CGI

La force de l'engagement[MD]

Gouvernance de la sécurité des TI

Une approche globale

Comprendre la gouvernance de la sécurité des TI

Pourquoi en avons-nous besoin? La technologie ne suffit-elle pas?

INTRODUCTION

La menace dont font l'objet les actifs informationnels fondés sur la technologie est plus grande aujourd'hui que par le passé. L'évolution de la technologie s'est également reflétée dans les outils et méthodes utilisés par ceux qui tentent d'accéder sans autorisation aux données ou de perturber les processus d'affaires.

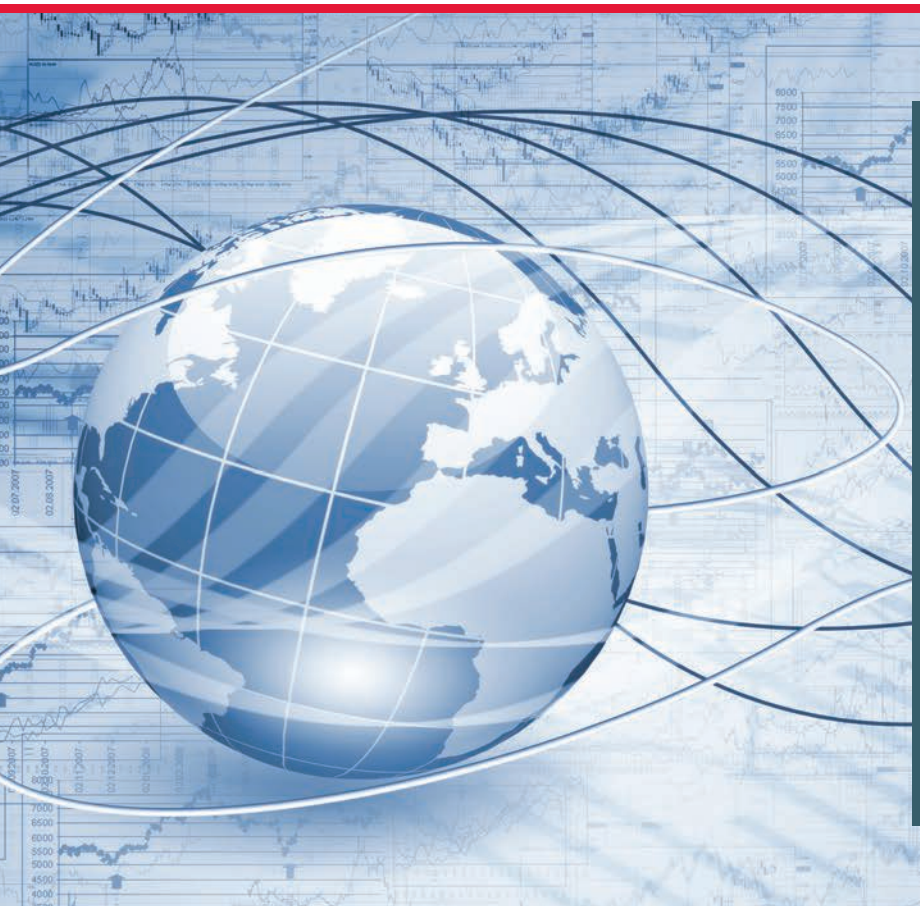
Les attaques sont inévitables, quelle que soit l'organisation. Mais le degré de sophistication et de persistance de ces attaques dépend de l'attrait de cette organisation en tant que cible, principalement en fonction de son rôle et de ses actifs. Aujourd'hui, les menaces posées par certains individus malavisés ont été remplacées par des groupes criminels internationaux organisés hautement spécialisés ou par des états étrangers qui disposent des compétences, du personnel et des outils nécessaires pour mener des attaques secrètes et sophistiquées de cyberespionnage.

Ces attaques n'ont pas seulement pour cible les entités gouvernementales; au cours des dernières années, plusieurs grandes entreprises ont été infiltrées, et leurs données ont été « consultées » pendant plusieurs années à leur insu.

En fait, l'amélioration de la cybersécurité s'est révélée l'une des principales priorités en matière de TI, tous secteurs d'activité confondus, lors des entrevues annuelles menées en personne en 2015* par CGI auprès de ses clients. Donc, tandis que des entreprises œuvrant dans des domaines comme l'industrie aérospatiale et les ressources stratégiques peuvent constituer des cibles idéales pour le cyberespionnage par des États-nations, d'autres gérant des actifs financiers ou des renseignements de cartes de crédit à grande échelle sont tout aussi attrayantes pour les groupes criminels internationaux.

