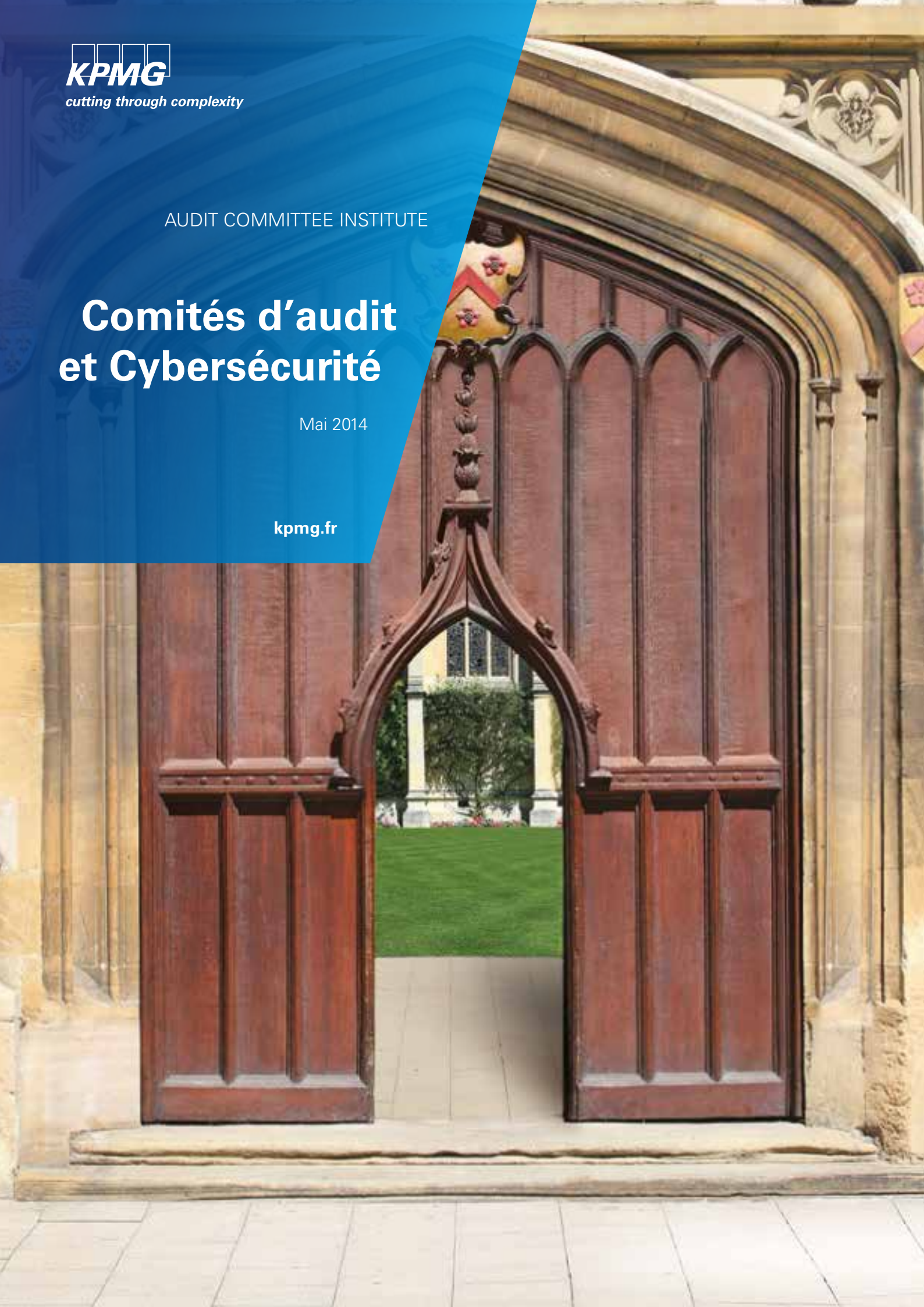
KPMG
cutting through complexity

AUDIT COMMITTEE INSTITUTE

Comités d'audit et Cybersécurité

Mai 2014

kpmg.fr



LA **CYBERSÉCURITÉ :**
présentation à l'attention des comités d'audit

Les comités d'audit ont un rôle essentiel à jouer pour aider les organisations à s'assurer qu'elles disposent de cyberdéfenses solides. Ceci ne passe pas forcément par une compréhension approfondie des technologies impliquées, mais plutôt par une orientation de leur gouvernance et de leur politique.

