Signaler les cyber-risques aux conseils d'administration

Édition RSSI/CISO

Contrôler, mesurer, signaler, répéter

Auteurs
Freddy Dezeure
George Webster
Jason Trost
Eireann Leverett
João Pedro Gonçalves
Patrick Mana
Greg McCord
Josh Magri

Réviseurs
Lokke Moerel
Alex Iftimie
Chris Deverell
Greg Bell
Jamie Hutchinson

Date : 14 mars 2022
Version : Finale

Table des matières

Introduction

Ce document fournit des méthodes et une inspiration aux responsables de la sécurité de l'information (RSSI/CISO) pour concevoir et mettre en œuvre des méthodes quantitatives afin de rendre compte du cyber-risque au niveau du conseil d'administration et de fournir une assurance raisonnable que le risque reste dans les limites de l'appétit pour le risque.

Il fut un temps où vous pouviez protéger vos secrets en fermant une porte à double tour. Pour vos secrets les plus précieux, vous avez peut-être installé une porte plus solide, renforcé les murs ou posté quelques gardes. Lorsque vous deviez déplacer vos secrets, vous les mettiez dans un sac et utilisiez la stéganographie ou la cryptographie pour protéger le secret des regards indiscrets. Cette solution digne d'un conte de fées s'appliquait également aux ordinateurs, mais l'époque où elle fonctionnait est révolue depuis longtemps. Notre société, notre économie et notre vie quotidienne dépendent de l'échange d'informations qui circulent dans nos systèmes interconnectés. Le concept d'une simple clôture protectrice est de l'histoire ancienne.

L'économie moderne et sa dépendance à l'égard des données ont conféré une valeur toujours plus grande à nos secrets, ce qui a attiré l'attention des criminels professionnels, qui ne cessent de mettre nos défenses à l'épreuve. Nos systèmes d'information représentent un risque important tant pour les gouvernements que pour les entreprises et les particuliers. En 2021, le coût moyen d'une violation de données dans une entreprise type était de 4 millions de dollars. Une violation majeure pourrait même dépasser les 400 millions de dollars[1] . Le coût total de tous les incidents liés à la cybersécurité en 2020 est estimé à 1000 milliards de dollars, soit une augmentation de plus de 50 % en deux ans[2] .

Il n'est pas étonnant que la cybersécurité soit une question prioritaire pour la plupart des organisations et des gouvernements, et cette attention est légitimement méritée. À titre d'exemple, les nouvelles réglementations de la SEC relatives à la divulgation des risques de cybersécurité comprennent des dispositions sur l'importance de communiquer les risques de cybersécurité aux conseils d'administration[3] .

Mais se faire entendre des hauts responsables ne résout pas les problèmes de cybersécurité et ne réduit pas les risques. Nos dirigeants d'entreprises et de gouvernements sont mal outillés pour traiter de la cybersécurité dont ils ne comprennent pas le langage. La cybersécurité n'est pas mieux outillée pour s'adresser aux parties prenantes de haut niveau parce que les professionnels de la cybersécurité ont du mal à mesurer l'efficacité de leur programme, à articuler son utilité ou même à communiquer ses succès. Cette incapacité à mesurer l'efficacité des contrôles de cybersécurité et à communiquer la réduction des risques qu'ils permettent aux parties prenantes de haut niveau place les professionnels de la cybersécurité dans une position où ils se battent

[1] https://www.ibm.com/security/data-breach
[2] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf
[3] https://www.mofo.com/resources/insights/220311-sec-proposes-cybersecurity-disclosure-rules.html

pour obtenir des budgets, sans savoir si ce qu'ils font réduit réellement le risque de pertes.

Le risque zéro est inaccessible et irréaliste. Il l'a toujours été. Mais la dynamique a changé. De plus, le rythme des changements dans le paysage des menaces de cybersécurité dépasse notre capacité à adapter les contrôles aux risques ou même à identifier les contrôles qui sont importants pour atténuer les risques. Le RSSI/CISO doit justifier le budget de cybersécurité et expliquer en quoi les approches choisies sont conformes à l'appétit de l'organisation pour le risque. S'il s'agit effectivement d'une tâche difficile, le présent document vise à fournir l'inspiration et les éléments nécessaires pour concevoir et mettre en œuvre des solutions pragmatiques.

Objectif

Ce document présente des orientations permettant aux RSSI/CISO de rendre compte des cyber-risques et de leur contexte à leurs parties prenantes de haut niveau, telles que leur conseil d'administration. Il décrit des méthodes qui aident les RSSI/CISO à s'engager dans la gestion des cyber-risques, à communiquer efficacement et à faciliter une surveillance adéquate. Bien qu'il ne s'agisse pas d'un point central de ce document, son contenu est également utile pour rendre compte des cyber-risques à d'autres parties prenantes, comme les régulateurs, les assureurs et les clients.

Nous pensons qu'un système de mesure est une composante nécessaire de tout effort couronné de succès. Les théories de Peter Drucker en matière de gestion en témoignent et ont, par conséquent, changé le fonctionnement des entreprises. Il en va de même pour la cybersécurité. Il est nécessaire de disposer d'un système de mesure pour guider la gestion des risques dans les organisations, pour accroître la cyberrésilience au fil du temps et pour démontrer aux parties prenantes internes et externes que les règles sont respectées. Toutefois, il faut bien choisir ce que l'on mesure et envisager le problème de manière globale. Malheureusement, mesurer les risques de cybersécurité et appliquer un système de mesure approprié s'apparente à la recherche du Saint Graal. Les bonnes pratiques en matière de mesure des risques sont peu nombreuses, elles sont rarement diffusées au sein de la communauté et la mesure du risque dans un paysage de menaces de cybersécurité non déterministe est un défi.

Le présent document résume les conclusions et les meilleures pratiques d'un groupe de travail de RSSI/CISO. Tout le mérite en revient aux participants. Sans leurs idées, leurs échanges et leurs interactions, ce document n'aurait pas vu le jour. Des annexes contenant des exemples de la communauté sont incluses dans ce document. Nous espérons susciter des contributions supplémentaires afin de créer un nouveau corpus de travaux et d'exemples de mise en œuvre. Pour encourager l'interaction et le partage au sein de la communauté, nous prévoyons une diffusion supplémentaire à l'avenir.

Attentes du conseil d'administration

Les préoccupations des conseils d'administration portent généralement sur les questions suivantes :

- Positionnement stratégique et croissance de l'organisation
- Valeur pour l'actionnaire, protection de la marque
- Plans stratégiques, affectation des ressources, rémunération des cadres
- Surveillance de la conformité (réglementations gouvernementales et sectorielles, ESG)
- Risques critiques pour les activités - y compris la cybersécurité
- Comparaison avec le secteur/les pairs
- La responsabilité fiduciaire des membres individuels du conseil d'administration.

Pour la plupart de ces domaines, il existe une pratique établie quant à la manière de recueillir des preuves et de faire rapport à leur sujet de manière utile, avec un niveau de granularité et une répartition des responsabilités/délégation appropriés.

En ce qui concerne la cybersécurité, la pratique établie dans le secteur est moins mature. Souvent, les conseils d'administration ne se sentent pas suffisamment compétents pour comprendre les cyber-risque ou trouvent le domaine trop technique, ils approuvent les ressources et délèguent la gestion de ce risque.

Les conseils d'administration ne perçoivent souvent pas l'importance permanente de la cybersécurité et réagissent de manière impulsive quand des affaires de cybersécurité font la une dans les médias, puis oublient rapidement jusqu'au prochain cyberincident. En général, ils ne s'intéressent à la cybersécurité que lorsqu'il est déjà trop tard.

Cette attitude est parfois accentuée par une culture de gestion non transparente, où le message donné systématiquement est que tout va bien / tous les indicateurs sont au vert, alors qu'en réalité, la plupart des conseils d'administration voudraient entendre parler des lacunes et de la manière dont elles peuvent être comblées.

Dans les cas où des rapports sur la cybersécurité sont présentés au conseil d'administration, une grande variété de méthodes, d'outils et de processus sont utilisés. Les organisations peinent à définir ce qu'elles doivent signaler et comment obtenir un retour d'information efficace de la part du Conseil.

La notion de risque est centrale

Notre cyberenvironnement 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 des pratiques établies d'évaluation des risques.

Il existe différentes définitions du risque, centrées sur la possibilité qu'un incident, un événement ou une circonstance se solde par un résultat non

souhaité, déterminé par sa **probabilité** et l'**impact** associé[4] . Un exemple concret de risque est la possibilité de mourir ou de tomber gravement malade à la suite d'une infection par un virus pandémique.

Pour notre discussion, nous utiliserons le modèle élargi dans lequel le risque est composé de trois facteurs : **Menace** x **Vulnérabilité** x **Impact**. Dans cette équation, la probabilité est étendue à une combinaison de menace et de vulnérabilité, ce qui est utile dans le contexte de la cybersécurité. Nous ne couvrons pas les événements accidentels.

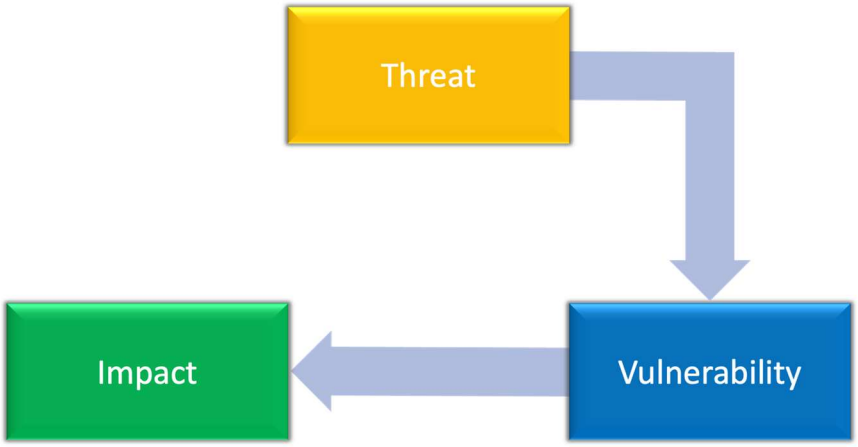


Figure 1 Le risque est une combinaison de menace, de vulnérabilité et d'impact.

La menace est principalement externe à notre organisation et est étroitement liée aux adversaires. L'identification de nos principaux adversaires et de leurs motivations est importante pour établir des priorités. Nous pouvons observer les menaces actuelles et essayer de prédire les menaces futures. Les entreprises spécialisées dans le renseignement sur les menaces et les services gouvernementaux peuvent nous aider à comprendre quels sont nos adversaires, quels sont leurs motifs, quels outils et méthodes ils utilisent et comment ils opèrent pour atteindre leurs objectifs.

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. L'identification des contrôles clés, la prise en compte de nos principaux actifs, ainsi que la motivation et les méthodes de nos principaux adversaires sont importantes pour l'établissement des priorités.

En termes d'**impact**, nous pouvons penser au vol de propriété intellectuelle, à la fuite de données à caractère personnel, 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.

[4] https://www.dhs.gov/xlibrary/assets/rma-risk-management-fundamentals.pdf

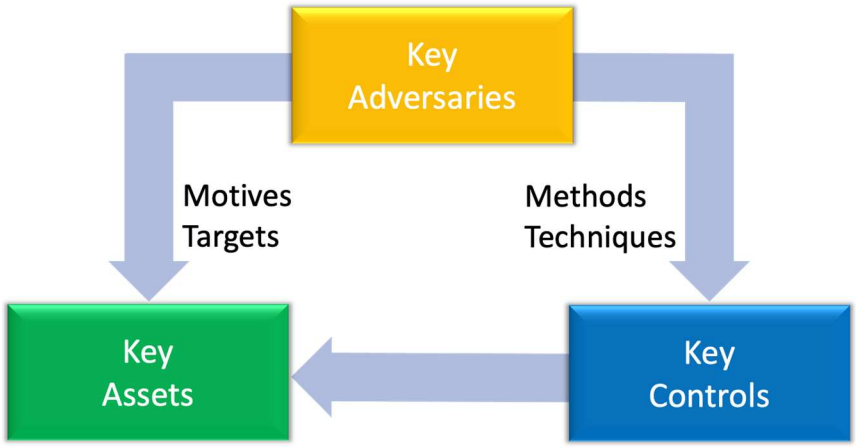


Figure 2 Le cyber-risque résulte du fait que les adversaires ciblent les actifs en exploitant les vulnérabilités.

Nous pensons que nous devons aborder le problème de la cybersécurité comme un problème de gestion des risques et utiliser la gestion et l'atténuation des risques en connaissance de cause pour hiérarchiser les actions en permanence. La cybersécurité doit être intégrée dans le système de gestion global, elle ne doit pas être considérée comme un élément spécial/isolé mais comme une partie intégrante des activités et processus organisationnels, y compris le processus de gestion des risques. Cette approche nécessite un alignement des méthodes et du vocabulaire.

Pour illustrer les flux d'informations pertinents dans le présent document, nous utiliserons le diagramme de la figure 3, inspiré du NIST Cyber Security Framework[5] .

