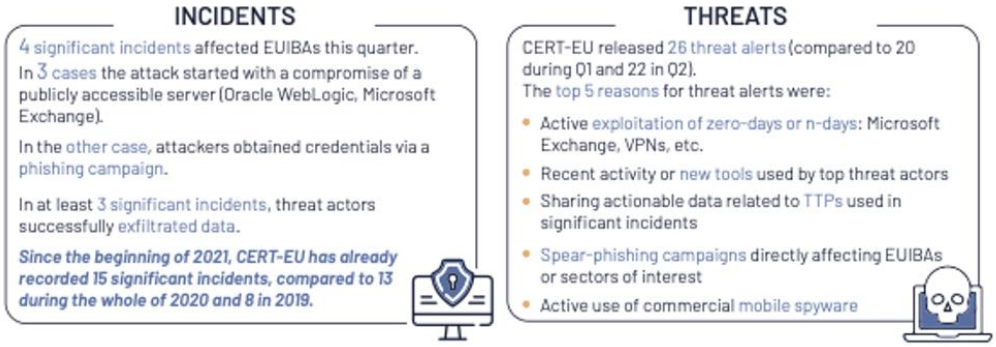
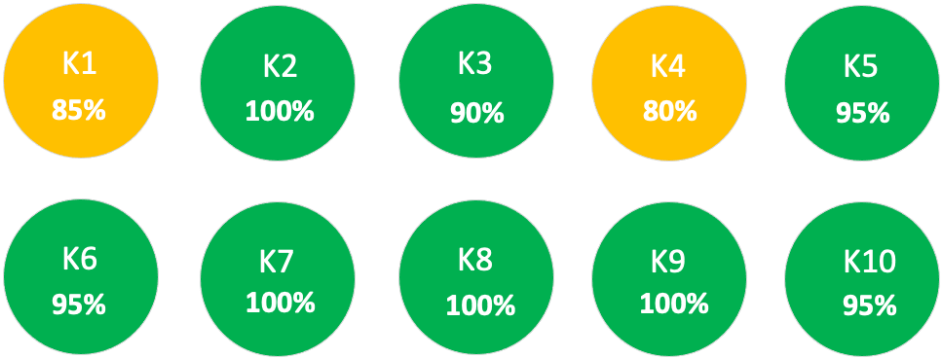
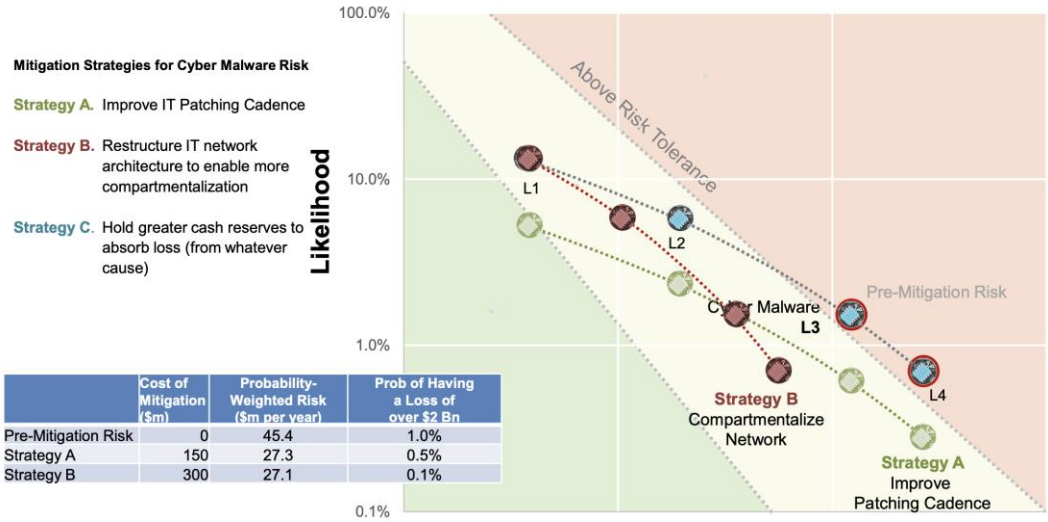



*Figure 3 Crédit CERT-EU*

## Couverture des contrôles clés




## Impact des mesures supplémentaires sur l'atténuation du cyber-risque




| | Cost of Mitigation ($m) | Probability-Weighted Risk ($m per year) | Prob of Having a Loss of over $2 Bn |
|---|---|---|---|
| Pre-Mitigation Risk | 0 | 45.4 | 1.0% |
| Strategy A | 150 | 27.3 | 0.5% |
| Strategy B | 300 | 27.1 | 0.1% |

*Figure 4 Credit Center for Risk Studies, Université de Cambridge*