Deloitte.

Dans le contexte d'affaires actuel caractérisé par la volatilité à l'échelle mondiale, les conseils d'administration devraient se concentrer sur les activités essentielles – les ingrédients du succès – qui leur permettent de faire face aux principaux défis de l'heure. La cybersécurité est l'une de ces principales activités.

Téléchargez
Alerte aux administrateurs 2016
La recette du succès :
Trouver un juste équilibre

Votre organisation est-elle cyberavertie? Éléments que les conseils d'administration devraient considérer

On ne se demande plus si une cyberattaque se produira, mais quand elle se produira, si elle n'a pas déjà eu lieu. En effet, durant la première moitié de 2015, des pirates informatiques ont volé plus de 245 millions d'éléments d'information à l'échelle mondiale, soit 16 éléments chaque seconde (Gemalto,"2015 First Half Review, Findings from the Breach Level Index".)

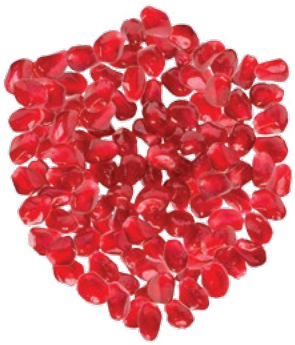
Les cyberattaques sont de plus en plus sophistiquées et difficiles à analyser et à maîtriser. Les menaces persistantes avancées, par exemple, sont des attaques discrètes qui soutirent lentement des données cruciales et sont difficiles à détecter à l'aide des méthodes traditionnelles.

Les cyberattaques prennent diverses formes, dont les suivantes :

- **Intrusion**, qui consiste à voler les données d'une organisation ou à les manipuler pour que l'organisation ne puisse plus s'y fier.
- **Le cybercrime**, soit le vol de données, comme les renseignements de cartes de crédit que le pirate utilise pour son propre avantage financier.
- **Les actes de sabotage**, comme le refus de fournir un service ou d'autres types d'attaques qui paralysent l'organisation.
- **L'espionnage**, qui vise à porter atteinte à la sécurité économique ou industrielle de l'organisation.

Les cyberattaques sont inévitables et souvent, les pirates se trouvent déjà dans le réseau de l'organisation.

En plus des perturbations immédiates, une cyberattaque entraîne souvent des litiges coûteux, des mesures des organismes de surveillance, des perturbations continuelles des activités, une capacité amoindrie d'exécuter la stratégie et une augmentation des primes d'assurance, autant d'éléments qui réduisent la valeur de l'entreprise. Il n'est donc pas surprenant que la cybersécurité soit devenue une activité de surveillance de plus



Dina Kamal
Deloitte Canada

Le conseil d'administration doit veiller à ce que la stratégie de l'organisation en matière de cyberprotection comprenne un plan robuste de gestion des cybercrises qui indique qui sont les personnes clés qui géreront les attaques et le rôle que chacune d'elles jouera. Le conseil d'administration doit aussi veiller à ce que le plan de gestion de crise de l'organisation soit répété.

Harry Raduege
Deloitte & Touche LLP
aux États-Unis

Les membres du conseil doivent tenir pour acquis que le réseau d'information de l'organisation a été ou sera bientôt attaqué et ils doivent accepter le fait que la cybersécurité n'est pas une question de tolérance zéro. Autrement dit, des attaques surviendront en dépit de tous les efforts déployés par l'organisation pour se protéger. Ce qui importe est la rapidité et l'efficacité de la réaction de l'organisation aux cybermenaces et aux attaques. Le conseil a un rôle clé à jouer pour ce qui est de garantir que la direction crée une organisation cyberavertie.

en plus importante des administrateurs, qui peut aussi avoir des implications personnelles pour les membres du conseil d'administration. En effet, à la suite de cyberattaques,des actionnaires ont exigé la destitution d'administrateurs ou ont engagé des poursuites contre eux. Les recours collectifs à la suite d'atteintes à la sécurité des données sont d'ailleurs de plus en plus fréquents. De plus, la *Cybersecurity Disclosure Act of 2015*, récemment introduite par le Congrès des États-Unis, obligerait les sociétés cotées à divulguer le nom des administrateurs qui possèdent une expertise en cybersécurité et à fournir des renseignements sur les administrateurs qui ont des connaissances sur la sécurité en ligne lors de dépôts auprès de la SEC.