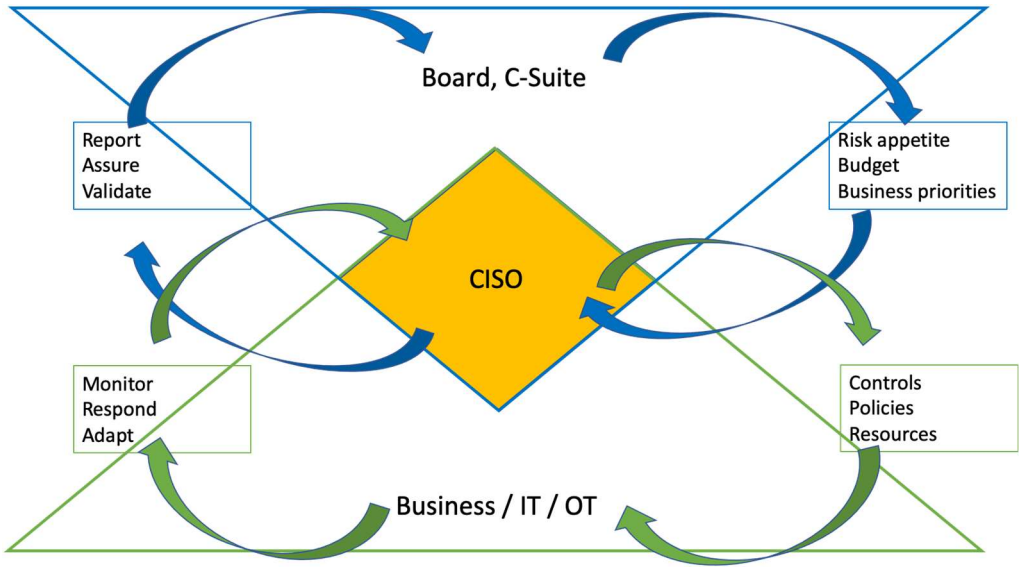


Figure 3 Flux d'information et de décision. Inspiré du CSF du NIST

Nous pouvons distinguer une partie supérieure, celle des cadres supérieurs, et une partie inférieure, celle de la mise en œuvre et des opérations, avec le RSSI/CISO dans la zone centrale de chevauchement, qui fait le lien entre le niveau opérationnel de la cybersécurité et le niveau stratégique.

[5] https://www.nist.gov/cyberframework

Des choix importants à faire

Il est nécessaire pour les organisations de faire des choix fondamentaux pour la gestion des cyberrisques. Ces choix sont illustrés dans la partie droite du diagramme : quels sont les principaux actifs, quelle est la propension au risque et quels sont les principaux contrôles/mesures d'atténuation à mettre en place. Et en relation avec ces choix, le budget et l'affectation des ressources aux moyens et au personnel de cybersécurité.

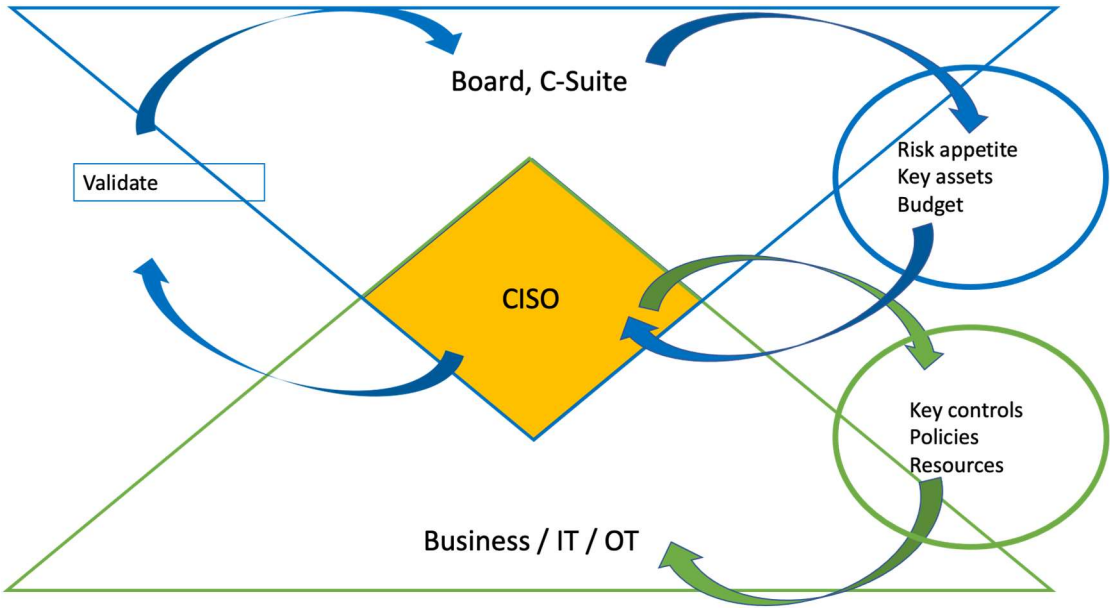


Figure 4 Choix à faire

Il est essentiel que les choix proposés par le RSSI/CISO soient approuvés et harmonisés dans l'ensemble de l'organisation (cybersécurité, risque, IT/OT, entreprise) et qu'ils soient compris/approuvés et tenus à jour au niveau de la direction.

Actifs clés – les joyaux de la couronne

Dans la plupart des organisations, le coût de la protection de tous les actifs contre toutes les cybermenaces possibles est prohibitif. Il faut identifier les priorités et allouer les ressources aux menaces les plus pertinentes visant les actifs les plus importants. L'identification de ces actifs clés est une composante essentielle de la gestion des risques de l'entreprise en général et de la gestion des risques de cybersécurité en particulier.

Il s'agit d'une tâche non négligeable, qui nécessite une analyse et une évaluation transversales, en tenant compte de l'impact potentiel sur la continuité des activités, la confidentialité, la réglementation et la position concurrentielle à long terme (propriété intellectuelle).

Lors de l'identification (et de la mise à jour) de la liste des actifs clés, le RSSI/CISO doit regarder au-delà des actifs informatiques (centres de données, systèmes de sauvegarde, répertoire actif, etc.) et inclure les actifs informationnels pertinents (référentiels, propriété intellectuelle), les actifs commerciaux (comptabilité, gestion de la production, logistique, accès physique), etc.

Il est beaucoup question de l'identification des actifs clés, aussi appelés les "joyaux de la couronne", qui est en soi une évaluation probabiliste des risques, une expression de la conviction qu'un attaquant est plus susceptible de voler x que y. Nous disons probabiliste ici, car cette approche part du principe que nous pouvons moins bien défendre certains actifs que d'autres. Toutefois, un autre élément clé du raisonnement probabiliste consiste à actualiser ces hypothèses en fonction des cybermenaces actuelles. Le cryptojacking, par exemple, se moque des joyaux de votre couronne et se contente de s'attaquer à des biens moins importants.

Il est important d'évaluer la probabilité de diverses cybermenaces (DDoS, rançongiciel, vol ciblé d'IP, violation opportuniste, phishing, fraude, infection par des logiciels malveillants - cette liste n'est pas exhaustive) dans le cadre de l'identification des actifs clés, les déchets des uns étant les trésors des autres.

Appétit pour le risque

Pour identifier les mesures d'atténuation et de contrôle des risques, une organisation doit déterminer au niveau de la direction quel niveau de contrôle est "suffisant", ou quel est le niveau de risque acceptable.

Ce faisant, nous devons exprimer l'appétit pour le risque d'une manière quantifiable, en utilisant un seuil ou une représentation graphique des situations acceptables et non acceptables. Certaines organisations utilisent des seuils financiers pour exprimer leur appétit pour le risque. Pour d'autres organisations (secteur du transport, hôpitaux, etc.), le seuil peut être lié au risque de blessure ou de mort. Dans certains cas, l'appétit pour le risque peut être lié à la continuité des activités ou à la durée acceptable d'une interruption de service.

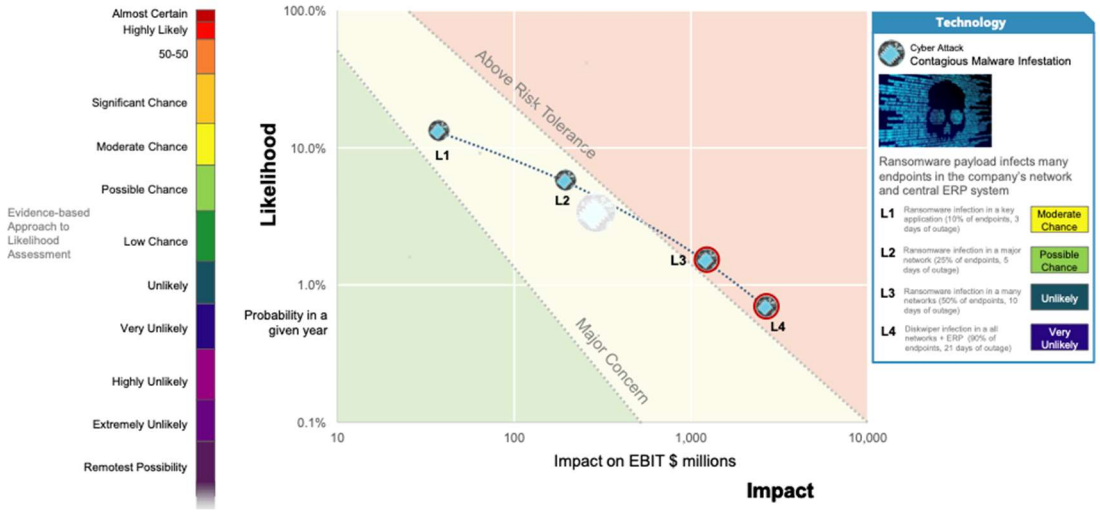


Figure 5 Exemple de cartographie de l'attitude envers le risque, crédit Center for Risk Studies, Université de Cambridge

Cadre(s) de cybersécurité et contrôles clés

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 de contrôle les plus utilisés sont l'ISO/IEC

27001[6] , le Cyber Security Framework (CSF) du NIST[7] , son dérivé le CRI Profile[8] , le NIST SP 800-53[9] ainsi que les CIS Critical Security Controls[10] . Comme alternative, ou en combinaison avec les cadres susvisés, de nombreuses organisations utilisent également le cadre MITRE ATT&CK® centré sur les menaces[11] . Bien qu'il puisse être difficile de choisir un seul cadre, ils ont tous leurs spécificités et le choix du cadre retenu importe peu car il existe des correspondances entre eux. Il est toutefois important d'en choisir un et de s'y tenir, afin que l'organisation puisse mesurer ses progrès au fil du temps.

Il est fortement conseillé à toute organisation de rechercher un accord interne sur le profil cadre à utiliser pour définir sa stratégie de cybersécurité et sa méthode d'atténuation des risques. Sans cet alignement interne entre le RSSI/CISO, l'IT/OT et la gestion des risques, il est difficile d'obtenir l'engagement du conseil d'administration sur les questions de cybersécurité.

Un bon point de départ pour l'identification et le suivi des contrôles clés est de cartographier l'adhésion aux orientations de base en matière de cybersécurité des autorités nationales de cybersécurité. Nous avons inclus une sélection de sources pertinentes dans l'annexe 1. Ces différents ensembles d'orientations de base se chevauchent largement et doivent encore être transposés à la situation spécifique d'une organisation. Cependant, elles constituent un excellent point de départ, succinct et pratique.

Quelques 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;
- K5: Identifier les vulnérabilités importantes et y apporter des correctifs en temps utile;
- K6: Recueillir 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 réaction aux incidents et de récupération;
- K10: Sensibiliser les utilisateurs (y compris les membres du Conseil d'Administration).

Nous ferons référence à ces identifiants de contrôle clé dans les exemples de systèmes de mesure ci-dessous.

[6] https://www.iso.org/isoiec-27001-information-security.html
[7] https://www.nist.gov/cyberframework
[8] https://cyberriskinstitute.org/
[9] https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
[10] https://www.cisecurity.org/controls/cis-controls-list/
[11] https://attack.mitre.org/

Mesures quantitatives

Il est judicieux de combiner la sélection d'un profil cadre avec la définition de mesures quantitatives (KPI, KRI, KCI, OKR[12]) assorties d'objectifs/de résultats et de relier ces derniers aux processus/systèmes et aux responsables de processus concernés. Ces paramètres peuvent être mesurés dans le temps par rapport aux objectifs acceptés, comparés à l'échelle de l'entreprise et comparés à ceux des pairs. Quelques bonnes pratiques sectorielles montrent le potentiel de cette approche :

- Mesures et métriques des contrôles CIS[13];
- Mesures de cybersécurité de l'EPRI pour le secteur électrique[14];
- Bibliothèque de mesures de cyber-résilience de l'association néerlandaise des paiements[15];
- Les ICP du secteur automobile allemand liés à la norme ISO27001[16];
- Guide de mesure de la performance du NIST[17].

La plupart des cadres supposent que les organisations qui les mettent en œuvre utilisent l'auto-évaluation, éventuellement combinée à une forme d'examen externe par un organisme de certification ou d'audit. L'auto-évaluation est également conforme aux pratiques standard de la gestion des risques d'entreprise.

La surveillance par auto-évaluation présente des inconvénients fondamentaux pour fournir l'état des mesures d'atténuation des cyber-risques et leur efficacité. Ces inconvénients sont notamment les suivants :

- l'auto-évaluation est subjective (pas de séparation des tâches, même niveau de connaissance);
- elle n'offre pas une degré de granularité suffisant;
- sa mise en œuvre prend beaucoup de temps;
- elle est déconnectée des événements sur le plan temporel;
- elle ne peut pas être utilisée pour l'alerte/le passage au palier d'intervention supérieur/la réaction;
- il se peut qu'un audit indépendant soit nécessaire pour qu'elle soit acceptée par les régulateurs;
- elle peut se limiter à des indicateurs de déploiement (qu'est-ce qui a été mis en œuvre ?).