Ces acteurs malveillants ne se contentent plus de déjouer les moyens de protection techniques. Au lieu de cela, ils sondent et exploitent une variété de faiblesses détectées dans l'environnement ciblé. Selon notre expérience, ces faiblesses ne sont pas uniquement d'ordre technologique, mais résultent également de défaillances dans les procédures de protection ou de lacunes dans les pratiques de gestion des vulnérabilités. La meilleure technologie du monde, si elle est mal appliquée ou mal employée, n'assurera pas une défense adéquate contre de telles menaces.

*En 2015, CGI a réalisé 965 entrevues en personne avec des clients issus de 10 secteurs d'activité et 17 pays dans le cadre de son programme *La voix de nos clients*.



« Les entreprises dépensent des millions de dollars sur les pare-feu, le chiffrement et les dispositifs de protection d'accès. C'est de l'argent jeté par les fenêtres, car aucune de ces mesures ne s'attaque au maillon le plus faible de la chaîne de sécurité. » [les personnes]

– Kevin Mitnick

Reconnu coupable aux États-Unis pour avoir pénétré les systèmes de grandes entreprises; maintenant reconnu mondialement en tant que conseiller en matière de sécurité.

AVOIR RECOURS UNIQUEMENT AUX TECHNOLOGIES DE SÉCURITÉ

Nous vivons dans un monde axé sur la technologie. Il n'est pas rare que les entreprises se tournent d'abord vers des solutions de sécurité techniques, sans vraiment tenir compte de la manière dont ces solutions seront mises en œuvre, maintenues et gérées de façon quotidienne.

Nous voyons trop souvent des organisations mettre en place des mesures de protection techniques comme les pare-feu ou la détection des intrusions, sans toutefois mettre correctement en œuvre **les politiques ou les procédures de sécurité**. Il en résulte **des pratiques inadéquates qui compromettent la sécurité et exposent les actifs à un risque important**.

Voici quelques exemples de telles pratiques.

- **Politique** ou procédures **de sécurité non existantes**
- **Politiques de sécurité** qui, lorsqu'elles existent, sont **périmées ou ignorées**
- **Sensibilisation insuffisante aux pratiques de sécurité** à tous les niveaux
- **Zonage inefficace des réseaux**, ou manque de conformité du zonage
- **Renforcement** et correctifs **inadéquats**
- **Mauvaises pratiques de contrôle d'accès**, comme les mots de passe de groupe non contrôlés, les comptes partagés, la prolifération des privilèges d'accès universel, l'accès partagé à la racine, l'absence de processus d'autorisation (sauf à un niveau opérationnel inférieur)
- **L'absence d'audits** et de revues de la **conformité en matière de sécurité**
- **L'absence de figure d'autorité pour les décisions** concernant la sécurité et l'intégrité de l'infrastructure et des actifs informationnels

Le résultat final est une entreprise qui se sent en sécurité parce qu'elle a investi dans des solutions de sécurité, mais dont les vulnérabilités inhérentes sont si nombreuses que la protection obtenue est en réalité très faible. Dans ce cas, l'organisation a **un faux sentiment de sécurité** qui peut s'avérer dangereux, car elle demeure extrêmement vulnérable aux attaques, puisque les intrus profitent de ces pratiques inadéquates pour contourner les solutions de sécurité et obtenir le contrôle des systèmes. Il ne s'agit pas d'un cas théorique. C'est **un scénario courant** qui a été observé comme cause fondamentale dans un grand nombre d'attaques réussies et très publicisées visant les grandes entreprises et les organismes gouvernementaux.

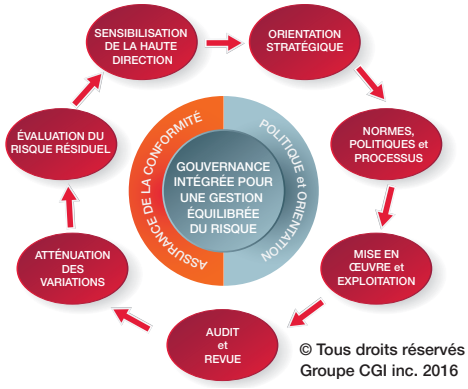
LE RÔLE DE LA GOUVERNANCE DE LA SÉCURITÉ DES TI

La gouvernance de la sécurité réunit tous les éléments de base de la cyberdéfense et de la gestion efficace du risque. Sans cette gouvernance, des lacunes dangereuses persistent et les actifs sont inévitablement compromis. En outre, l'équipe de direction n'est pas consciente de l'exposition au risque de son organisation, pour laquelle elle sera ultimement tenue responsable.