La mauvaise nouvelle est que ce problème risque de s'aggraver parce que les cyberrisques ne cessent d'augmenter dans les organisations. Par exemple :

- Les organisations sont liées à d'autres organisations de leur écosystème par leurs chaînes d'approvisionnement qui, pour fonctionner efficacement, requièrent l'échange d'information. Chaque relation introduit des vulnérabilités.

- Le cyberespionnage et le vol de données sont en voie de devenir monnaie courante dans les fusions et acquisitions, les pirates tentant d'obtenir des données financières ou opérationnelles qui seront utilisées dans les négociations ou pour dévaluer l'une des organisations dans la transaction.

- Les employés utilisent souvent leurs appareils numériques personnels pour accéder aux données d'une organisation – un point d'entrée dont la sécurité dépend en grande partie de la sensibilisation de l'employé aux cyberrisques et des précautions qu'il prend avec ses appareils au travail et à l'extérieur.

- De plus en plus de personnes et d'entreprises utilisent les technologies infonuagiques en raison de leur coût inférieur et de leur commodité, une commodité qui profite aussi aux cybercriminels et autres malfaiteurs.

Créer une organisation cybersécuritaire

On dit que la cybersécurité d'une organisation est aussi solide que son plus faible employé, car les pirates recherchent des personnes naïves sans formation ni éducation qui peuvent leur fournir un point d'entrée dans le réseau de leur employeur. Les pirates utiliseront de faux comptes de courriel conçus pour paraître comme des messages envoyés par un ami ou un collègue et qui, une fois ouverts, transféreront des logiciels malveillants dans le réseau de l'organisation. Les cadeaux comme les clés USB, qui sont distribués en grandes quantités dans les salons professionnels et autres événements peuvent aussi contenir des logiciels malveillants. Les employés qui utilisent leurs appareils numériques pour accéder à un réseau WiFi non sécurisé peuvent, sans le savoir, donner l'accès à des pirates.

Dans ce contexte, les organisations doivent créer une culture de sécurité des données, un processus qui devrait être mené par le conseil d'administration et la direction, et auquel doivent participer l'ensemble de l'organisation et non juste le service des TI. De fait, l'organisation doit faire en sorte que tous ses employés soient cyberavertis afin de garantir qu'ils travaillent constamment avec vigilance dans un environnement sécuritaire et résilient.

Tse Gan Thio
Deloitte & Touche LLP
à Singapour

Dans le monde d'aujourd'hui où la technologie est omniprésente, tout membre du conseil qui se dit responsable doit se préoccuper de la cybersécurité. Les conseils d'administration doivent s'informer sur la cyberstratégie de l'organisation et son écosystème de sécurité, et demander quels renseignements l'organisation expose aux tierces parties.

Sécurité – Bon nombre d'organisations ont investi beaucoup de temps et d'argent dans des contrôles de sécurité et des mesures de prévention, et cet investissement devra augmenter. Malgré cela, il est impossible de tout protéger de façon égale. Les organisations doivent donc se concentrer sur leurs actifs les plus précieux, soit les données essentielles qu'elles doivent absolument protéger. Elles doivent aussi être au fait des pratiques liées à Internet de leurs partenaires et des autres parties avec lesquelles nous communiquons – contractants, fournisseurs et vendeurs – qui peuvent être des alliés en matière de sécurité ou représenter un danger. Il est important de réfléchir en termes de chaîne d'approvisionnement de l'information et de décider qui pourra accéder au réseau d'information et qui n'y aura pas accès.

