Pourquoi le risque cyber est aussi l'affaire des Directions Financières

MAXIME CARTAN,
Co-fondateur et CEO

ALFREDO GARCIA,
CFO, Citalid

Les entreprises de toutes tailles et de tous secteurs s'appuient chaque jour un peu plus sur la technologie pour piloter l'ensemble de leurs opérations. En parallèle, les menaces cyber évoluent au rythme de ces avancées technologiques et du contexte géopolitique.

Directions financières et RSSI : unis face au risque cyber

Si les RSSI sont en première ligne face au risque informatique, la cybersécurité n'est pas seulement un problème technologique ; c'est un sujet qui concerne toutes les fonctions de l'entreprise. Pour qu'une entreprise valorise son image de marque, préserve la confiance de ses clients et sa stabilité financière, des mesures de cybersécurité appropriées doivent être mises en place pour protéger les actifs et les données.

Pour réduire la pression de la menace, il faut la comprendre et évaluer les risques qui en découlent. Cette évaluation précise du risque permet ainsi aux directeurs financiers de projeter une véritable stratégie d'investissement au sein de leur organisation.

Les dépenses de sécurité passent parfois au second plan par rapport à des priorités informatiques ou commerciales. Par conséquent on constate que les entreprises sont parfois mal préparées pour faire face aux menaces, notamment cyber. Il est essentiel de consulter le RSSI pour déterminer comment le financement pourrait contribuer au développement d'une culture de sécurité et de confidentialité. En valorisant la cybersécurité, la protection de la vie privée et la protection du partage de la donnée, les organisations améliorent leur profil de sécurité.

La difficulté à laquelle sont aujourd'hui confrontées les directions financières est la faible lisibilité, à la fois des réelles menaces qui pèsent sur leurs organisations et sur les réponses apportées par les fournisseurs de solutions technologiques. Nombreux sont les rapports et études qui mettent en lumière l'ampleur du risque cyber, sa technicité, sa force de frappe, etc. Pourtant, il est important pour chacun – au sein de sa propre organisation – de comprendre le risque qui lui est propre, en fonction de son industrie, de son périmètre géographique, de sa taille, etc.

Déployer les solutions de cybersécurité pertinentes, c'est-à-dire adaptées au risque spécifique de l'organisation, tout en faisant face aux contraintes financières associées est une problématique majeure pour les entreprises. Pour garantir que leurs activités sont suffisamment protégées contre les cyber-risques, les directeurs financiers doivent pouvoir s'appuyer sur des outils d'aide à la décision et ainsi accompagner les RSSI dans l'arbitrage des investissements réalisés.

Mesurer le risque cyber avec précision pour optimiser son pilotage

Les assureurs ont tout intérêt à collaborer étroitement avec les entreprises assurées pour comprendre la menace, les mesures de cybersécurité implémentées et les potentiels dommages. Cette collaboration, rendue possible par un modèle unifié de quantification du risque cyber, permettrait aux assureurs d'offrir une protection appropriée et de définir des polices qui représentent équitablement le degré de risque.

Les directions financières et les RSSI peuvent, ensemble, traduire le jargon de la cybersécurité en termes business et coordonner les risques et les objectifs de cybersécurité en objectifs organisationnels et stratégiques. C'est le cœur de l'exercice de quantification : traduire le risque cyber en risque financier. Ensemble, ils peuvent également définir le niveau de risque en fonction d'un secteur ou d'un environnement spécifique, en mettant en perspective les scenarios applicables à des entreprises similaires.

De la même manière, les directeurs financiers et les assureurs doivent également suivre les dernières positions légales et obligations de régulation en matière de cybersécurité. Accompagnés de la direction des risques, ils peuvent ainsi assurer une couverture et une maîtrise suffisantes et fixer des provisions qui reflètent fidèlement l'exposition. Pour cela il est essentiel que les assureurs et les sociétés quantifient en bonne intelligence les différents risques cyber de la structure.

Directions financières : un rôle-clé dans le pilotage de la stratégie cyber

Si la finance est l'un des secteurs les plus sensibles aux attaques cyber, il faut plus largement que toutes les directions financières participent activement au pilotage du risque cyber. Ce n'est qu'ainsi que la cybersécurité ne sera plus un coût pour l'entreprise, mais un investissement. Le directeur financier doit être bien informé sur les questions de sécurité informatique et le contexte juridique associé pour pouvoir ajuster l'allocation des ressources au regard de la nécessité de protection des actifs et données. Il doit hiérarchiser les objectifs de l'entreprise et tenir compte du retour sur investissement potentiel des solutions de sécurité et d'assurance pour offrir une couverture suffisante et fixer des provisions qui reflètent de manière appropriée le degré de risque.

Ainsi, il est important pour les parties prenantes de comprendre les tendances cyber pour pouvoir mieux les appréhender. Équipées d'un produit qui les accompagne dans cette compréhension des risques propres à leur organisation et des solutions qui pourraient les aider à le réduire, les directions financières joueront aux côtés des RSSI un rôle actif dans les prises de décisions et la définition d'une stratégie de pilotage du risque. Les fonctions traditionnellement dites « support » doivent devenir la clé de voûte de la résilience de l'entreprise, de sa réputation et de sa stabilité financière. ■