La sécurité ne peut pas exister en vase clos et doit faire partie d'une stratégie globale de gestion du risque fondée sur les objectifs d'affaires et les valeurs de l'organisation. Les organisations doivent connaître leur seuil de tolérance au risque, ou leur « niveau de risque acceptable ». Ce seuil peut varier selon la catégorie d'actifs. Par exemple, une organisation peut tolérer un certain niveau de risque dont les répercussions sont considérées comme mineures, mais être très réfractaire à tout risque pouvant nuire à sa réputation.

La gouvernance est le mécanisme par lequel ces valeurs relatives au risque sont reflétées dans l'orientation et le jugement qui déterminent les plans d'affaires, l'architecture de l'information, les politiques et procédures de sécurité, ainsi que les pratiques d'exploitation. Cependant, il ne sert à rien de déterminer l'orientation à prendre si l'on ne met aucune mesure en place pour s'assurer qu'elle est respectée.

Par conséquent, la **conformité constitue une boucle de rétroaction essentielle pour la gouvernance de la sécurité**. Elle permet de s'assurer que tous travaillent ensemble conformément au plan dans l'exécution de leurs activités d'affaires et assurent la protection des actifs, compte tenu du contexte de gestion du risque ainsi que de la stratégie et de l'orientation à suivre en matière de sécurité. Lorsque ce n'est pas possible, elle permet de s'assurer que les écarts qui résultent de certaines expositions au risque sont communiqués à l'équipe de direction, pour qu'elle puisse prendre la décision d'accepter ces risques ou d'appliquer les mesures et les ressources nécessaires pour y remédier.



« Si vous croyez que la technologie [à elle seule] peut résoudre vos problèmes de sécurité, c'est que vous ne comprenez pas ces enjeux et que vous ne comprenez pas la technologie. »

– Bruce Schneier

Cryptographe reconnu dans l'industrie, spécialiste en sécurité et confidentialité informatiques, associé au Berkman Center for Internet & Society de la Harvard Law School, associé de programme au New America Foundation's Open Technology Institute et directeur de la technologie de Resilient Systems.

GOUVERNANCE DE LA SÉCURITÉ DES TI – LA RESPONSABILITÉ DE LA HAUTE DIRECTION

Dans le passé, la sécurité était souvent déléguée aux gestionnaires et administrateurs des niveaux techniques et opérationnels. Cependant, en raison de l'envergure et de la complexité accrue de la technologie déployée et de la nature des menaces, **la responsabilité finale pour la protection de la mission et des actifs d'une organisation incombe désormais à la haute direction**.

Un exemple probant est celui de l'atteinte massive à la sécurité dont une grande entreprise multinationale a été victime en 2013. Selon les estimations, cette brèche de sécurité aurait compromis des dizaines de millions de comptes de carte de crédit et de renseignements personnels de clients, entraînant dans son sillage la démission du chef de la direction informatique, puis du chef de la direction de l'entreprise. Selon des sources de l'industrie, la multinationale a dépensé plus de 60 millions $ US en mesures d'atténuation à la suite de cette intrusion. S'appuyant sur les dures leçons tirées de cet incident et des pertes massives qui en ont découlé, l'entreprise a mis en place des mesures d'atténuation supplémentaires. Bon nombre d'analystes considèrent qu'elle propose désormais un programme de sécurité modèle qui responsabilise tous les niveaux de l'organisation et assure la visibilité des mesures de sécurité.

Il est intéressant de constater les divergences entre les perspectives des chefs de la direction et celles des gestionnaires des fonctions techniques et opérationnelles. En effet, d'après les entrevues menées dans le cadre du programme *La voix de nos clients en* 2015, les chefs de la direction ont affirmé que, selon eux, l'incidence de la protection des données était mineure, l'exhaustivité de leurs programmes de sécurité satisfaisante et les dépenses encourues pour assurer la cybersécurité peu élevées – contrairement aux points de vue énoncés par les responsables techniques et opérationnels.

Nous avons vu que les équipes de direction des organisations insistent maintenant sur la création de politiques et de procédures de sécurité, car l'industrie reconnaît l'accroissement de la menace et l'importance des pratiques de sécurité exemplaires. Nous avons également vu des cas dans lesquels les politiques et procédures adéquates existent, mais n'ont pas du tout été mises en œuvre ou l'ont été de manière incohérente au niveau opérationnel.