Les données générées par des machines peuvent compléter très utilement l'auto-évaluation, voire la remplacer dans une large mesure. Elles peuvent rendre le reporting sur les risques pour la cybersécurité objectif, reproductible et automatisé. L'identification des sources de données générées par la machine et des analyses nécessaires pour les mesures est une étape importante dans le

[12] Objectifs et résultats clés, High Output Management, Andrew S. Grove.
[13] https://www.cisecurity.org/insights/white-papers/cis-controls-v7-measures-metrics
[14] https://www.epri.com/research/products/000000003002010426
[15] https://www.betaalvereniging.nl/wp-content/uploads/Library-of-Cyber-Resilience-Metrics-Shared-Research-Program-Cybersecurity.pdf
[16] https://www.vda.de/vda/en/News/publikationen/publication/vda-isa-catalogue-version-5.0.4
[17] https://csrc.nist.gov/publications/detail/sp/800-55/rev-2/draft

processus de conception et de mise en œuvre d'un ensemble de mesures cohérent, complet et efficace.

Le principal danger des mesures du cyber-risque est qu'elles commencent à refléter le travail effectué ou l'effort mis en œuvre, plutôt que la réduction du risque. Un conseil d'administration ou une équipe de direction doit s'opposer rigoureusement à l'inclusion de telles mesures. Il faut que les mesures donnent une indication du bon déroulement des activités et non des risques. En d'autres termes, évitez les mesures du nombre d'incidents traités ou de logiciels malveillants mis en quarantaine. Ce sont des mesures opérationnelles fantastiques, mais elles ne disent pas au conseil d'administration si le budget consacré à la réduction des risques donne des résultats. Un élément déterminant réside dans le fait qu'une mesure de risque prend généralement la forme d'une proportion ou d'un ratio, comme le nombre d'accidents pour 1000 kilomètres parcourus. Si une mesure ne comporte pas de ratio, il faut se pencher davantage sur la mesure de la variance du risque.

De même, il est parfois bon qu'une mesure indique une augmentation du risque. Les systèmes d'alerte précoce démontrent l'efficacité de l'équipe de gestion des risques, or le cyber-risque est dynamique. Par conséquent, soyez ouverts aux mesures ou aux équipes qui communiquent une augmentation du risque, elles peuvent être porteuses d'un message très opportun pour vous.

Un certain nombre de mots-clés viennent à l'esprit lorsqu'on réfléchit à ce qui constitue une bonne méthode de mesure :

- objective
- immuable
- reproductible
- continue
- pertinente
- efficace
- informée
- définie d'un commun accord
- réalisable

Un modèle de mesure

Nous proposons un modèle de mesure comportant les trois étapes suivantes :

1. rassembler les cyber-preuves pertinentes;
2. traduire ces preuves en risques commerciaux[18];
3. faire rapport au conseil d'administration, fournir une assurance raisonnable et mettre en évidence les lacunes.

Dans ce modèle, chaque étape est décomposée en blocs que nous illustrons et commentons ci-dessous, et pour lesquels des exemples de la communauté sont inclus dans l'annexe 2. L'objectif est de fournir une inspiration et des idées pour des solutions spécifiques à l'organisation plutôt que d'en déduire que nous

[18] Le risque commercial est l'exposition d'une organisation à des facteurs qui réduiront ses objectifs financiers ou la conduiront à l'échec. Un risque d'entreprise peut être de plusieurs types : stratégique, opérationnel, de réputation, de conformité ou financier.

proposons une solution parfaite au défi que constituent la mesure et le reporting du cyber-risque.

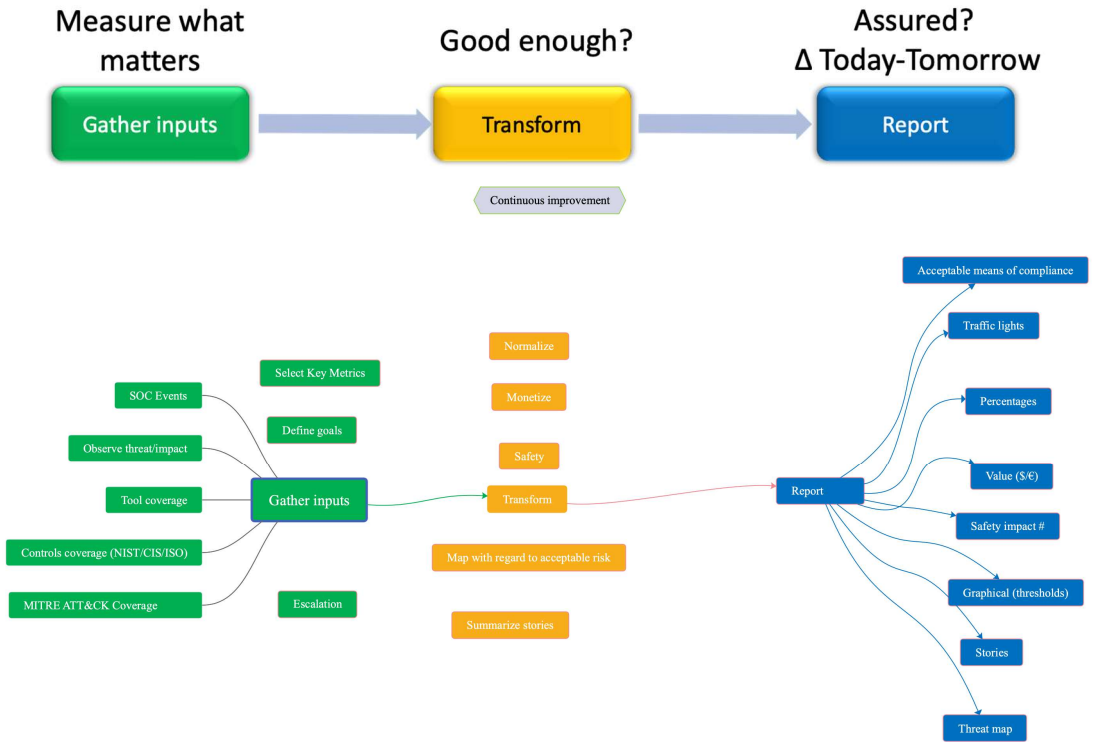


Figure 6 Modèle de système de mesure

Des boucles d'amélioration (locales et globales) doivent être incorporées dans le modèle de mesure et ses processus pertinents, en l'adaptant aux changements dans les attentes des parties prenantes ainsi que dans la posture de risque (paysage des menaces, vulnérabilités, dépendances). Les idées et les méthodes issues de la communauté sont également source d'améliorations.

Recueillir des données - mesurer ce qui compte le plus

Du côté des entrées du modèle de mesure, nous trouvons des mesures techniques, qui devraient être (un sous-ensemble de) celles qui sont utilisées par les entreprises/opérations pour mettre en œuvre et surveiller l'atténuation des cyber-risques opérationnels. Dans la Figure 7, nous trouvons ces systèmes de mesure technique dans la partie inférieure gauche du diagramme.

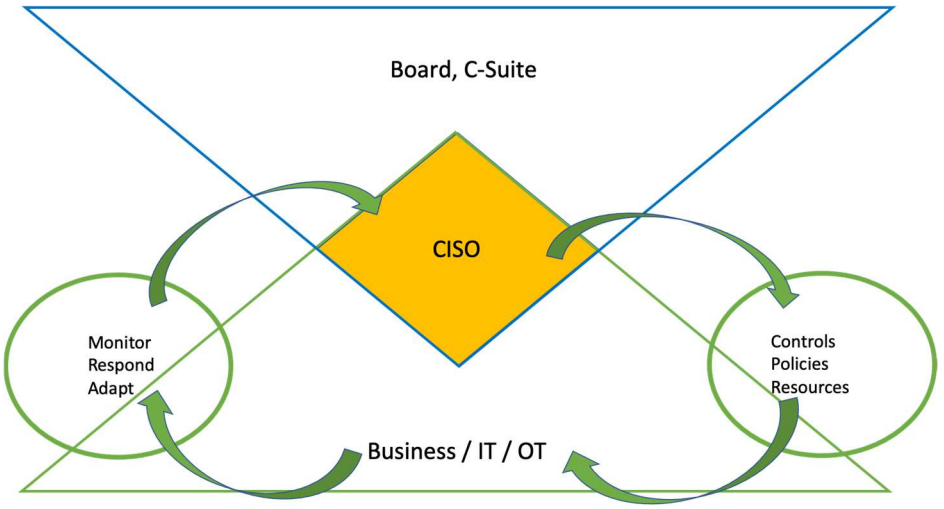


Figure 7 Mesures techniques - entrées

Figure 8 Collecte des données - composantes

Nous pouvons distinguer différentes familles de mesures clés opérationnelles que nous regroupons par nature (**centrées sur le contrôle**, **sur la menace**, **sur les outils** et **sur les événements**).

Centré sur le contrôle

Dans cette catégorie, nous trouvons des paramètres que l'organisation identifie pour mesurer l'alignement avec un ensemble de contrôles clés. Ils sont liés à un cadre de contrôle (NIST CSF, ISO, CIS, etc.).

Les mesures centrées sur le contrôle pourraient inclure:

- le degré de couverture d'un contrôle - pour tous les biens ou un groupe sélectionné de biens (clés);
- l'efficacité d'un contrôle;
- la source de données et la fréquence de mise à jour;
- le seuil défini.

Une variante (offrant un degré de granularité plus élevé) de cette approche centrée sur le contrôle décompose la couverture d'un contrôle en trois éléments : déployé, opérationnel et efficace. Il est important de noter que ces mesures doivent être effectuées en continu car le paysage des menaces et la capacité du contrôle à gérer les risques évoluent dans le temps. Ces trois contrôles sont définis comme suit :

- déployé - le contrôle est-il en place là où il doit l'être;
- opérationnel - le contrôle fonctionne-t-il comme prévu;
- efficace - le contrôle fonctionne-t-il efficacement, une mesure ("preuve") de la contribution d'un contrôle donné à la réduction du risque sur une période donnée.

Pour chacun de ces trois domaines, un score est établi en collectant des preuves. Un score combiné des trois domaines donne un "score de couverture".

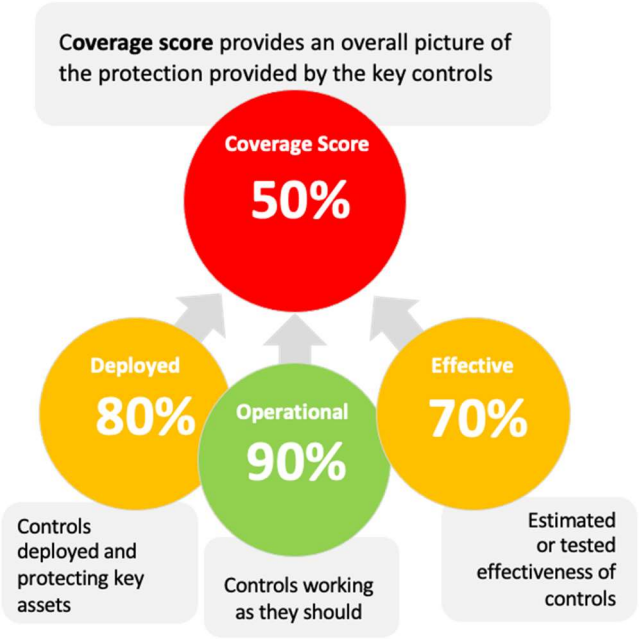


Figure 9 Exemple de mesure centrée sur le contrôle dans une infection pandémique

Un exemple concret de ce concept peut être trouvé dans les infections pandémiques, un vaccin étant l'un des contrôles clés possibles :

- le déploiement concernerait la partie de la population vaccinée (dans cet exemple, 80 %);

- si le vaccin ne génère une réponse immunitaire qu'après une certaine période, cela génère une différence dans la part des vaccins déployés qui sont opérationnels (dans ce cas, 90 %);
- un vaccin n'est efficace que dans une certaine mesure (dans ce cas, 70 %);
- par conséquent, dans ce cas, la couverture globale est de 50 % (une combinaison des trois facteurs).

$$\eta = \frac{70}{100} \times \left(\frac{90}{100} \times 80\right)$$
$$\eta = 50.4$$

L'efficacité des contrôles peut être testée sur des contrôles individuels (test d'intrusion) ou sur l'ensemble des contrôles déployés (équipe rouge, ou *Red Teaming*). Dans ce dernier cas, le résultat pourrait être utilisé pour estimer le niveau global d'atténuation du cyber-risque.

Une approche centrée sur les contrôles se retrouve généralement dans les environnements fortement réglementés. À titre d'exemple, les services gouvernementaux américains sont censés mettre en œuvre la norme NIST 800-53, qui comprend quelque 1 000 contrôles et améliorations de contrôle.

Cependant, même dans les environnements réglementés avec des contrôles obligatoires, il est judicieux d'identifier les contrôles clés qui comptent le plus pour atténuer le cyber-risque actuel. La sélection des contrôles clés pourrait être favorisée par la compréhension des principales menaces (motifs et techniques) et des principaux actifs ciblés.