Sir Iain Lobban, directeur du service de renseignements chargé de la sécurité nationale *(Government Communications Headquarters)* au Royaume-Uni a déclaré[1] qu'avec 70 opérations de cyberespionnage menées chaque mois contre des réseaux du gouvernement et de l'industrie, des secrets commerciaux sont volés « en quantité industrielle ». Il ne serait clairement pas viable d'adopter une attitude attentiste à ce sujet.

Plusieurs questions sont à considérer, telles que :

Quels sont les principaux actifs à protéger ?

Comment sont-ils protégés ?

Qui est responsable de leur protection ?

Quel est le niveau de risque acceptable en matière de cybersécurité ?

Comment l'organisation réagirait-elle face à un incident majeur ?

Vous ne pouvez pas répondre à ces questions du tac-au-tac ? Vous n'êtes pas le seul. Néanmoins, il revient aux comités d'audit d'être de plus en plus exigeants en matière de cybersécurité.

1 Lors d'une interview avec la BBC en juillet 2013 au sujet de cyberattaques visant les entreprises britanniques

Quelle est la menace pour les organisations ?

Le cyberespace offre au crime organisé des opportunités fort lucratives. En effet, en exploitant les faiblesses de systèmes informatiques, les fraudeurs peuvent atteindre et contrôler à distance des ordinateurs, et ainsi enregistrer les principales combinaisons de touches utilisées, surveiller les écrans et les manipuler afin d'obtenir des données sensibles.
Le cyberespace permet à un pirate se trouvant n'importe où dans le monde de mener ses attaques dans plusieurs pays et juridictions, ce qui complique les enquêtes et l'application des lois.

Des **employés mal intentionnés** peuvent également collecter et sortir des locaux de leur entreprise une grande quantité d'informations sensibles la concernant au moyen de logiciels malveillants pouvant corrompre ses bases de données ou saboter les tâches relatives à l'exploitation de son réseau.

Autre pratique répandue dans le cyberespace : **l'espionnage industriel.** Ces attaques visent souvent une propriété intellectuelle sensible. Les opérations de certaines grandes entreprises ont été compromises pendant plusieurs mois en raison du vol de données particulièrement sensibles.

L'activisme est également devenu monnaie courante dans le cyberespace. Les **actions de sabotage et d'attaque** par déni de service sont de plus en plus fréquentes. Par le passé, elles auraient été attribuées à des groupes d'« hacktivistes » tels qu'Anonymous, mais il semble qu'elles sont aujourd'hui de plus en plus souvent commises pour des raisons politiques.

Quel est l'impact **potentiel** d'une atteinte à la cybersécurité ?

Une violation de cybersécurité peut affecter :

- **les systèmes et les actifs financiers** – par la fraude, le vol et l'extorsion ;
- **la propriété intellectuelle et les secrets commerciaux** – par l'espionnage ;
- **la marque et sa présence sur Internet** – par le boycott, la diffamation, l'engagement de la responsabilité et l'atteinte à l'image ;
- **la continuité d'exploitation** – par le sabotage ou la perturbation des opérations.

En quoi consiste le rôle du comité d'audit ?

A travers le monde, la plupart des codes de gouvernance d'entreprise attribue aux comités d'audit **la responsabilité de superviser les systèmes de contrôle interne et de gestion des risques de l'entreprise,** à moins que ces sujets ne soient expressément traités par un comité des risques distinct émanant du Conseil d'administration, ou par le Conseil lui-même.

