Le b.a.- ba de la sécurité de l'information

Un rappel succinct pour ne pas en oublier l'importance.

Par Jérôme Darbellay, Expert sécurité - Itecor Vevey

governance & service management / information security

septembre 2021

Fondamentaux

- Information

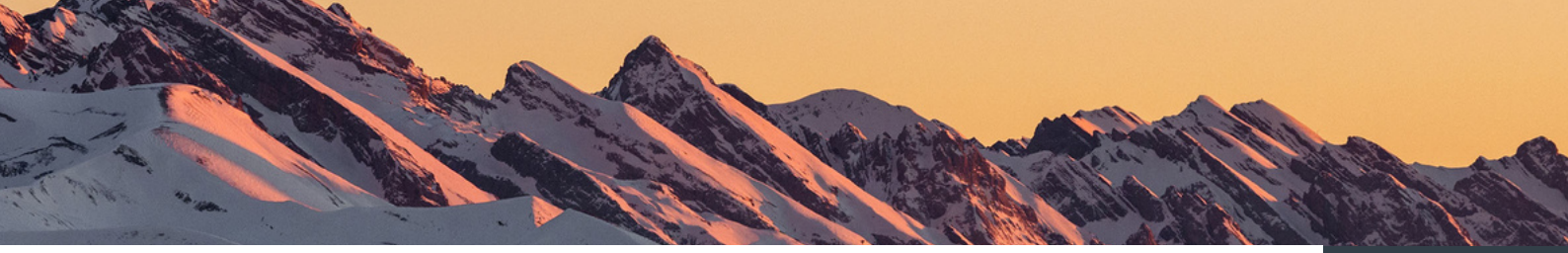
L'Information englobe, dans notre cas, l'ensemble des éléments (des actifs) d'une entreprise qui n'ont pas corps ou qui pourraient techniquement être encodés et transférés par email ou sur disque. C'est large et cela inclut une multitude de données, dont les données personnelles des employés ou des clients, des informations stratégiques, d'autres non nécessairement publiques, telle la participation des investisseurs, et autres…

- Technologie de l'information (IT)

La technologie de l'information est l'ensemble des outils mis en place pour maintenir ces informations, les transférer ou les traiter. Actuellement, il s'agit essentiellement d'outils informatiques. Du temps des Égyptiens, il s'agissait de papyrus. A cette époque, l'informaticien s'appelait scribe. Il était déjà en charge du transfert de l'information sur un outil adapté, de son stockage et de sa restitution.

- Sécurité de l'information

La sécurité de l'information consiste à s'assurer que seules les personnes autorisées aient accès à l'information, que l'information n'ait pas été modifiée et qu'elle puisse être restituée quand c'est nécessaire. Par exemple, la liste des sites possibles pour édifier la prochaine pyramide du pharaon est utile à l'architecte. Lorsqu'on demande au gardien de ne pas parler de la liste, il s'agit de sécurité de l'information au sens large.



- Sécurité des technologies de l'information (ITS)

Lorsqu'on demande au scribe de laisser le papyrus contenant la liste dans un coffre, il s'agit de la sécurité des technologies de l'information. Aujourd'hui, la majeure partie de la sécurité de l'information s'occupe des technologies de l'information. La sécurité de l'information non-technique est essentiellement humaine : ne pas parler de ceci ou cela, présenter son casier judiciaire…

L'évolution de la sécurité de l'information

Au cours des dernières décades, le métier de la sécurité a élargi son champ d'action. Au début de la digitalisation, il s'agissait essentiellement de s'assurer qu'un intrus ne puisse pas entrer dans le réseau par un firewall. De nos jours, le réseau est devenu poreux : côté serveurs on envoie des données dans le cloud et côté utilisateur, on voyage avec des données sur un mobile.

On n'aborde donc plus la sécurité comme un périmètre. Mais il s'agit de s'assurer des destinataires, de l'intégrité et de la disponibilité des informations de l'entreprise au sens large. Autrement dit, on veut s'assurer que seule une personne autorisée puisse accéder à l'information dès que c'est nécessaire, sans qu'elle n'ait été altérée.

