Cyber et sûreté, deux pans de la protection des entreprises. Quid du positionnement et du pilote du dispositif ?

Kevin Gomart
Senior advisor
CyberCercle

La protection de l'information occupe une place centrale dans le fonctionnement de toute organisation. Et loin de se limiter à une question d'informatique, elle concerne la protection de l'ensemble du patrimoine informationnel, qu'il s'agisse de données numériques, de documents physiques, ou tout autres formes d'informations sensibles.

Dans ce cadre, deux acteurs concourent à cette défense au sein des entreprises : la sûreté, qui a comme enjeux de protéger l'entité des actes de malveillance (historiquement la protection des personnes et des biens matériels et immatériels), et la cybersécurité qui a la charge de traiter les risques liés à l'omniprésence des systèmes d'information et de communication.

La gouvernance, clef de voute de la protection de l'Information.

Pour garantir une protection efficace de cet actif précieux qu'est l'Information, la gouvernance est la clef de voute pour veiller à ce que les mesures de protection soient appropriées, systématiques, systémiques et évolutives, tout en s'assurant de leur mise en œuvre et de leur contrôle. Elle implique la définition des politiques, des procédures, des normes, et des pratiques qui garantissent que le patrimoine informationnel de l'organisme est correctement défendu contre les accès inopportuns et les altérations en tout genre. Elle vise également à équilibrer les besoins de sécurisation avec les impératifs opérationnels, à minimiser les risques, et à s'adapter en permanence à l'évolution des menaces et des technologies.

Afin de garantir la mise en place et le pilotage d'une stratégie claire, il est essentiel de désigner un pilote, une personne, et une entité associée, responsable de la sécurité de l'information et en charge de coordonner une démarche globale organisée, transversale, collaborative et dynamique. Ce pilote doit être capable de rendre des comptes quant à la mise en place et au maintien des mesures de protection, ainsi que de garantir leur adéquation avec les évolutions du contexte sécuritaire.

Le patrimoine informationnel n'est pas uniquement composé de documents ou de données. Il est aussi composé des acteurs clefs de l'entreprise : sa composante humaine. Comment peut-on aujourd'hui protéger l'information sans protéger ses collaborateurs dans leur vie professionnelle au quotidien : travail sur site, déplacements nationaux ou internationaux, etc. ?

Une convergence accrue entre cybersécurité et sûreté.

Longtemps séparées, les activités de sûreté et de cybersécurité commencent donc à se rapprocher. Cette convergence est malheureusement aujourd'hui le théâtre de débats de politique interne et de luttes de pouvoir avec comme seul et unique but : l'attribution de ce budget conséquent porté par « la cyber ». La mainmise du numérique sur les activités de toutes les entités et la prise de conscience de cette menace par les dirigeants ont augmenté fortement les budgets des directions des systèmes d'information (DSI) de nombreuses entreprises.

Mais comment s'assurer que la sécurité des systèmes d'information est correctement dotée alors que le Directeur de la DSI se retrouve constamment à arbitrer des choix entre disponibilité et sécurité des systèmes ? Sans critique, cette position n'est confortable pour personne mais ce biais, bien connu, doit être pris en compte par les organisations.

Désigner le pilote : les facteurs à prendre en compte

Où donc positionner cette entité chargée de protéger l'entreprise de toute menace extérieure, et surtout à qui donner en donner les clefs ?

Cette question complexe se résout par la prise en compte de plusieurs facteurs :

- Organisationnels : le positionnement doit permettre une vision transverse de l'entreprise, en limitant au maximum les biais cognitifs ;

- Métier : avant de concevoir et d'implémenter une quelconque stratégie, la pensée qui pilote cette action doit se situer dans le futur de l'organisation et dans l'anticipation constante à court, moyen et surtout long termes. Il est donc nécessaire que cette entité et son pilote soient au niveau hiérarchique et dans les organes de gouvernance permettant l'acquisition de l'information nécessaire à la réalisation de la mission ;

- Humains : le pilote de cette activité est majoritairement vu comme « un mouton à 5 pattes ». Ses compétences doivent être larges, dotées en outre d'une bonne adéquation entre qualités humaines et compétences professionnelles.

En effet, ce leader doit allier la capacité du politique à pouvoir échanger à tous les niveaux de l'organisation (de l'ouvrier au dirigeant), l'aptitude à anticiper « à plusieurs coups des stratèges » l'adaptation constante afin d'accompagner le business sans l'entraver, une tête froide face aux crises et surtout une connaissance fine de conception de dispositifs de protection qui trouveront par la suite une mise en application technique en descendant dans les équipes.

Chaque organisation d'entreprise est différente. C'est la raison pour laquelle il est difficile de donner un positionnement unique. Certains positionneront cette entité directement chez le PDG (CEO), avec certains risques si le leader n'est pas membre du comité exécutif. D'autres auprès du DRH (CPO), avec le risque de ne prendre en compte que la protection humaine et la responsabilité sociétale, ce qui entravera l'action globale. On pourra le voir aussi auprès du Directeur Technique (CTO) ou du DSI (CIO), avec le risque du biais technique qui privilégiera majoritairement la protection numérique.

En définitive un rattachement au Directeur des Opérations (COO) est sûrement le plus à même de servir l'entreprise. Pour les entreprises n'ayant pas ce type de poste dans leur gouvernance, il conviendra de privilégier le membre du comité exécutif (EXCOM) qui porte la gestion des risques, voire de nommer ce pilote au sein de cette instance afin de lui donner la vision globale des enjeux de la structure.

Mais quel que soit le positionnement choisi, il est primordial que le pilote de cette protection globale dispose d'un mandat clair et de la liberté d'action nécessaire à l'accomplissement de sa mission. Sans ces deux éléments, il y a fort à parier qu'à terme l'entreprise augmentera sa surface de risque plutôt que de la réduire.