Quelques exemples de mesures centrées sur le contrôle

- K1 : Pourcentage d'actifs (clés) (terminaux, réseau, serveurs) inventoriés;
- K1: Bases de données non cryptées stockant des informations personnelles identifiables ;
- K2: Pourcentage d'actifs clés conformes à la politique de sauvegarde ;
- K4: Pourcentage de points d'accès sans droits d'administration locaux ;
- K4: Pourcentage de points d'accès pour lesquels la mise sur liste blanche des applications est mise en œuvre;
- K4: Pourcentage de comptes privilégiés pour lesquels une solution de contrôle d'accès s'applique;
- K8: Pourcentage des actifs (clés) accessibles sur internet qui font l'objet d'une analyse hebdomadaire pour détecter les vulnérabilités et les problèmes de configuration;
- K9: Pourcentage d'applications critiques pour lesquelles aucune analyse d'impact sur les activités n'a été effectuée;
- K10: Pourcentage du personnel ayant suivi une formation sur la cybersécurité au cours de l'année écoulée (y compris les membres du conseil d'administration);
- Efficacité des contrôles clés vérifiée par l'équipe rouge ou par des tests automatisés.

Centré sur la menace

Dans cette catégorie, nous trouvons des systèmes de mesure dans lesquelles l'organisation identifie ses adversaires les plus importants et suit les TTP (techniques, tactiques, procédures) que ceux-ci ont l'habitude de déployer en utilisant le cadre ATT&CK® de MITRE. Les mesures d'atténuation sont mises en correspondance avec ces techniques de manière similaire à l'approche centrée sur le contrôle. Ces connaissances doivent être tenues à jour au vu des dernières informations sur les adversaires notables et des incidents pertinents.

Dans la figure ci-dessous, l'utilisation de techniques par différents groupes d'adversaires pertinents est mise en évidence en couleur, du jaune (moins répandu) au rouge (techniques utilisées par tous les adversaires pertinents).

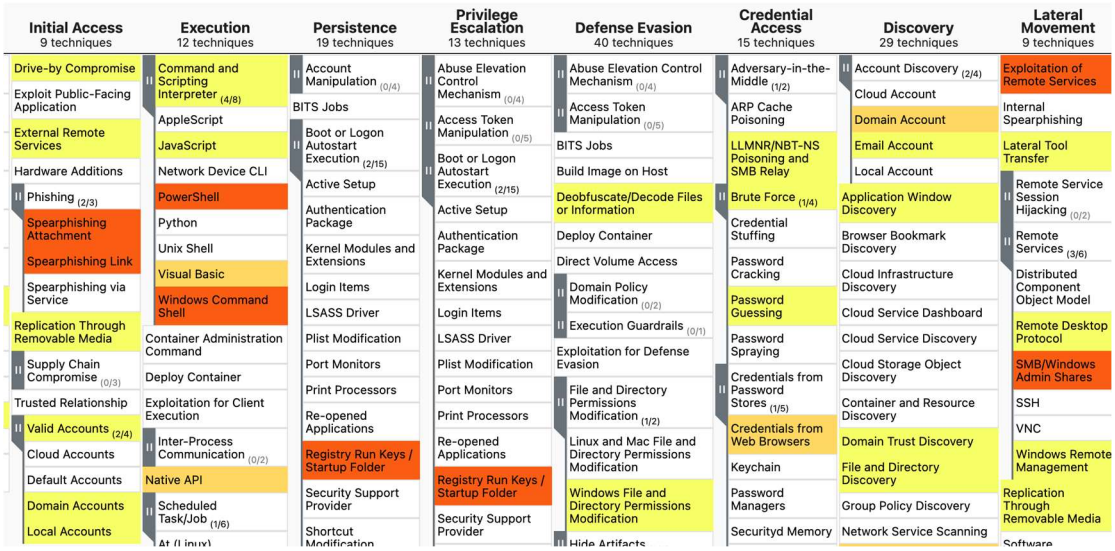


Figure 10 Exemple d'utilisation d'une carte thermique pour montrer la prévalence des techniques

Les approches centrées sur les menaces et sur les contrôles peuvent être combinées par la mise en correspondance des cadres de contrôle et de menaces[19] pour identifier les menaces pertinentes et les contrôles d'atténuation et les convertir en mesures clés.

Quelques exemples de mesures centrées sur la menace:

- le pourcentage de couverture d'atténuation des techniques connues pour être utilisées par des groupes d'adversaires notables;
- le pourcentage de couverture des mesures d'atténuation clés par un programme de test actif (automatisé ou Red Team);
- le pourcentage de couverture des adversaires notables et de leurs techniques avec les playbooks SOC et les programmes de chasse.

Centré sur l'outil

Dans cette catégorie, nous trouvons des mesures dans lesquelles l'organisation se concentre sur le déploiement d'outils de cybersécurité spécifiques (EDR, défenses périmétriques, MFA, etc.) afin d'atténuer les risques. La collecte de données sur le déploiement des outils est simple et la cartographie de

[19] https://github.com/center-for-threat-informed-defense/attack-control-framework-mappings

l'efficacité de chaque outil contre les menaces connues est également bien documentée.

Des principes similaires pourraient être utilisés comme dans l'approche centrée sur le contrôle, en utilisant la couverture/efficacité ou le déploiement/opérationnel/activable. Une approche centrée sur les outils pourrait être un tremplin vers une approche plus cohérente et complète basée sur un cadre (centré sur le contrôle ou sur la menace).

Voici quelques exemples de mesures centrées sur les outils:

- K3: Pourcentage de mise en œuvre de l'authentification multifactorielle (MFA);
- K6: Pourcentage de systèmes disposant d'un ensemble complet d'outils et de politiques de sécurité (EDR, journalisation, logiciels et configuration de référence, politiques, etc ;)
- K6: Pourcentage d'actifs (clés) avec visibilité du journal;
- K8: Pourcentage d'actifs contraints de se connecter à l'internet via un proxy;
- Pourcentage d'actifs couverts par des contrôles automatisés et des mesures correctives.

Centré sur l'événement

De nombreuses organisations collectent des données sur les événements de cybersécurité (#alertes, #incidents, #faux positifs, #vulnérabilités, etc.). Ces statistiques peuvent fournir des informations précieuses pour la gestion du risque de cybersécurité, mais elles doivent être interprétées. Est-il bon ou mauvais que davantage de vulnérabilités soient découvertes ou que davantage d'incidents se produisent ? Les méthodes de détection se sont-elles améliorées ou les systèmes se sont-ils dégradés ?

Voici quelques exemples de mesures centrées sur les événements :

- K1: Nombre de systèmes de sécurité mis en œuvre par rapport à la couverture des actifs;
- K4: Nombre de problèmes constatés dans le suivi/le filtrage des actifs privilégiés;
- K5: Pourcentage de systèmes corrigés dans les limites de l'accord de niveau de service ;
- K6: Nombre de faux positifs dans le Security Operation Cente;
- K8: Nombre d'actifs orphelins (orientés vers l'extérieur) trouvés;
- K9: Nombre d'incidents critiques/temps moyen pour découvrir/contenir;
- K9: Pourcentage d'alertes de sécurité critiques et élevées examinées dans les limites de l'accord de niveau de service;
- K10: Nombre d'identifiants d'entreprise dans la nature (Account Take Over);
- Coût annuel des cyberincidents;
- Nombre de problèmes de sécurité et de confidentialité à haut risque ouverts au-delà de l'accord de niveau de service sans plan de remédiation.

Les données chronologiques sur les incidents et les vulnérabilités peuvent fournir des informations utiles sur les performances de l'organisation et des systèmes de cybersécurité. Des progrès notables ont été réalisés à ce sujet dans le cadre du First Metrics SIG[20] .

Risque lié à la chaîne d'approvisionnement

De plus en plus d'entreprises subissent l'impact des cyberincidents qui touchent leurs fournisseurs, soit directement par les connexions réseau ou les produits, soit indirectement par les interruptions de la chaîne d'approvisionnement qui affectent la continuité des activités. Cartographier les dépendances à l'égard des fournisseurs, se faire une idée de leur position en matière de cybersécurité et mettre en place des contrôles appropriés devient une partie intégrante de la gestion du cyber-risque et devrait donc également être inclus dans les mesures.

La surveillance du cyber-risque des fournisseurs peut être confiée à des sociétés spécialisées et les mesures d'atténuation peuvent, dans une certaine mesure, prendre la forme de clauses contractuelles et de couvertures d'assurance. Toutefois, il convient d'établir une image claire des dépendances et des scénarios de détection et de réponse. Des conseils supplémentaires peuvent être trouvés dans la publication du NIST sur les pratiques clés de la gestion des risques de la cyber chaîne d'approvisionnement[21] .

Voici quelques exemples de mesures de la chaîne d'approvisionnement:

- Pourcentage de vendeurs/fournisseurs critiques pour lesquels un inventaire des actifs, de la dépendance, de l'évaluation des risques et de l'atténuation a été réalisé;
- Pourcentage de vendeurs/fournisseurs critiques disposant d'annexes de sécurité;
- Pourcentage de fournisseurs critiques qui ont été audités;
- Nombre de vendeurs/fournisseurs critiques dont les conclusions d'audit sur la sécurité et la confidentialité présentent un risque élevé et qui ne disposent pas d'un plan de gestion des risques documenté.

Observer l'impact - Histoires

De nombreuses organisations documentent les incidents pertinents (internes, ayant un impact sur les pairs, le secteur ou la région) en utilisant des récits dans des "histoires". Ce type de preuves anecdotiques est très attrayant pour les membres non techniques de la C-Suite et du conseil d'administration, car elles illustrent ce qui peut arriver (ou est arrivé) à l'organisation. Elles permettent également au RSSI/CISO d'attirer l'attention sur les tendances en matière de fréquence, d'impact et de méthodes dans le paysage des menaces, et de soutenir la hiérarchisation des actions en termes de contrôles et d'affectation des ressources.

Sélectionnez soigneusement les indicateurs clés et les objectifs

Il faut choisir les indicateurs clés avec soin, car la sélection et la communication des indicateurs sont les moteurs de l'organisation. Le choix de ces mesures indique ce qui compte le plus pour les dirigeants et les gens s'y conformeront.

[20] https://www.first.org/global/sigs/metrics/events
[21] https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8276.pdf

Si les indicateurs mesurés sont mal choisis, cela va à l'encontre des objectifs de cybersécurité souhaités et conduit à de fausses hypothèses sur la situation en matière de risques. En outre, le conseil d'administration pourrait vouloir concentrer son attention sur l'amélioration des indicateurs plutôt que sur la position sous-jacente du cyber-risque.

Les indicateurs clés doivent évoluer dans le temps en fonction de la maturité croissante de l'organisation, des modifications des exigences réglementaires, des objectifs commerciaux et des changements dans les menaces. Pour les indicateurs sélectionnés, des objectifs doivent être fixés et acceptés par l'ensemble de l'organisation. Ils doivent avoir un sens en termes d'atténuation des risques et d'appétit pour le risque. Ils peuvent inclure une composante temporelle au cas où l'organisation souhaite inclure une évolution de la maturité dans le temps.

Processus d'escalade

Il est recommandé de définir un processus/seuil qui déclenche le signalement d'urgence des écarts/développements au niveau exécutif entre les périodes de reporting. Évidemment, on peut penser à des incidents/violations critiques, mais le déclencheur peut également provenir de vulnérabilités importantes ou de développements dans le paysage des menaces nécessitant une attention immédiate de la part du niveau exécutif. Un exemple récent d'un tel cas est la vulnérabilité de Log4j et les dépendances de nombreuses organisations à l'égard de produits utilisant ce composant logiciel.

Un processus de passage au palier d'intervention supérieur pourrait également être conçu pour les indicateurs qui ne sont communiqués au conseil d'administration qu'en cas de dépassement d'un seuil prédéfini. Une telle approche pourrait réduire la surcharge d'informations non pertinentes transmises au conseil d'administration.

Les sources de données - une vérité indéniable

Données collectées en interne

Les systèmes de mesure techniques doivent être composés de données collectées automatiquement à partir de l'infrastructure source, avec une implication humaine minimale. Il s'agit notamment de :

- systèmes de gestion et de découverte des actifs (exhaustivité, criticité);
- systèmes et consoles de gestion des outils (déploiement);
- logs et SIEMs (déploiement et exploitation);
- analyse des logiciels (versions, vulnérabilités, configurations, politiques);
- gestion des identités, des privilèges et des accès (contrôles et politiques);
- traces réseau (exhaustivité, contrôles).

La plupart de ces données concernent le déploiement de contrôles, d'outils et de politiques. Quant à l'efficacité de l'atténuation des risques, elle peut être dérivée de manière théorique sur la base de l'atténuation attendue d'un contrôle spécifique.

Données recueillies lors des essais

Des informations supplémentaires sur la mise en œuvre (déploiement et fonctionnement), en particulier sur son efficacité, peuvent être obtenues en testant les contrôles. En règle générale, ces tests peuvent être effectués à l'aide de tests d'intrusion manuels ou d'équipes rouges (red team), ou par des tests automatisés à l'aide d'outils spécifiques ou de programmes de primes aux bogues (bug bounty). Cette catégorie de mesures sera particulièrement utile dans une organisation qui a déjà mis en place un système de gestion de la sécurité de l'information mature[22].

Données collectées en dehors de l'infrastructure

Certaines données sur les infections et les vulnérabilités confirmées peuvent être collectées à l'extérieur de l'infrastructure d'une organisation en scannant ou en observant les traces réseau qui indiquent la présence d'une infrastructure malveillante connue.

Transformation - Nos contrôles sont-ils suffisants ?

Si les indicateurs clés opérationnels sont importants pour le RSSI/CISO afin de piloter la mise en œuvre de la stratégie de cybersécurité et d'appliquer une surveillance granulaire des contrôles au sein du conseil d'administration, ils ne sont pas appropriés pour être communiqués à la direction générale, au conseil d'administration et aux autres parties prenantes stratégiques. Ils seraient perçus comme trop nombreux, énigmatiques et déconnectés du risque commercial.