Cela tient en une phrase mais touche à de nombreux aspects du fonctionnement de l'entreprise. Cela pose d'emblée les questions du qui, du quoi et du comment. On y a répondu par différents acronymes anglais, certains de l'ordre de la gouvernance, d'autres plus techniques. Selon les moments, certains termes sont plus sous les projecteurs que d'autres :

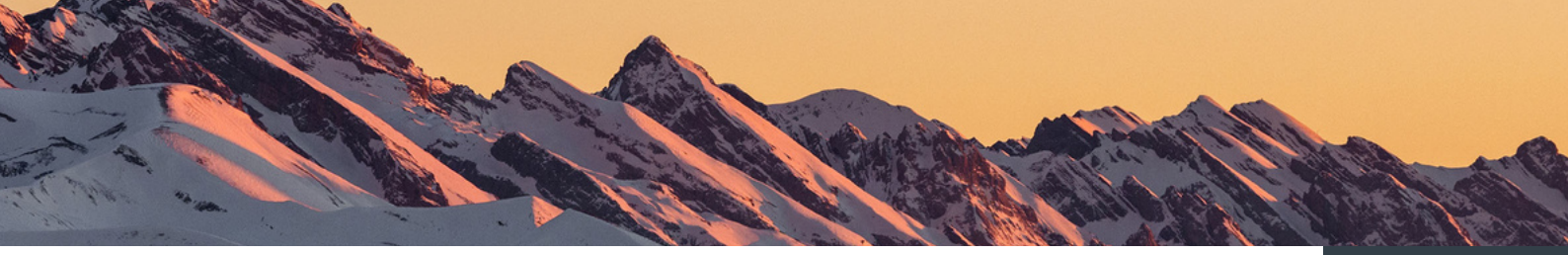
Qui ?

- **Identity & Access Management (IAM)** : gestion centralisée des identités, de leurs attributs, comptes, rôles et droits auprès des différents logiciels de l'entreprise.
- **Identity Federation, SSO** : authentification centralisée des utilisateurs (SSO) avec distribution centralisée de leurs attributs et droits (IDF)
- **Physical Access Control** : droits d'accès physique à différents espaces
- **Protection des données personnelles (LPD, GDPR)** : efforts de préservation des informations personnelles encadrés par des règlementations.

Quoi ?

- **Asset Inventory** : solution d'inventaire central des actifs : données, logiciels, matériel, ressources humaines et infrastructures. Sert de base à la gestion de risque.

“
On n'aborde donc plus la sécurité comme un périmètre. Mais il s'agit de s'assurer des destinataires, de l'intégrité et de la disponibilité des informations de l'entreprise au sens large. Autrement dit, on veut s'assurer que seule une personne autorisée puisse accéder à l'information dès que c'est nécessaire, sans qu'elle n'ait été altérée.
”



Où ? Et sous quelle forme ?

- **Network Security** : Régule les accès dans différents segments d'un réseau.
- **Communications Security** : Encadre le transfert d'information, généralement par des techniques de chiffrement ou de VPN.
- **Cloud Security** : Définit des standards de sécurité pour l'utilisation de solutions du cloud. Dépend fortement du niveau de sécurité proposée par le fournisseur de la solution cloud.
- **Data Security, Cryptography** : sécurité des données stockées ou transportées par des techniques de chiffrement.

Comment ?

- **Development Security** : Régule le développement de logiciels afin qu'il ne serve pas de point d'entrée à des attaquants, et afin qu'il ne soit pas altéré par des attaquants.
- **PKI, Digital Signature, SSL, S/MIME** : Permet l'authentification forte, la signature digitale d'un contenu, ainsi que son chiffrement fort (asymétrique).