Selon l'étude internationale menée par KPMG en 2014 sur la pratique des comités d'audit, à l'échelle mondiale, seuls **38 %** des comités d'audit ont la responsabilité première de surveiller les risques liés à la cybersécurité et **45 %** estiment que le comité d'audit (ou le Conseil d'administration) ne consacre pas suffisamment de temps à cette question. Lorsqu'il leur a été demandé de « noter la qualité des informations reçues concernant la cybersécurité », **25 %** des interrogés ont répondu qu'elle était bonne, **43 %** qu'elle était généralement bonne, mais que des problèmes se posaient régulièrement et **32 %** ont indiqué qu'elle nécessitait des améliorations – il s'agit du **premier sujet d'insatisfaction parmi les 11 domaines à risque** évalués dans le cadre de cette étude.

La cybersécurité et le **rôle grandissant** des comités d'audit

Les gouvernements du monde entier sont conscients de l'importance croissante de la cybersécurité, non seulement pour les institutions publiques et militaires, ainsi que les organisations gérant les infrastructures publiques clefs, mais également pour les entreprises du secteur privé.

Par exemple, en juillet 2013, le gouvernement britannique a invité les entreprises de l'indice FTSE 350 à participer à un « bilan de santé en matière de cybergouvernance ». Dans le cadre de ce contrôle, le Président de l'entreprise et le Président de son comité d'audit remplissent un questionnaire afin que soit évaluée la gestion de questions telles que la protection de la propriété intellectuelle et des données clients. Cette approche vise à s'assurer que la sensibilisation à la cybersécurité figure bien à l'ordre du jour du Conseil et non uniquement à celui du Directeur des Systèmes d'Information.

Aux États-Unis, la Securities and Exchange Commission (SEC) a publié des directives relatives à la présentation des questions de cybersécurité dans les rapports annuels. Elle y invite les entreprises à « présenter le risque de cyberincidents s'il est l'un des principaux facteurs rendant un investissement dans leur société spéculatif ou risqué ». **Les entreprises doivent considérer la probabilité de tels cyberincidents et l'ampleur du risque, ainsi que la pertinence de leurs contrôles de sécurité par rapport à leur secteur.** La déclaration des risques peut également inclure ceux liés à l'externalisation, aux cyberincidents matériels, aux incidents pouvant ne pas être détectés avant un certain temps, ainsi que la couverture par les cyberassurances.

Indirectement, un **risque pour tous**

Le risque demeure par ailleurs que des organisations considèrent présenter un faible intérêt pour les cybercriminels et sous-investissent par conséquent dans des mesures de protection.

L'édition 2013 de l'étude sur la cybercriminalité « Rapport Norton » estime que sur les 12 derniers mois, **la cybercriminalité dans le monde a coûté plus de 113 milliards de dollars US.** Les banques ne sont pas les seules cibles des hackers souhaitant dérober de l'argent, comme par exemple le réseau international de hackers qui a dérobé 45 millions de dollars US dans des distributeurs automatiques de billets dans plus de 20 pays. En réalité, **toutes les entreprises sont intéressantes** aux yeux des cybercriminels dont les motivations sont multiples.

Les cas de violation de données à caractère personnel se sont généralisés. En 2011, une entreprise a déclaré le vol de données à caractère personnel de plusieurs millions de ses clients par des hackers – un exemple d'incident médiatisé ayant des conséquences significatives en termes financiers mais aussi de réputation.