Les hauts dirigeants de ces entreprises croient s'être acquittés de leur responsabilité de diligence et croient que les risques sont gérés de manière efficace. Pourtant, l'inverse est souvent vrai, **et ils n'ont pas conscience que leur organisation demeure extrêmement vulnérable en raison des failles endémiques dans leur processus de gouvernance**. En dernière analyse, les risques critiques demeurent, et l'équipe de direction, bien que mal informée, continue d'être tenue responsable. Ce faux sentiment de sécurité est extrêmement dangereux pour une organisation et entraîne une situation incontrôlée en matière de risque et de responsabilité.

LA RÉPONSE : VISIBILITÉ, RESPONSABILITÉ ET GESTION DE LA CONFORMITÉ

Pour relever les défis modernes en matière de sécurité, les organisations doivent constamment **appliquer des pratiques efficaces de gestion du risque à tous les niveaux**. Les risques doivent être visibles pour la haute direction, qui doit jouer un rôle clé en acceptant ces risques ou en dirigeant les activités et en allouant les ressources nécessaires pour ramener ces risques à des niveaux acceptables sur les plans commercial, juridique, législatif et réglementaire. Pour ce faire, **l'équipe de direction doit avoir une visibilité de l'imputabilité et de la responsabilité dans chaque cas**.

L'imputabilité et la responsabilité doivent être attribuées à toutes les personnes qui participent à la gestion du risque ainsi qu'à la mise en place et à l'utilisation d'un environnement d'information résilient, sensible et offrant une confidentialité, une intégrité et une disponibilité adéquates. À cette fin, une stratégie ou politique globale de l'entreprise en matière de sécurité doit inclure une matrice RACI[1] qui remplit exactement cette fonction. Cette matrice RACI doit constituer un élément clé des audits et examens de conformité.

L'AUDIT ET L'EXAMEN DE CONFORMITÉ — VOTRE FILET DE SÉCURITÉ

Les audits et examens de conformité sont « les ingrédients secrets » qui permettent de s'assurer que les politiques et les processus en matière de sécurité sont rigoureusement respectés, conformément à la stratégie de gestion du risque ou de la sécurité de l'entreprise. Ils constituent également un élément intégral de tous les programmes de gestion des opérations, y compris ISO 27001, COBIT, Sarbanes Oxley et ITIL. **En l'absence d'un processus d'assurance de la conformité, il est impossible de garantir que les risques sont gérés comme prévu**, ou de détecter et de corriger les problèmes éventuels lorsque ce n'est pas le cas.

Les audits et examens d'assurance de la conformité représentent un baromètre du fonctionnement de la gouvernance de la sécurité et fournissent à la haute direction une visibilité dans les secteurs qui comportent une exposition aux risques et où des ajustements sont nécessaires. En outre, à moins que les intervenants comprennent que les actions, les décisions et les résultats seront vérifiés en fonction des normes et des contrôles établis, ils sont peu motivés à assurer la conformité, ce qui entraîne une « dérive de la conformité ». Cet écart, et tous les risques associés augmenteront avec le temps.

Bien que les gestionnaires des opérations considèrent souvent les audits et examens comme étant intrusifs et même punitifs, il faut éviter que cette perception ne prévale. Les audits et examens permettent aux gestionnaires de mettre en évidence les secteurs dans lesquels les mesures de contrôle et les normes ne sont pas respectées pour diverses raisons échappant à leur contrôle, par exemple aucun établissement des priorités, un manque de ressources, ou encore l'absence de technologie ou de financement. **Les audits et les examens sont les mécanismes essentiels par lesquels la haute direction peut prendre connaissance des enjeux à résoudre au niveau opérationnel**.

Il existe généralement trois types d'activités liées à l'assurance de la conformité.

- **Examens internes de la conformité –** Effectués au niveau de la gestion des opérations, ils visent à détecter les problèmes rapidement et à mettre en place des mesures correctives relevant du champ d'application des ressources au niveau opérationnel. Les examens de la conformité doivent régulièrement inclure des évaluations comme l'analyse de

[1] **Responsabilité, approbation, consultation, information.** Une approche matricielle pour la mise en correspondance des rôles et des responsabilités. Compatible avec ITIL v3 et ISO 27001-2013

vulnérabilité et les essais de pénétration. En outre, il est recommandé d'envisager des services de mises à l'essai et de certification. Tout comme la conformité aux normes ISO 9000 a servi d'amorce externe pour la mise en œuvre de la gouvernance de la qualité, nous croyons qu'il peut en être de même avec la gouvernance de la sécurité.