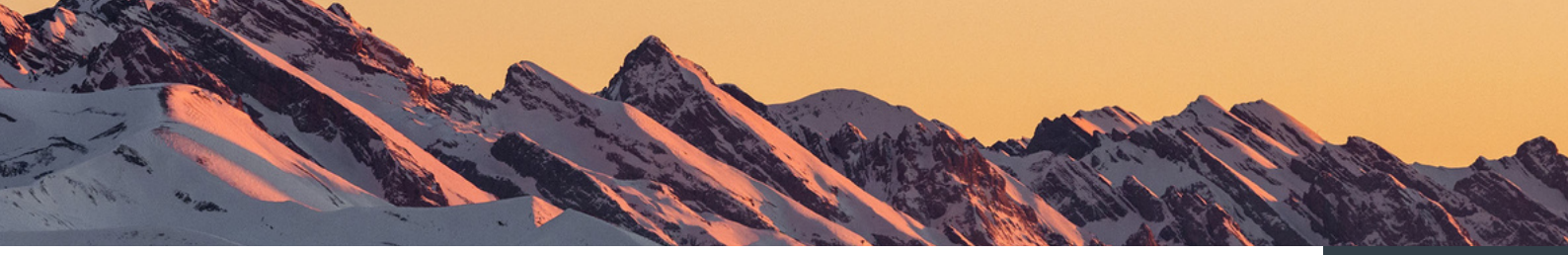
Avec quelle vérification ?

- **Compliance** : vérifie la conformité de solutions, environnements ou opérations à des standards et plans de réduction de risque.
- **Audit** : enquête de vérification des mesures de sécurité effectuée par un tiers
- **Pen testing** : tentatives de pénétration ou corruption d'un système effectuée en prenant le rôle d'un attaquant.

Selon quelle orchestration ?

- **Corporate Governance, Policies & Standards** : documentation réglementant la gestion de l'information.
- **Incident Management :** Identification, analyse et correction d'événement non planifiés.
- **Business continuity planning** : Prévient les interruptions d'activité dues à des menaces et y remédie.
- **Disaster recovery** : Ensemble de régulations, outils et procédures visant à la préservation des éléments critiques de l'entreprise et à leur restauration rapide.
- **Standards ISO 27K** : Suites de standards couvrant la gestion de la sécurité de l'information

govern
GOVERNANCE & SERVICE MGT



La gestion du risque

L'ensemble de la sécurité de l'information obéit à un principe, formalisé par la gestion du risque.

Il ne s'agit pas d'une science en soi, mais d'un processus logique pour aborder l'ensemble des problèmes de sécurité, qu'ils soient techniques ou organisationnels. La raison en est simple : il n'existe pas de sécurité absolue. La seule méthode pour s'assurer que quiconque n'entre jamais dans votre maison serait de la brûler. Si on tient à ce qu'elle reste entière, il faut faire son possible pour que seules les personnes autorisées y rentrent.

La sécurité consiste donc à rendre l'effort nécessaire à la violer trop important au regard du bénéfice que l'on pourrait en retirer. La gestion du risque se demande : de quoi parle-t-on (actif), qui pourrait être intéressé, avec quelle facilité pourrait-on contourner la sécurité (vraisemblance), quel bénéfice pourrait-on tirer, et quelles seraient les conséquences (impact) ?

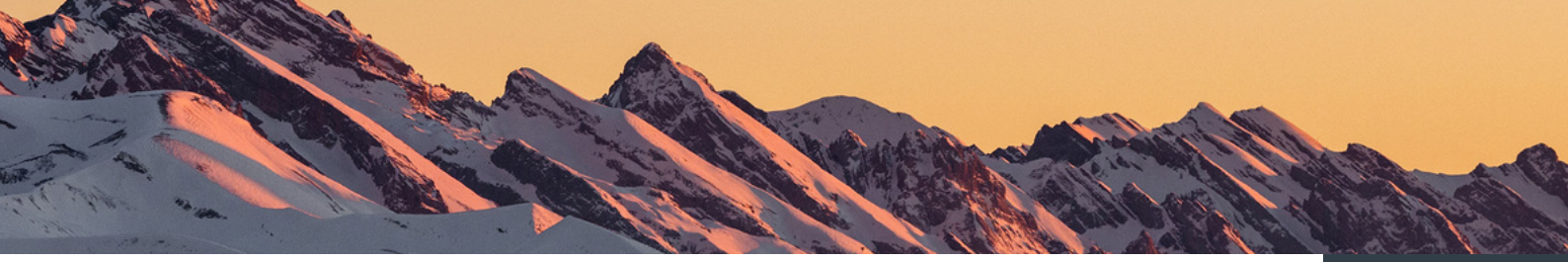
Lors de l'énonciation d'un risque, les réponses sont de quatre types :