Si l'image traditionnellement répandue de l'espionnage correspond à ce que l'on voit dans les films de James Bond, il fait en réalité aujourd'hui partie du quotidien de nombreuses entreprises, que la menace provienne de leurs concurrents ou d'un État. Des données de propriété intellectuelle sont systématiquement ciblées et volées dans le cadre

Les banques ne sont pas les seules **cibles des pirates informatiques.**

de cyberattaques, et pas uniquement dans les secteurs de l'aéronautique et de la défense. En février 2013, l'entreprise de cybersécurité Mandiant a publié un rapport détaillé concernant une campagne de cyberespionnage qui a duré sept ans et touché 150 entreprises du monde entier. Nombreuses sont les campagnes de ce genre ayant été révélées par la communauté de la cybersécurité au cours de ces dernières années.
Dans certains cas, l'ampleur des vols de données et des dommages causés aux infrastructures informatiques est telle que les entreprises concernées se retrouvent proches de la faillite. En août 2012, une attaque destructrice a perturbé à elle seule plus de 30 000 ordinateurs de bureau dans une entreprise pétrolière du Moyen-Orient.

Les entreprises qui gèrent les infrastructures publiques clefs au Royaume-Uni sont des cibles potentielles d'Etats hostiles et de terroristes. **Les cyberattaques deviennent habituelles en cas de tensions internationales** – prenons pour exemple les attaques perpétrées contre les États-Unis, Israël, le Pakistan, l'Inde ou la Corée du Sud au cours de ces deux dernières années, toujours animées par des motivations politiques.

> La cybersécurité n'est pas simplement une question technique ; c'est une **approche intégrée destinée à prévoir et détecter les cyberincidents, à s'en prémunir et y réagir.**

Si les « hacktivistes », qui œuvrent à des fins politiques ou sociales ciblent également des entreprises, leur objectif est généralement d'impacter la réputation de ces dernières et d'encourager un changement de stratégie des entreprises plutôt que d'accéder à de précieuses données financières ou de perturber la production.

Le crime organisé utilise également ces cyberattaques afin de prendre les organisations en otage. À l'instar des bourses de valeurs, sites de paris en ligne et plateformes de négociation en ligne, tout domaine dont la survie dépend de sa disponibilité sur Internet est vulnérable aux attaques.

Les cyberattaques peuvent cibler **toute partie de l'activité d'une organisation** – pas uniquement ses opérations principales, mais également ses fonctions supports telles que les ressources humaines, ou encore les services financiers et de développement commercial. Aujourd'hui, en raison du niveau élevé d'automatisation, les ordinateurs non seulement nous apportent les technologies d'information nécessaires à notre travail, mais ils jouent également un rôle invisible de contrôle des processus industriels, des immeubles et de l'infrastructure.

Un pirate peut en outre accéder aux systèmes d'une organisation par le biais de l'infrastructure informatique de l'un de ses clients ou fournisseurs, ou encore au moyen de l'ordinateur ou du téléphone mobile personnels de l'un de ses employés.
Les organisations traversant une phase de restructuration (par exemple, dans le cadre d'une acquisition ou d'une fusion) peuvent être particulièrement vulnérables en raison de la sensibilité au marché, de problèmes liés au moral du personnel, de reconfigurations du réseau et du recours à des conseillers externes.

Les efforts doivent être concentrés sur la **recherche d'une plus grande rapidité d'adaptation.**

Trouver le bon équilibre entre **sécurité et coût**

La sécurité absolue n'existe pas. Un adversaire disposant des ressources et de la détermination nécessaires finira certainement par trouver un moyen de mettre en échec les meilleures mesures de sécurité, que leur point faible soit lié à la sécurité des données, à la sécurité physique ou encore aux personnes. **Chaque organisation doit trouver l'équilibre entre la défense de ses principaux actifs face à des cyberattaques et le coût des mesures de cybersécurité.**

Les cybermenaces doivent être intégrées à la politique de gestion des risques et de gouvernance des organisations et leur cartographie des risques doit refléter le risque éventuel d'une cyberattaque contre ses actifs ou processus clés.

Nombre d'organisations élaborent des **scénarii d'attaque** afin de tester leur capacité à réagir face à une cyberattaque. Ces scénarii comprennent une description des circonstances de l'attaque ainsi que des motivations, des intentions et des techniques de l'éventuel pirate.