Pour que les mesures du cyber-risque trouvent un écho au niveau du conseil d'administration, elles doivent être transformées en reporting d'entreprise significatif (coût, sécurité, valeur de la marque, etc.) et comparées à l'appétit pour le risque. Nos mesures d'atténuation des risques sont-elles suffisantes ? Pouvons-nous fournir une assurance raisonnable ? Le conseil d'administration peut-il valider nos hypothèses et nos orientations ? Dans la figure suivante, nous montrons le flux d'informations allant des mesures techniques/opérationnelles aux mesures présentées au conseil d'administration.

[22] https://www.iso.org/isoiec-27001-information-security.html

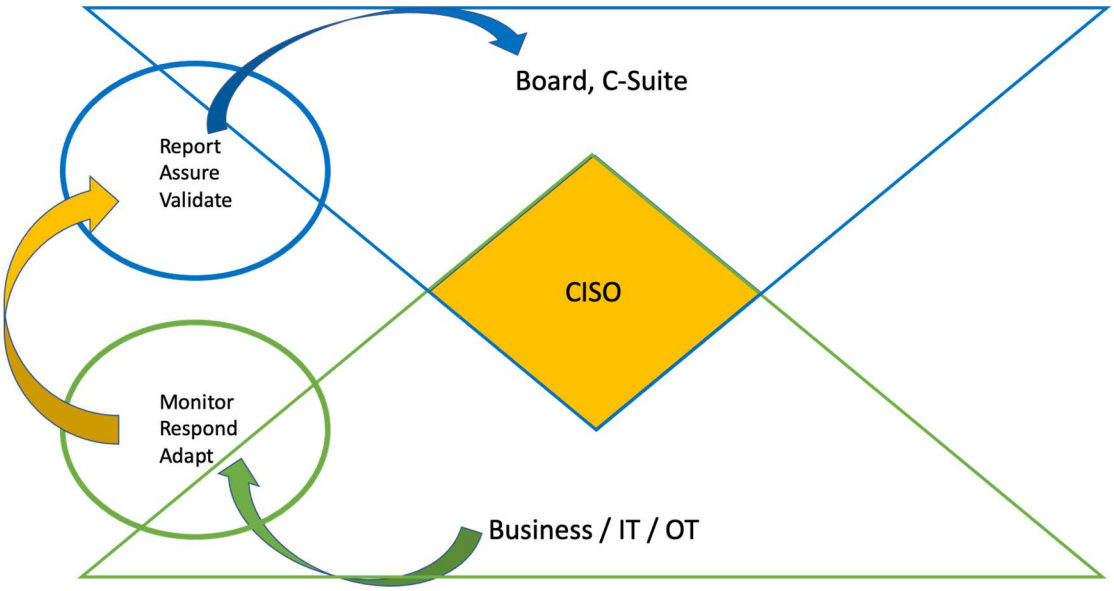


Figure 11 Transformation des métriques techniques en métriques stratégiques

Là encore, nous distinguons un certain nombre de blocs dans l'étape de transformation. Ceux-ci convertissent les indicateurs clés opérationnels en valeurs qui peuvent être comparées au risque tolérable, être intégrées au risque d'entreprise et faire l'objet d'un reporting au conseil d'administration.

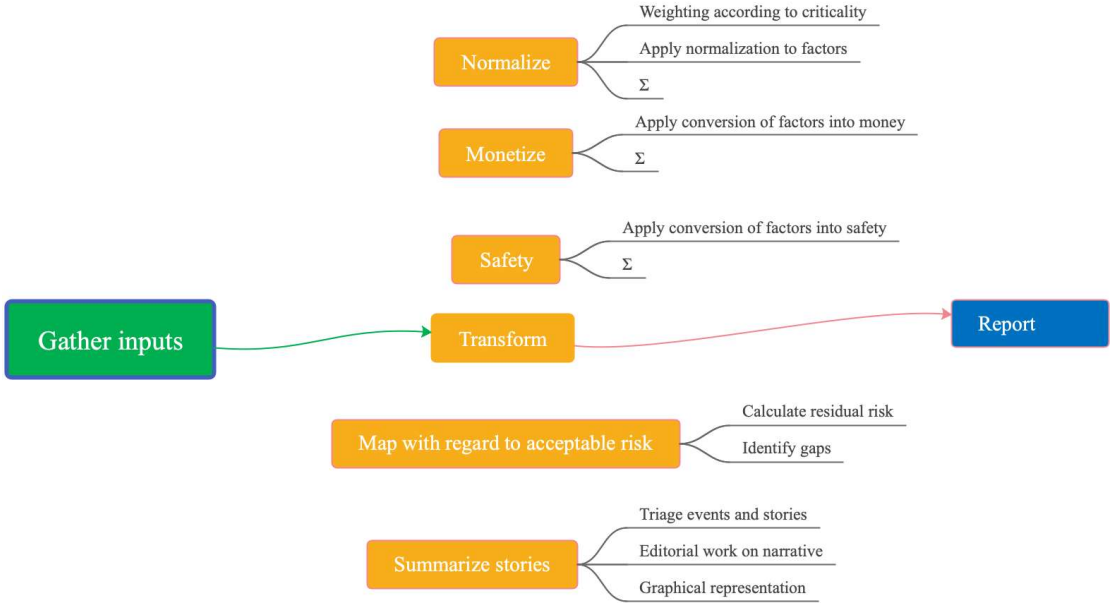


Figure 12 Transformer - blocs de construction

Normaliser

Dans toute organisation, il peut y avoir un grand nombre de mesures pour décrire l'état des contrôles et les performances de l'organisation. Cela peut avoir un effet négatif lorsque les parties prenantes sont submergées par les détails. Un autre problème est que la valeur d'une mesure seule peut être insignifiante lorsqu'elle est considérée indépendamment, mais devient critique lorsqu'elle est considérée dans un ensemble de mesures.

Par exemple, si vous voulez comprendre la santé de vos points d'accès contre les logiciels malveillants, la visualisation du déploiement d'un logiciel antivirus

sur un système d'exploitation donné ne suffira pas. Vous devrez examiner les différentes mesures sur les différents systèmes d'exploitation. De plus, un logiciel antivirus seul ne fournira pas la réponse. Vous devrez consulter les mesures d'autres outils tels que la réponse à la détection d'événements (EDR).

Pour surmonter ce défi, des ensembles de mesures, même s'ils sont de nature différente, peuvent être normalisés ou harmonisés pour fournir une vue plus globale. Une telle normalisation devrait fournir un aperçu simplifié d'un grand nombre de domaines de contrôle distincts tout en révélant des lacunes importantes qui pourraient être masquées par la consolidation.

La normalisation pourrait également inclure une composante de pondération pour prendre en compte les différents niveaux de criticité des actifs. Par exemple, la couverture des contrôles dans les actifs hautement critiques pourrait être évaluée comme plus importante que dans les autres actifs. Dans un système de mesure consolidé, cette distinction pourrait être prise en compte par une pondération.

En utilisant une normalisation d'échelle min/max à trois niveaux (rouge/orange/vert), il est possible de cartographier le système de mesure selon une nouvelle échelle, tout en conservant la proportion exacte au sein de chaque niveau (c'est-à-dire qu'une mesure d'entrée qui se trouve à l'extrémité supérieure du rouge restera à l'extrémité supérieure du rouge même si sa valeur numérique change).

Dans ce graphique, plusieurs mesures de bas niveau sont normalisées selon une échelle commune. Une fois normalisées selon une échelle commune, ces mesures peuvent être agrégées ou combinées de manière significative et ces agrégations peuvent être mises en cascade pour obtenir quelques mesures résumées de haut niveau.

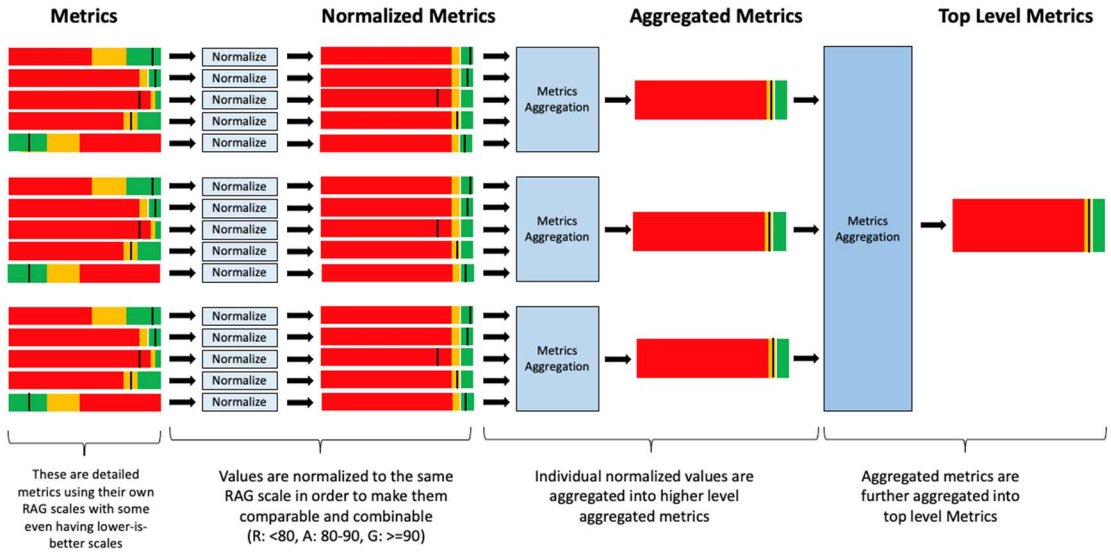


Figure 13 Normalisation de l'échelle min/max à trois niveaux (rouge/orange/vert)

Estimer financièrement (valeur à risque)

Dans les entreprises, l'appétit pour le risque d'entreprise est exprimé en termes financiers. Puisque c'est le cas, il est nécessaire d'essayer de traduire les

résultats des mesures afin de les rendre compréhensibles par les principales parties prenantes afin de pouvoir travailler dans le cadre des processus d'entreprise habituels. Cette manière de procéder a un impact particulier quand il s'agit de demander un financement. Par exemple, si la cybersécurité a besoin de 10 millions de dollars pour déployer un nouveau système EDR, le fait d'identifier qu'il réduira le risque actuel de l'organisation de 12 millions de dollars et replacera l'entreprise dans les limites de son appétit pour le risque est une justification solide.

Cette étape convertit les mesures opérationnelles clés individuelles ou agrégées en valeur du risque géré. En termes de valeur, nous devons prendre en compte l'impact direct de l'incident sur l'entreprise (continuité des opérations, litige par les clients, pénalités de conformité, coût de la réponse à l'incident, paiements liés à des rançongiciels) ainsi que l'impact indirect (atteinte à l'image de marque, cours des actions).

L'une des méthodes d'évaluation financière est l'analyse factorielle du risque informationnel (FAIR™)[23] , un modèle permettant de comprendre, d'analyser et de quantifier le cyber-risque et le risque opérationnel en termes financiers. Cette méthode est bien établie et largement diffusée. Cependant, elle peut être trop élaborée et difficile à maintenir pour les organisations plus petites ou moins matures.

Le calculateur PHOSI (Potential Harm of Security Incident) de l'opérateur de télécommunications néerlandais KPN est une alternative à faible coût, disponible sous forme d'application sur les smartphones[24][25] . Elle facilite le calcul de la valeur à risque à partir d'une petite série de questions. Ces estimations PHOSI peuvent être combinées avec des menaces/contrôles individuels ou également avec les résultats du Red Teaming (quel dommage potentiel a été évité en appliquant à temps un correctif à une vulnérabilité critique ou en effectuant un exercice Red Team ?) ou l'exposition à des vulnérabilités importantes.

Une façon plus large et plus simple d'évaluer financièrement les principales mesures opérationnelles consiste à utiliser le résultat de la normalisation/consolidation comme facteur d'atténuation à multiplier par la fréquence et l'impact moyens d'un cyberincident observé dans la communauté. Les travaux de recherche sur la fréquence et l'impact des rançongiciels ont donné des exemples intéressants pour de telles approximations[26] . On peut également trouver des travaux universitaires récents dans ce domaine dans "A System to Calculate Cyber-Value-at-Risk"[27] .

Il est important de noter qu'il s'agit d'un domaine de recherche actif et que les méthodes de quantification du risque sont imparfaites. Bien qu'il s'agisse d'un objectif à atteindre et qu'il soit essentiel pour communiquer avec les principales parties prenantes, les résultats doivent être traités avec prudence.

[23] https://www.fairinstitute.org/what-is-fair
[24] https://apps.apple.com/us/app/kpn-RSSI/CISO/id1122223795
[25] https://play.google.com/store/apps/details?id=com.kpn.ksp&hl=en&gl=US
[26] https://www.youtube.com/watch?v=kSi-oXq4xV0
[27] https://www.sciencedirect.com/science/article/pii/S0167404821003692

Impact sur la sécurité (vies en danger)

Certaines organisations sont, de par leur activité, non seulement concernées par l'impact financier mais aussi par l'impact sur la sécurité. C'est le cas des compagnies aériennes/de la gestion du trafic aérien, des constructeurs automobiles, des hôpitaux, des fournisseurs d'énergie nucléaire, etc.

Les cyber-risques susceptibles d'entraîner des pertes de vies humaines mériteraient d'être estimés et l'efficacité des contrôles et de l'atténuation des risques mesurée et contrôlée. Beaucoup moins de travaux ont été publiés dans ce domaine, mais le principe sous-jacent serait similaire au calcul de la valeur à risque.