Vigilance – Être vigilant signifie être cyberaverti. Tous les membres de l'organisation et leurs partenaires externes doivent être à tout moment conscients des cyberrisques. Les organisations cybervigilantes mettent en place et maintiennent des mécanismes de protection qu'elles surveillent et mettent à l'essai de manière proactive. Lorsque des pirates tentent de pénétrer un réseau ou que d'autres activités suspectes se produisent, l'organisation doit être en mesure de réagir de manière appropriée afin de repousser l'attaque, et elle doit aussi en tirer des leçons afin d'apporter les correctifs nécessaires.

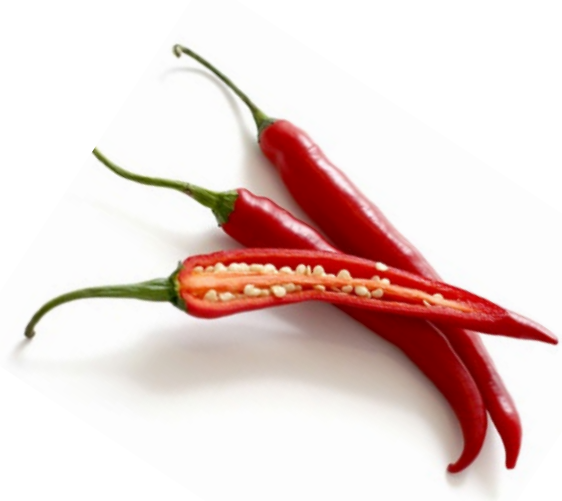
Résilience – Inévitablement, des intrusions se produiront et c'est pourquoi les organisations ont besoin d'une stratégie de gestion de crise et d'un plan de gestion des cyberrisques qui leur permettent de réagir et de reprendre leurs activités rapidement. Consultez l'article sur la gestion de crise dans notre *Alerte aux administrateurs 2016* intitulée « La recette du succès : Trouver un juste équilibre ».

La cybersécurité et le conseil d'administration

Le conseil d'administration doit remettre en question l'évaluation faite par la direction de la position de l'organisation sur le plan de la cybersécurité et examiner de manière critique ses capacités de gestion des cybercrises énoncées dans le plan de gestion.

De plus, le conseil aurait intérêt à revoir ses propres processus en matière de surveillance de la cybersécurité. Par exemple, le conseil pourrait élargir le mandat de son comité responsable de la surveillance des risques afin d'y inclure la surveillance des ressources attribuées à la gestion des risques. Il pourrait aussi envisager de nommer un responsable de la cybersécurité au sein du conseil, qui superviserait les activités de la direction et s'assurerait que les hauts dirigeants se concentrent adéquatement sur la cybersécurité.

Enfin, le conseil d'administration pourrait mettre sur pied un processus à l'égard des risques définissant les priorités de l'organisation en matière de gestion des cyberrisques et décrivant les mécanismes de responsabilisation. Il pourrait en outre vouloir consulter ses propres experts en matière de cybersécurité.



Questions que les administrateurs devraient poser :

1. Quelle est l'empreinte de l'organisation sur Internet? Quels renseignements diffusons-nous et quels canaux empruntons-nous pour le faire? Quels renseignements transmettons-nous aux tierces parties? Sommes-nous convaincus que notre réseau d'information et d'approvisionnement est suffisamment robuste pour protéger les données dans toute la chaîne?

2. Dans quelle mesure le conseil comprend-il les cyberrisques? Devrait-il faire appel à des experts externes pour informer ses membres sur les cyberrisques, les moyens de les réduire et la façon de reconnaître les signes d'une atteinte à la sécurité? À quelle fréquence le conseil reçoit-il des rapports ou mises à jour des personnes chargées de la surveillance des cyberrisques?

3. Quels sont nos actifs les plus précieux – l'information essentielle sans laquelle notre organisation ne pourrait pas poursuivre ses activités en raison d'une atteinte à cette information? Comment protégeons-nous cette information?

4. Notre organisation a-t-elle une stratégie globale en matière de cybersécurité et un plan de gestion des cyberrisques? Comportent-ils des éléments qui peuvent être mis en œuvre de manière proactive et d'autres, en réaction à une attaque? La direction a-t-elle établi des relations de travail avec les autorités policières locales? L'équipe de direction effectue-t-elle régulièrement des évaluations de la cybersécurité et des exercices de simulation?