- **Audits internes** – Effectués par des membres indépendants du personnel à l'interne, les audits internes sont conçus pour permettre une vérification de l'état de la situation en matière de conformité, servir de préparation en vue des audits externes, ou concentrer les efforts sur les secteurs qui semblent aux prises avec des problèmes persistants. Les audits internes ne doivent pas être effectués par le groupe même qui a la responsabilité d'atteindre la conformité.
- **Audits externes** – Ils sont effectués dans le cadre d'un processus de certification, ou lorsqu'un problème particulièrement critique requiert une opinion « externe » indépendante. Lors des audits externes, il est important de travailler en étroite collaboration avec les associations internationales de sécurité et les organismes de normalisation.

Les problèmes critiques et persistants définis durant les revues internes doivent être communiqués à un comité de direction d'examen des risques (ERRB), composé de cadres supérieurs clés (p. ex., hauts dirigeants), afin qu'ils soient informés de tous les risques associés et puissent également envisager l'affectation de ressources afin d'atténuer les risques.

Pour les mêmes raisons, les rapports des audits internes et externes doivent toujours être présentés au comité ERRB.

Dans tous les cas, le comité ERRB doit exiger qu'un plan d'atténuation du risque soit fourni et que des ressources soient attribuées en conséquence.

DIX MESURES POUR UNE BONNE GOUVERNANCE DE LA SÉCURITÉ DES TI

Définition de la gouvernance

1. Déployez le modèle de gouvernance émanant du conseil d'administration dans l'ensemble des fonctions de l'entreprise par l'entremise de la haute direction.
2. Développez et mettez en œuvre une approche de gestion du risque et une politique de sécurité globale de l'entreprise, en conformité avec vos exigences et processus d'affaires.
3. Établissez un comité ERRB, ou intégrez-le à votre structure actuelle de gestion du risque, comme défini dans votre stratégie globale de gestion du risque.
4. Nommez une autorité de sécurité des TI de l'entreprise, préférablement dotée d'une chaîne de commandement différente de celle de l'exploitation des TI. Définissez clairement les rôles et responsabilités.
5. Établissez une autorité d'audits et de revues internes dotée de lignes de communication directes avec l'ERRB.
6. Établissez et mettez en œuvre un cadre de gestion de conformité aux audits et aux revues, pour vous assurer que ses objectifs sont communiqués dans toute l'organisation.

Mise en œuvre de la gouvernance

7. En collaboration avec les équipes fonctionnelles et opérationnelles, définissez les actifs et l'information essentielle ainsi que les menaces et risques qui y sont associés.
8. Développez et mettez en place des mesures de contrôle de sécurité ainsi que les procédures qui y sont associées, en vous assurant que la responsabilité et l'imputabilité sont définies en conformité avec le modèle RACI pour la gestion du risque.
9. Créez et déployez un programme obligatoire de sensibilisation à la sécurité, auquel le personnel devra participer pour bien comprendre ses responsabilités et les objectifs visés par la gestion du risque et les contrôles de sécurité, et le raisonnement sous-jacent.

Mise à jour de la gouvernance

10. Examinez régulièrement tous les éléments du programme afin d'effectuer les ajustements nécessaires et de vous assurer que les risques sont gérés efficacement et d'une manière équilibrée qui tient compte des besoins opérationnels.

CONCLUSION

Dans les grandes organisations modernes, il n'est plus possible d'assurer une sécurité et une gouvernance des actifs informationnels de manière ponctuelle, ou en ne déployant que des solutions techniques. Ces organisations ont plutôt besoin d'une approche globale **appliquant une gestion efficace du risque et une bonne gouvernance dans l'ensemble de l'organisation**, et par laquelle les valeurs clés que sont la **visibilité, l'imputabilité et la responsabilité** sont exprimées à tous les niveaux. Cependant, une organisation peut avoir besoin d'assistance pour effectuer cette transition, et CGI a travaillé avec plusieurs entreprises pour les aider à élaborer un processus adéquat de gouvernance de la sécurité des TI.

La haute direction joue un rôle crucial en prenant des décisions fondées sur le risque, en définissant une orientation et en s'assurant que les ressources adéquates sont disponibles pour concrétiser cette orientation. Cette démarche n'est possible qu'au moyen d'**un processus rigoureux de conformité et de production de rapports par lequel l'équipe de direction est engagée et tenue informée** et, au besoin, fait appel à de l'assistance externe. En prenant les mesures décrites dans la présente étude technique, une organisation sera mieux préparée à gérer les risques à mesure qu'ils surviendront et à devenir suffisamment résiliente en matière de sécurité pour contrer les menaces d'aujourd'hui.

Un fournisseur mondial de services en technologies de l'information et en gestion des processus d'affaires qui offre des services-conseils en management, ainsi que des services d'intégration de systèmes et d'impartition.

---

cgi.com