Il s'agit certainement d'un domaine dans lequel les organisations se sentiraient moins à l'aise pour partager des évaluations ou exposer des compromis et des risques calculés. Une perception externe de l'acceptation des risques de perte de vie par une organisation pourrait très rapidement conduire à une atteinte à l'image de marque.

L'estimation financière de la perte de vie n'étant pas acceptable (du moins dans certaines régions du monde), la notion de risque acceptable de perte de vie est évaluée par un mélange de moyens quantitatifs et qualitatifs pour calculer le risque, dans le but de parvenir à une absence de perte dans la mesure où cela est raisonnablement possible et toléré par la réglementation.

Cartographie pour la détermination de l'appétit pour le risque

Le résultat des évaluations de la valeur et de la vie en danger doit être comparé à la propension au risque de l'organisation. Dans de nombreuses organisations, cette appétence pour le risque a déjà été établie dans le cadre des processus de risque de l'entreprise. Si ce n'était pas le cas, le RSSI/CISO devrait inciter l'entreprise/le conseil d'administration à déterminer l'appétit pour le risque :

- Combien sommes-nous prêts à perdre au cas où le risque se matérialiserait ?
- Dans quelle mesure voulons-nous que le risque soit atténué ?
- Combien de ressources sommes-nous prêts à mettre à disposition pour l'atténuation ?
- Assurons-nous une partie du risque ?

Certains diront probablement qu'il n'est pas possible d'évaluer la probabilité d'une violation. Cependant, nous devons nous rappeler qu'en l'absence d'un indice de référence pour l'appétit pour le risque, aucune quantification de la probabilité ne se fera. Nous préconisons d'entamer une discussion sur la tolérance au risque, par exemple "moins de 5 % de chances par an qu'une perte due à une cyber-violation dépasse 1 million de dollars". Tout en reconnaissant que ce type d'approche quantitative du cyber-risque est difficile à réaliser et constitue l'exception plutôt que la norme, l'objectif est ambitieux à la fois pour qu'une quantification du risque ait lieu, mais aussi pour permettre que les budgets soient raisonnables.

Commencez par vous tromper sur ces chiffres, et laissez les cadres s'efforcer de répondre à la question selon une méthodologie reproductible. Si vous n'avez aucune idée des chiffres à utiliser, prenez comme point de départ certains des

autres risques au sein de votre organisation, tels que les tolérances au risque d'incendie, d'inondation ou d'accident du travail. Ces risques sont sans aucun doute très différents, mais ils peuvent vous servir d'indication sur la façon d'exprimer la tolérance au risque que vous espérez atteindre. Vous découvrirez peut-être au final que le risque de votre organisation s'approche en réalité des 10 %, mais la discussion sur le coût de la réduction de ces risques devient alors plus facile et rationnelle.

La mise en correspondance de la valeur/du risque de perte de vies avec l'appétit pour le risque est nécessairement une analyse multidimensionnelle dans laquelle la fréquence attendue et l'impact possible sont combinés et dans laquelle la situation actuelle pourrait être exprimée en un certain nombre de points de données basés sur des hypothèses concernant l'efficacité des contrôles.

La cartographie peut également être utilisée pour montrer les voies d'amélioration liées aux contrôles/investissements proposés. Cependant, rien de tout cela n'est susceptible de se produire si le conseil d'administration ne fixe pas d'emblée une tolérance au risque. Ce n'est qu'alors que l'on pourra discuter du réalisme des chiffres et des attentes en matière de résilience au cyber-risque.

Faire la synthèse de situations vécues

Sélectionner des situations vécues pertinentes (incidents à l'intérieur et à l'extérieur de l'organisation, renseignements sur les cybermenaces, évolutions réglementaires) et en extraire l'essentiel (pourquoi est-ce pertinent ?) constitue un complément indispensable aux mesures quantitatives.

Le RSSI/CISO et son équipe doivent posséder des compétences spécifiques pour synthétiser les narratifs et les présenter de manière convaincante. Les histoires sélectionnées doivent fournir un contexte supplémentaire à la posture de risque de l'organisation et servir un objectif. Sinon, elles risquent de détourner l'attention et de capter une énergie et des ressources qui pourraient être mieux utilisées ailleurs.

Signaler les cyber-risques - fournir une assurance raisonnable

Le reporting sur la cybersécurité à l'intention du conseil d'administration devrait permettre de (r)assurer ce dernier sur le fait que le cyber-risque reste dans les limites de l'appétit pour le risque aujourd'hui et demain :

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

Sachant que le conseil d'administration et ses comités ne sont pas spécialisés dans la cybersécurité, il serait judicieux d'aider le conseil à poser les bonnes questions et de ne pas le submerger d'informations. Pour donner une comparaison visuelle, l'image suivante montre un cockpit "RSSI/CISO" avec des instruments opérationnels et des consoles qui permettent aux pilotes d'interagir

avec l'avion pour amener les passagers à destination en toute sécurité et dans les délais.

Figure 14 Crédit Aeropers / Pilotes de Swiss airlines

L'image suivante montre un cockpit "conseil d'administration" avec différents instruments et sans possibilité de contrôle, qui dépend entièrement du contrôle au sol.

Figure 15 Crédit NASA/SpaceX

Le conseil d'administration attend du RSSI/CISO qu'il signale toute évolution susceptible de modifier sensiblement la situation, en bien ou en mal, et qu'il propose en conséquence des actions et des ressources appropriées.

La mise en place d'un ensemble de mesures de cybersécurité et la communication cohérente de leur contexte au conseil d'administration, à ses membres individuels et à ses comités compétents (audit, conformité) peuvent constituer un moyen efficace et fiable de fournir une cyberassurance.

Il peut être combiné/aligné avec le reporting sur d'autres types de risques d'entreprise ainsi que le reporting sur la stratégie de transformation numérique.

Système de mesure et narratif

Le vieil adage "une image vaut mille mots" est également vrai lorsqu'il s'agit de l'engagement de votre conseil d'administration dans le domaine de la cybersécurité. Une grande diversité de représentations graphiques des mesures de cybersécurité est utilisée dans la communauté et l'examen de ces exemples et l'interaction avec les pairs du secteur peuvent être très inspirants pour la conception du système de reporting d'une organisation. Dans la Figure 16, nous avons inclus quelques éléments de base, fondés sur des exemples de la communauté, qui figurent dans les annexes.

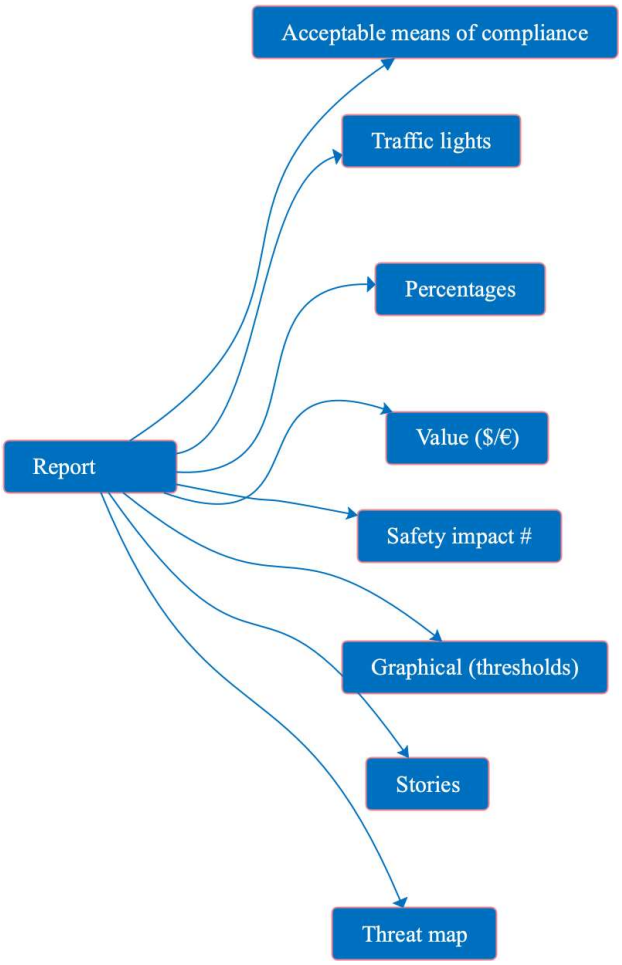


Figure 16 Reporting - éléments constitutifs

Canal(aux) de communication

L'idéal serait qu'une organisation établisse un canal de communication cohérent et intégré pour recueillir les données, les traduire, puis les communiquer au conseil d'administration. Les flux de communication dans la Figure 17 seraient mis en œuvre comme prévu. Pour ce faire, différentes fonctions doivent coopérer et s'aligner sur le cadre, sur les processus permettant d'effectuer les mesures, ainsi que sur les rôles et responsabilités en matière de reporting.

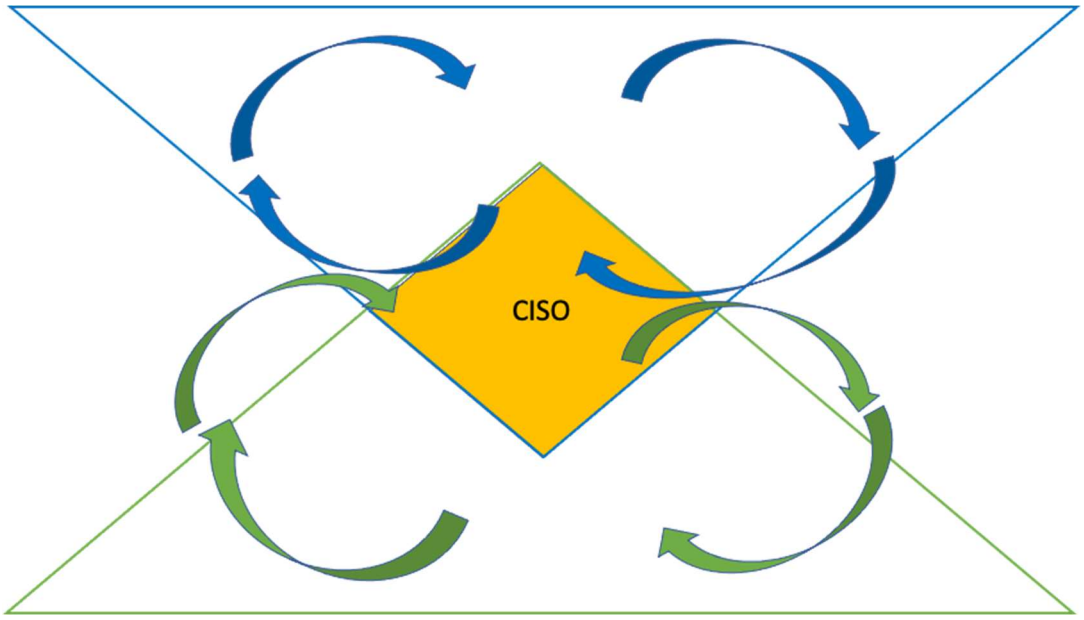


Figure 17 Flux de communication optimal

Indépendamment de l'intervenant qui rend effectivement compte au conseil d'administration, le RSSI/CISO doit jouer un rôle clé dans le processus, en garantissant une vision professionnelle et indépendante du cyber-risque. Dans le meilleur des cas, ce serait le RSSI/CISO qui rendrait compte au conseil d'administration en personne, ce qui permettrait une interaction et personnifierait l'assurance.

Il convient d'éviter ou de supprimer des situations alternatives, comme illustré dans la Figure 18, dans lesquelles, dans le premier diagramme, aucune information n'est fournie au conseil d'administration, dans le diagramme du milieu, les informations qui lui sont fournies ne sont pas fondées sur la réalité, ou dans le troisième diagramme, des informations contradictoires lui sont communiquées par différents canaux.

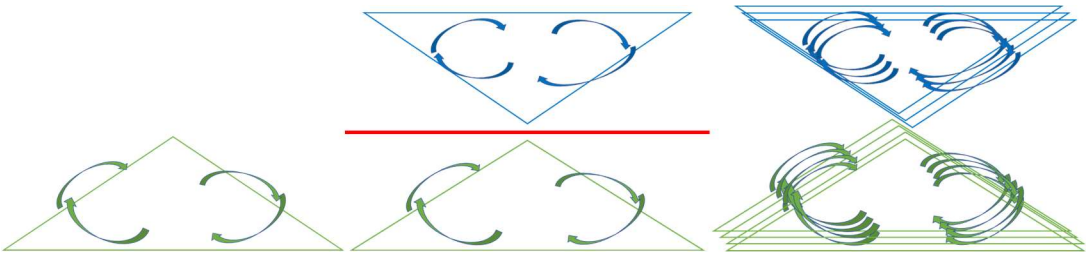


Figure 18 Flux de communication parallèles, inexistants et non connectés.

Vaincre la résistance

Si les concepts décrits dans le présent document sont, dans une certaine mesure, déjà utilisés par les services de cybersécurité, ils constituent également une base pour intégrer les risques de cybersécurité dans le cadre des processus de gestion des risques d'entreprise. Cependant, ces interactions sont encore difficiles dans de nombreuses organisations où :

- la cybersécurité et le risque sont gérés par différents départements/sont cloisonnés ;

- la cybersécurité est considérée par les services d'entreprise comme une discipline réservée aux initiés, de la "magie noire" ;
- les modèles de gestion des risques sont considérés comme complexes et abstraits par les services de cybersécurité ;
- le vocabulaire et les mesures de cybersécurité ne sont pas traduits en termes d'entreprise.