5. Notre organisation est-elle capable de détecter rapidement une atteinte à la sécurité? Quels contrôles sont en place? Comment savons-nous que ces contrôles sont efficaces? Ont-ils été validés récemment? Combien d'attaques avons-nous subies, comment avons-nous répondu à ces attaques et quelles leçons en avons-nous tirées?

6. Avons-nous une assurance cyberrisque afin de réduire nos risques? Dans l'affirmative, quelle est l'étendue de notre protection?

Ressources

Vous voulez approfondir ces sujets? Nous avons choisi pour vous les points de vue suivants de Deloitte afin de vous aider à mieux cerner les occasions et les risques potentiels que ces sujets présentent pour votre organisation.

- Cinq étapes essentielles pour améliorer la cybersécurité – En route vers une organisation plus sécurisée, vigilante et résiliente (Deloitte Canada, avril 2015)
- Cybersecurity: The changing role of audit committee and internal audit (Deloitte Singapour, septembre 2015)
- Cyber Risk: Getting the boardroom focus right (Deloitte Royaume-Uni, mai 2015)
- Cyber threats and the Board's role in curbing it (Deloitte Inde, avril 2015)
- Digital Directors: The board's role in the cyber world (Deloitte Singapour, août 2015)
- La cybersécurité : un impératif pour tous (Deloitte Canada, mars 2015)
- Responding to cyber threats in the new reality: A shift in paradigm is vital (Deloitte Singapour, mai 2015)
- Sondage sur la cybersécurité 2015 : Rehaussez votre sécurité et résilience (Deloitte Canada, décembre 2015)

Leaders de la cybersécurité

National

Nick Galletto
Leader, Cybersécurité
ngalletto@deloitte.ca

Mark Fernandes
Leader, Cybersécurité
markfernandes@deloitte.ca

Est

Amir Belkhelladi
Associé, Services liés aux cyberrisques
abelkhelladi@deloitte.ca

Central

Dina Kamal
Associée, Services liés aux cyberrisques
dkamal@deloitte.ca

Ouest

Justin Fong
Associé, Services liés aux cyberrisques
jfong@deloitte.ca

Groupe consultatif sur la gouvernance

Albert Baker
Associé, Fiscalité
abaker@deloitte.ca

Arthur Driedger
Associé, Fiscalité
adriedger@deloitte.ca

Jonathan Goodman
Associé, Consultation
jwgoodman@deloitte.ca

Terry Hatherell
Associé, Service des risques d'entreprise
thatherell@deloitte.ca

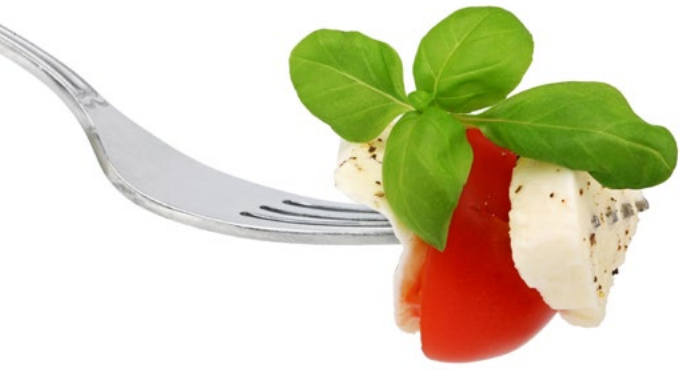
Eddie Leschiutta
Associé, Service des risques d'entreprise
eleschiutta@deloitte.ca

Chantal Rassart
Associée, Centre de gouvernance d'entreprise
crassart@deloitte.ca

Bill Stamatis
Associé, Conseils financiers
bstamatis@deloitte.ca

Heather Stockton
Associée, Consultation
hstockton@deloitte.ca

Don Wilkinson
Associé, Audit
dowilkinson@deloitte.ca



www.deloitte.ca