- « Oui mais… » aussi appelé le traitement du risque par acceptation. Il s'agit de prendre bonne note et de confirmer que l'on accepte le risque.
- « Il faut regarder avec… » aussi appelé le traitement du risque par transfert. Le transfert d'un risque consiste à laisser une société tierce assumer le risque. Prendre une assurance ou passer sur une solution applicative dans le cloud sont des transferts.
- « Alors on arrête tout ! » aussi appelé le traitement du risque par évitement. Lorsqu'on on considère qu'une solution induit trop de risque au regard des bénéfices qu'elle amène, on peut décider de l'abandonner.
- « On va voir ce qu'on peut faire… » aussi appelé le traitement du risque par mitigation. C'est l'approche la plus intuitive : colmater les brèches. L'employé pense généralement que c'est ce qu'on attend de lui. On peut tenter de mitiger l'occurrence ou l'impact : diminuer la fréquence ou la gravité d'un problème.

Certaines entreprises ont désigné des responsables du risque. Ils se basent sur un inventaire des actifs incluant les données, les applications, le matériel et les infrastructures. Chaque entrée est évaluée selon la méthode de gestion de risque choisie. Ils sollicitent ensuite les équipes pour mettre en place des plans permettant de réduire les risques les plus élevés, appelés contrôles.
D'autres sociétés ont préféré éduquer l'ensemble des employés à la logique du risque et chacun l'applique dans ses évaluations et sa prise de décision.

“
Certaines entreprises ont désigné des responsables du risque.

Ils se basent sur un inventaire des actifs incluant les données, les applications, le matériel et les infrastructures.
”



Comment appréhender la sécurité de l'information : la pyramide des processus et actifs

Imaginons une PME du tertiaire. Elle fournit, par exemple, des cours d'anglais.

Une entreprise du tertiaire peut être considérée comme un logiciel. Elle a des inputs, elle transforme l'information, interagit, puis elle génère des outputs.

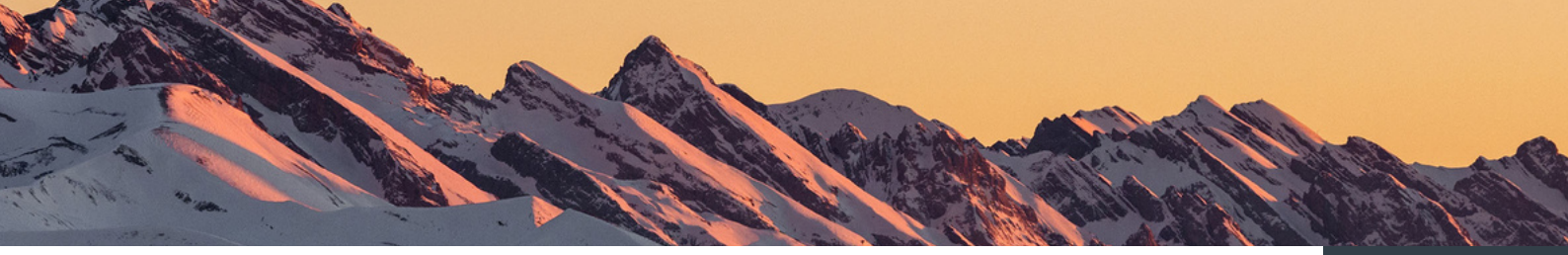
En entrée, elle reçoit des demandes de clients potentiels, en sortie elle produit des anglophones. C'est son processus clé : transformer des anglophones aspirants en anglophones confirmés. Et tout doit supporter cet objectif. En plus des inputs/outputs, elle interagit avec des tiers : elle a des fournisseurs, par exemple des éditeurs de logiciels d'apprentissage, et des partenaires, par exemple une école enseignant l'allemand.