Faire de la cybersécurité une question récurrente à l'ordre du jour du conseil d'administration demande des efforts et de la persuasion, mais cela peut être facilité par un certain nombre d'initiatives proactives :

- comprendre les attentes du conseil d'administration et de ses membres individuels et s'adapter à l'évolution de ces attentes ;
- organiser des séances de sensibilisation avec le conseil d'administration, expliquant les menaces et les risques d'une manière compréhensible ;
- mener des exercices de réponse aux incidents en y associant le conseil d'administration ;
- adresser au conseil d'administration des cyber-bulletins mensuels avec des situations vécues pertinentes et leur contexte;
- organiser des séances d'information bilatérales avec des membres individuels du conseil d'administration ayant manifesté leur intérêt ;
- commencer progressivement et améliorer le système au fil du temps (par exemple, commencer par la mise en œuvre d'une approche basée sur un modèle de maturité avant de mettre en œuvre un modèle quantitatif complet) ;
- mettre en place une coopération transparente et positive avec le comité d'audit.

Affecter des ressources aux mesures et au reporting

Il ne fait aucun doute que la mise en œuvre et le maintien d'un système de mesure et de reporting tel que décrit dans ce document nécessitent que des ressources leur soient spécifiquement consacrées. Cependant, ce système permet également d'économiser des ressources grâce à l'alignement/la rationalisation interne, en évitant les réponses réactives inutiles aux médias et, en fin de compte, en concentrant les ressources sur ce qui compte vraiment, à savoir réduire le cyber-risque à un niveau acceptable, en évitant les réponses aux incidents et les répercussions négatives.

Annexe 1 : Par où commencer ?

Questions à poser au conseil d'administration

- Disposons-nous d'un inventaire des principaux actifs ?
- Qui nous cible (principaux adversaires) 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 situons-nous par rapport à nos pairs ?

Contrôles essentiels de base

Vous trouverez ci-dessous une sélection (non exhaustive) de recommandations de base :

- Les sept principales mesures de sécurité (Cybersecurity Centre Belgium)[28]
- Les dix premiers (Centre national de cybersécurité du Royaume-Uni)[29]
- Essential eight (Centre australien de cybersécurité)[30]
- Les 42 principales mesures pour un réseau sain (FR ANSSI)[31]
- Les huit principales mesures de sécurité (NL National Cyber Security Centre)[32]

Ces autorités sont également une source d'informations actualisées sur le paysage des menaces et la nature évolutive des vulnérabilités et des techniques hostiles.

[28] https://cyberguide.ccb.belgium.be/en/take-security-measures-0
[29] https://www.ncsc.gov.uk/files/2021-10-steps-to-cyber-security-infographic.pdf
[30] https://www.cyber.gov.au/acsc/view-all-content/essential-eight
[31] https://www.ssi.gouv.fr/en/guide/40-essential-measures-for-a-healthy-network/
[32] https://www.ncsc.nl/onderwerpen/basismaatregelen

Annexe 2 : Exemples de la communauté

Collecte d'informations

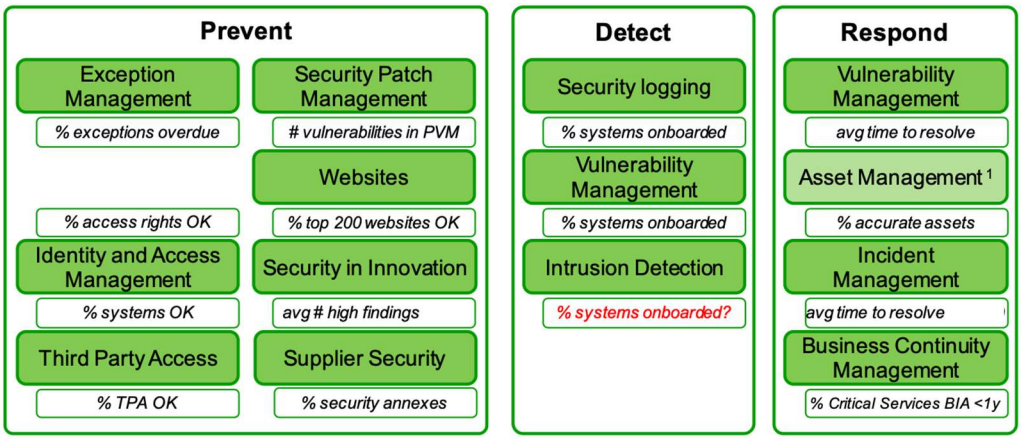


Figure 19 Exemple de systèmes de mesure centrés sur les événements

Incident Timeline	Applicability Level	Description
Time of First Activity	Recommended for significant incidents	This is the earliest event in a confirmed or potential chain of events, that caused the incident.
Time of Detection	All incidents	The time that a control (e.g. telemetry, technology) or another detection mechanism (e.g. a human) recognizes that something has occurred.
Time of Containment	All incidents that require Containment	Time of Containment is the point in time at which the incident can no longer spread nor do damage.
Time of Remediation	All incidents that require Remediation	Time of Remediation is the point in time at which an affected target asset is returned to its pre-incident state or removed from the environment permanently.

Figure 20 Systèmes recommandés de mesure du temps. Source : FIRST Metrics SIG.

Function	Category	Subcategory	Subcategory Risk	Sub Cat Score	Subcategory Composite Risk Score
	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	Critical	6	30
		ID.AM-2: Software platforms and applications within the organization are inventoried	Weighted Medium	4	
		ID.AM-3: Organizational communication and data flows are mapped	Weighted Medium	4	
		ID.AM-4: External information systems are catalogued	Critical	6	
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	Critical	6	
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	Weighted Medium	4	
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	Weighted Low	2	
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	Low	1	
		ID.BE-3: Priorities for organizational mission, objectives			

Figure 21 Un exemple de mise en œuvre des systèmes de mesure liés au NIST CSF

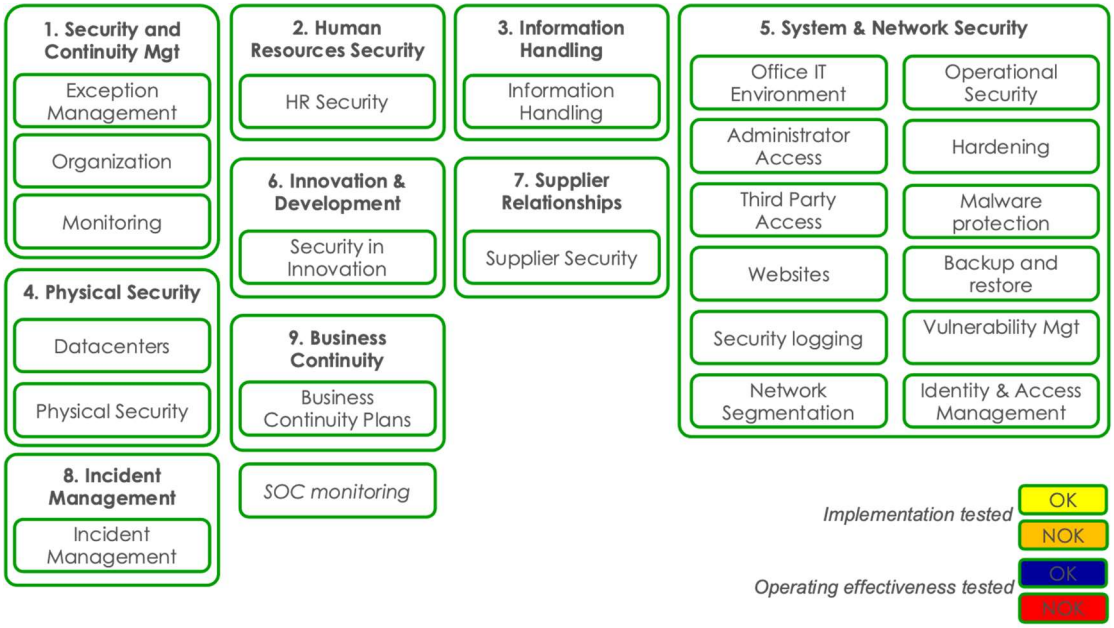


Figure 22 Exemple de systèmes de mesure issus des tests

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
Spearphishing Attachment	Command-Line Interface	Registry Run Keys / Startup Folder	Scheduled Task	Obfuscated Files or Information	Credential Dumping	System Network Configuration Discovery	Remote Desktop Protocol	Input Capture	Remote File Copy	Data Compressed	Data Encrypted for Impact
Valid Accounts	Scripting	Scheduled Task	Valid Accounts	Scripting	Input Capture	Process Discovery	Remote File Copy	Data from Local System	Commonly Used Port	Data Encrypted	Disk Structure Wipe
Drive-by Compromise	PowerShell	Valid Accounts	Process Injection	Valid Accounts	Brute Force	Account Discovery	Pass the Ticket	Data Staged	Standard Application Layer Protocol	Data Transfer Size Limits	Resource Hijacking
External Remote Services	Scheduled Task	New Service	New Service	Code Signing	Credentials in Files	File and Directory Discovery	Remote Services	Email Collection	Connection Proxy	Exfiltration Over Command and Control Channel	System Shutdown/Reboot
Spearphishing Link	Exploitation for Client Execution	External Remote Services	Accessibility Features	Deobfuscate/Decode Files or Information	Credentials from Web Browsers	Network Service Scanning	Windows Admin Shares	Audio Capture	Web Service	Exfiltration Over Alternative Protocol	
Exploit Public-Facing Application	User Execution	Create Account	Bypass User Account Control	File Deletion	Network Sniffing	Remote System Discovery	Windows Remote Management	Automated Collection	Custom Command and Control Protocol		
Supply Chain Compromise	Windows Management Instrumentation	Redundant Access	Web Shell	Masquerading	Account Manipulation	System Information Discovery	Component Object Model and Distributed COM	Data from Information Repositories	Multi-Stage Channels		
Trusted Relationship	Dynamic Data Exchange	Web Shell	Exploitation for Privilege Escalation	Process Injection		System Network Connections Discovery	Exploitation of Remote Services	Video Capture	Standard Non-Application Layer Protocol		
	Rundll32	Accessibility Features	DLL Search Order Hijacking	Connection Proxy		System Owner/User Discovery	Pass the Hash	Screen Capture	Uncommonly Used Port		
	Service Execution	Bootkit	Application Shimming	Redundant Access		Network Share Discovery		Data from Network Shared Drive	Fallback Channels		
	Graphical User Interface	Component Firmware		Rundll32		Permission Groups Discovery			Multi-hop Proxy		
	Mshta	BITS Jobs		Software Packing		Security Software Discovery			Data Obfuscation		
	Regsvr32	Modify Existing Service		Web Service		System Service Discovery			Domain Fronting		
	Execution through API	DLL Search Order Hijacking		Bypass User Account Control		Virtualization/Sandbox Evasion			Data Encoding		
	Component Object Model and Distributed COM	Shortcut Modification		DLL Side-Loading		Query Registry			Domain Generation Algorithms		
	Windows Remote Management	Windows Management Instrumentation Event Subscription		DLL Search Order Hijacking		Network Sniffing			Standard Cryptographic Protocol		
	CMSTP	Winlogon Helper DLL		Hidden Files and Directories		Peripheral Device Discovery					
	Compiled HTML File	Account Manipulation		Hidden Window							
		Application Shimming		Indicator Removal from Tools							
		Hidden Files and Directories		Indicator Removal on Host							
				Modify Registry							
				Mshta							
				Network Share Connection Removal							
				Process Hollowing							
				Regsvr32							
				Rootkit							
				Template Injection							
				Virtualization/Sandbox Evasion							
				Binary Padding							
				BITS Jobs							
				Disabling Security Tools							
				Execution Guardrails							
				Compiled HTML File							
				Component Firmware							
				CMSTP							
				Clear Command History							
				Compile After Delivery							

Figure 23 Exemple d'utilisation d'une carte thermique pour montrer la couverture des TTPs

Transformer

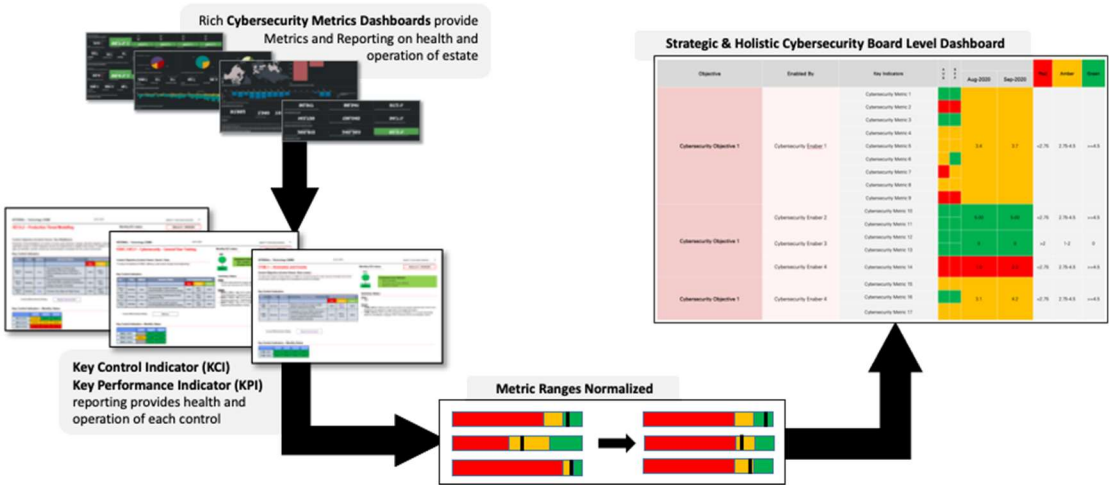


Figure 24 Exemple de normalisation

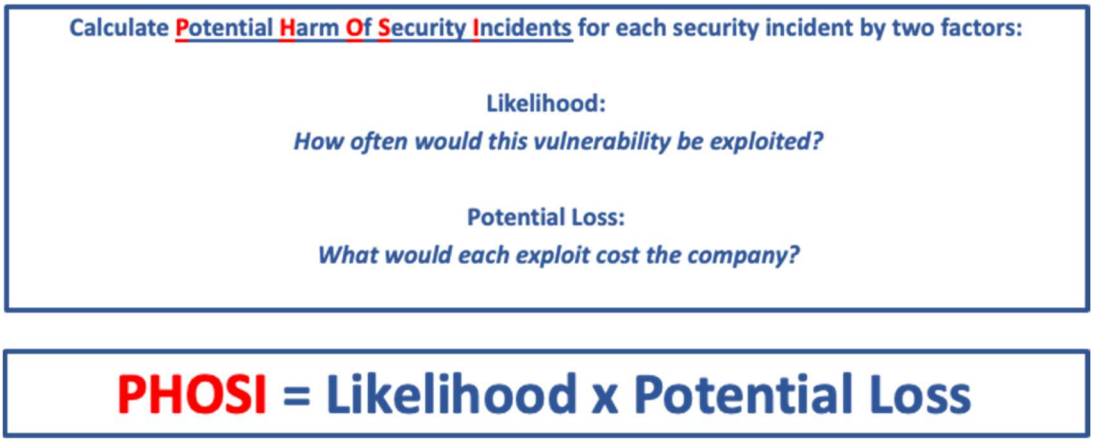


Figure 25 Exemple d'évaluation financière

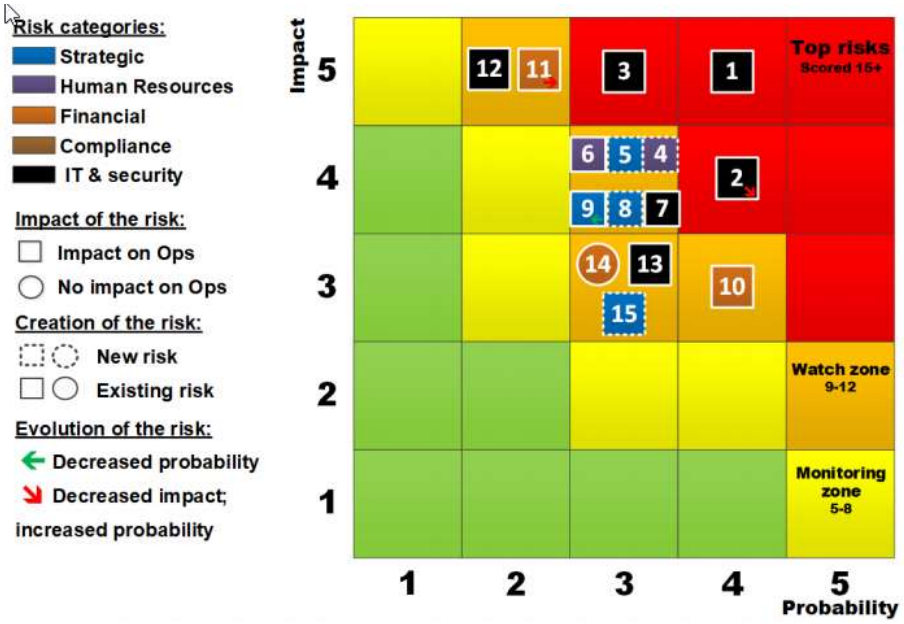
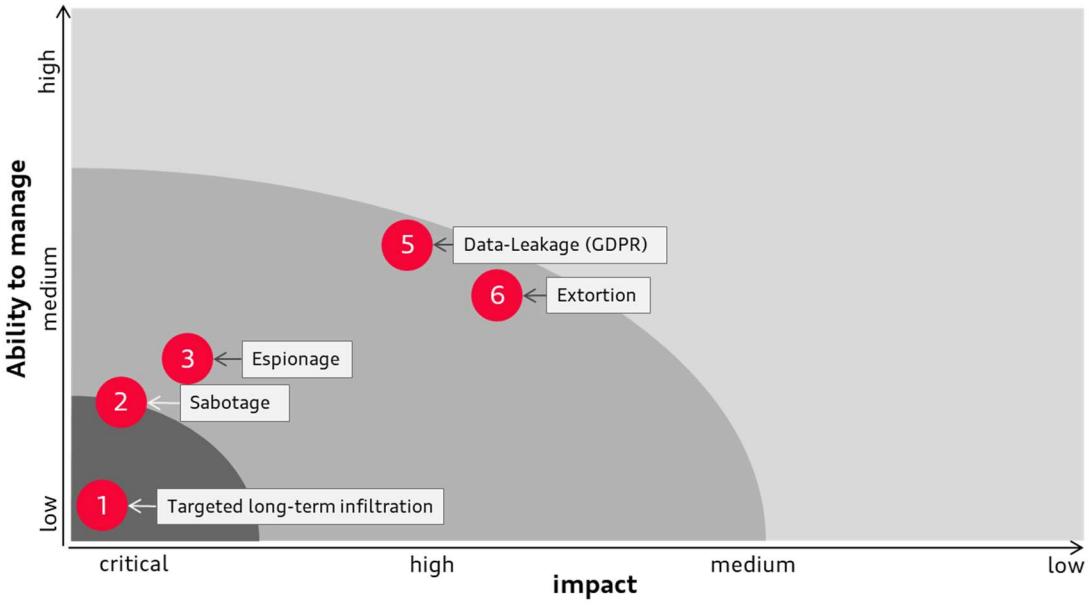


Figure 26 Exemple de cartographie du risque

Signaler un cyber-risque



Manufacturing industry or geographically close

When?	What?	Category	Group
Q1.2021	Hackers exploit IT tool Z to establish persistence	1	Unknown
Q4 2020	Ransomware attack at enterprise X	2 6	Cyber-Crime
Q4 2020	Enterprise Y hit by ransomware, data leaked	2 6	Cyber-Crime

Figure 27 Exemple de reporting sur le paysage des menaces

When	Type	What?	Status	Group
4/2020	3	Spear phishing campaign with malicious Excel attachment.	Closed	APTX

Figure 28 Exemple de rapport d'incident

Group	Motive	Trend
Adversary 1	Adversary known to steal intellectual property in high tech industry.	↗
Adversary 2	Adversary known to steal intellectual property in our sector.	→
Targeted Cyber-Crime	Ransomware actor increasingly prevalent and sophisticated	↑

Figure 29 Exemple de suivi d'un adversaire notable

CERT-EU

TLP:WHITE

Threat Landscape Report 2021 Q3 - Executive Summary

Direct Threats to EU Institutions, Bodies, and Agencies

INCIDENTS

4 significant incidents affected EUIBAs this quarter.

In 3 cases the attack started with a compromise of a publicly accessible server (Oracle WebLogic, Microsoft Exchange).

In the other case, attackers obtained credentials via a phishing campaign.

In at least 3 significant incidents, threat actors successfully exfiltrated data.

Since the beginning of 2021, CERT-EU has already recorded 15 significant incidents, compared to 13 during the whole of 2020 and 8 in 2019.

THREATS

CERT-EU released 26 threat alerts (compared to 20 during Q1 and 22 in Q2).
The top 5 reasons for threat alerts were:

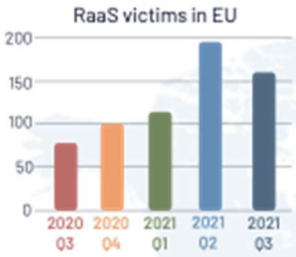
- Active exploitation of zero-days or n-days: Microsoft Exchange, VPNs, etc.
- Recent activity or new tools used by top threat actors
- Sharing actionable data related to TTPs used in significant incidents
- Spear-phishing campaigns directly affecting EUIBAs or sectors of interest
- Active use of commercial mobile spyware

Top threat actors: CERT-EU currently tracks 13 top threat actors. The level of exposure of EUIBAs has been high for 4 of them: two alleged Russian threat actors, one alleged Chinese, and one allegedly of North Korean origin.

Social media: The most frequently used social media network for impersonation of EU staff or the digital identities of EUIBAs has been Instagram, followed very closely by Facebook and at a distance by Twitter.

Malware and tools: The three most observed pieces of malware or malicious tools to which EUIBAs have been exposed were Cobalt Strike, Mimikatz, and Dridex. However, no infections have been confirmed.

Threats in Europe



Ransomware

A supply chain attack conducted by REvil against Kaseya VSA, software used by many MSPs, had a major impact on several organisations including in Europe, causing significant disruptions.

Taking into consideration the first 9 months of 2021, the average number of ransomware victims per month increased by 129% in 2021, compared to last year.

Nation-state activity

The EU has acknowledged and condemned Russian "Ghostwriter" cyberespionage / information operation activity against EU member states. The Russian APT29 threat actor targeted European governments with a zero-day exploit earlier in 2021. The EU, the UK, and the US attributed the Hafnium ProxyLogon attacks to China and are calling for an immediate stop to such adversarial activities. France reported a significant cyberespionage campaign by the Chinese Zirconium (aka APT31) threat actor. The NSO group and its Pegasus spyware have been used in several espionage cases against politicians and journalists.

Hacktivism

Belarussian hacktivists continue hack-and-leak operations against the Minsk regime.

Threats in the World

China: China is establishing full control over all domestic knowledge of software vulnerabilities. As always, China is active on social media, working to amplify pro-Chinese messages.

Russia: Political opposition and anti-corruption entities in Russia fall victim to DDoS attacks and data leaks. Stricter internet controls and censorship established before the September parliamentary election remain in place after the election. Proposed legislation prohibits foreign companies from processing biometric data of Russian citizens.

Iran: Iranian governmental websites were taken offline after a "cyber disruption".

North Korea: A North Korean cyber threat actor compromised a major South Korean major producer of combat ships & submarines.

CERT-EU, CERT for the EU Institutions, Bodies, and Agencies https://cert.europa.eu - services@cert.europa.eu

Figure 30 Exemple de système de mesure et de narration, crédit CERT-EU

Annexe 3 : Exemple de reporting

Évolution 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	Adversary known to steal intellectual property in our sector.	→
Targeted Cyber-Crime	FIN11 (TA505)	Public and corporate IT-infrastructure is a growing market for ransomware	↑

Incidents notables et évolution des menaces

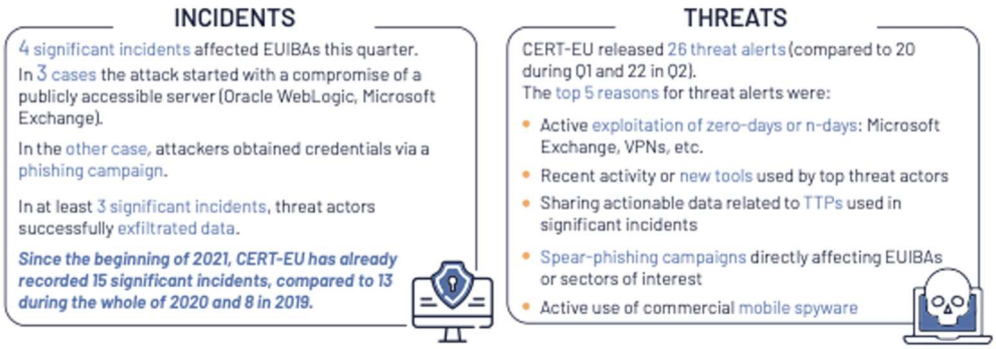
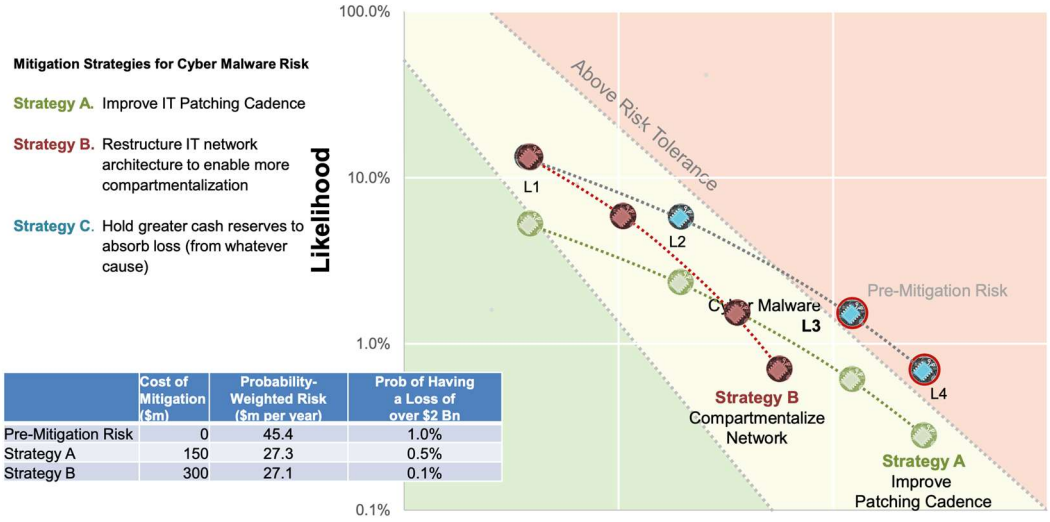


Figure 31 Crédit CERT-EU

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 32 Crédit Center for Risk Studies, Université de Cambridge