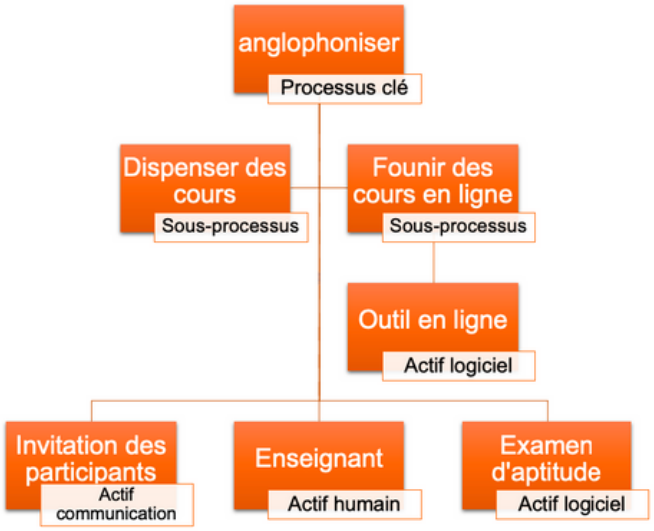
Pour aborder la question de la sécurité de l'information, je viendrais d'emblée avec une approche orientée risque, sur le processus clé. En d'autres termes, que peut-il arriver qui empêcherait notre PME de transformer des anglophones aspirants en confirmés ?

1. Les aspirants pourraient ne pas réussir à entrer en contact,
2. La formation pourrait échouer,
3. Les certificats pourraient ne pas être délivrés.

Chaque processus est soutenu par des sous-processus, puis finalement par des actifs. Par exemple, le processus formation dépend du déroulement d'un cours, qui dépend des actifs « professeur » et « outil de formation en ligne ». Dans un esprit aligné au standard COBIT, on peut évaluer les risques sur les processus. Et dans un esprit ISO, on peut l'évaluer sur les actifs. On peut donc s'imaginer le processus clé au sommet d'une pyramide de processus et actifs, chacun qualifié en termes de risque.

Dès lors l'ensemble des efforts de la société peuvent être perçus comme des tentatives de réduction de risque. La réceptionniste qui répond au téléphone minimise le risque d'échec de prise de contact. La dernière méthode d'enseignement diminue le risque d'échec d'apprentissage. Et la base de données client à jour assure que les certificats seront envoyés aux bonnes adresses.
La procédure consiste donc dans un premier temps à cartographier l'entreprise.





Le sommet de la pyramide est constitué de processus. Le bas de la pyramide est composé des actifs supportant les processus.

Le risque peut dans un second temps être évalué individuellement pour chaque risque et chaque processus. Dans un second temps, on peut cascader les risques en les additionnant de bas en haut.

Par exemple, les risques d'échec de contact est constitué des risques : réceptionniste malade, email en panne, téléphone hors service, pandémie virale et porte bloquée. L'analyse de risque n'est pas de la voyance, c'est un modèle de prise de décision collective dans un esprit pessimiste. L'exercice mental d'analyse de risque doit aussi amener à envisager des problèmes rares, graves et exogènes. Par exemple un stockage de données sensibles peut se répliquer entre deux pays, en cas de tensions dans l'un d'eux. Cette approche aurait été également intéressante en cas de foyer infectieux localisé.

En conclusion, l'informatique ne doit jamais être considérée comme une fin en soi. Elle n'est que l'évolution moderne du scribe, de la bibliothèque d'Alexandrie et des cartons de fichiers centraux. Ce qui est plus récent est la masse d'informations traitées, la complexité des systèmes qui les hébergent et la fréquence de l'échange d'information avec des tiers. Ainsi la sécurité n'est plus tellement une question de « où ». Elle est devenue une question de « qui et quoi ».

govern
GOVERNANCE & SERVICE MGT

digital strategy & organisation - risk, compliance & audit - information security - portfolio & project practice - service management

Contact:

info@itecor.com
www.itecor.com