Il faut encourager le Conseil d'administration à imaginer tous les scénarii possibles et à être prêt à en appliquer plusieurs afin de tester les différents aspects de la cybersécurité de leur organisation.

À quoi ressemble un **système de cybersécurité efficace ?**

Il est important de partir sur de bonnes bases – des mesures de sécurité techniques telles que **l'utilisation de logiciels antivirus et la mise en place de pare-feu** pour protéger les réseaux de l'entreprise, à l'élaboration d'une politique relative aux cyberincidents, en passant par l'organisation d'une vaste campagne de formation et de sensibilisation des utilisateurs. Ces mesures n'arrêteront pas toutes les attaques mais permettront d'en bloquer un certain nombre.

Cette préconisation relève de la gestion des risques liés à l'information. La responsabilité du Conseil d'administration en la matière est d'identifier les ressources informatiques clefs et de gérer les risques qu'elles induisent dans l'organisation.

Les programmes visant à accroître la cybersécurité doivent s'appuyer sur une vision globale de la sécurité tenant compte à la fois de l'aspect humain et culturel, ainsi que des processus de l'organisation et des mesures techniques de sécurité. La cybersécurité n'est pas simplement une question technique ; c'est une approche intégrée destinée à prévoir et détecter les cyberincidents, à s'en prémunir et y réagir.

Le personnel peut involontairement représenter la plus grande cause de vulnérabilité – sa formation et sa sensibilisation sont par conséquent indispensables à la mise en place des comportements adéquats. Une approche optimale de ces pratiques comprend par ailleurs une structure de gouvernance qui contrôle l'efficacité du système de cybersécurité et une organisation de renseignement pistant les cybermenaces et aidant à façonner les décisions en matière de risque.

Notre perception du sujet : les **perspectives** d'aujourd'hui – et de demain

Le nombre d'attaques menées par des organisations sophistiquées du crime organisé visant à accéder à de précieuses données connaît une croissance significative. Il en va de même des « chevaux de Troie » compromettant des sites officiels, afin d'inciter les utilisateurs à télécharger par inadvertance des logiciels malveillants, donnant ainsi aux pirates accès aux réseaux de l'entreprise.

La tendance est également à l'espionnage d'État : des intrusions sur le long terme peuvent entraîner différents problèmes tels que le vol d'une quantité significative de données de propriété intellectuelle. Bon nombre d'organisations sous-estiment largement l'ampleur de ce problème. Ceci provient d'une réticence à la fois à attribuer directement des attaques à des États-nations et à dénoncer de telles atteintes à la sécurité lorsqu'elles sont identifiées, le cas échéant.

Le grand défi de demain, quelles que soient les nouvelles menaces, consiste à protéger l'éventail toujours plus large des outils

technologiques, notamment les appareils mobiles. Il faudra également certainement se pencher sur la question de savoir comment protéger au mieux les services de « cloud computing ». Enfin, la militarisation croissante du cyberespace pourrait aussi poser problème – elle pourrait en effet y générer des perturbations, voire même en diminuer la valeur pour les autres utilisateurs, tels que les entreprises et leurs clients.

↗ **Protéger** la valeur

Il existe un grand nombre de moyens de renforcer de manière indépendante les aptitudes d'une entreprise à la cybersécurité. Une **appréciation de la maturité des systèmes informatiques** (Cyber Maturity Assessment), par exemple, permet d'évaluer de manière systématique la cybersécurité de l'entreprise – de ses mesures techniques de sécurité à sa gestion globale des risques relatifs aux systèmes, en passant par son cadre de gouvernance, dont dépend la cybersécurité.
Les **processus de sécurité et les contrôles individuels** peuvent également être évalués, testés et certifiés. Si l'ensemble de ces mesures peut renforcer la confiance vis-à-vis de l'approche de la cybersécurité adoptée par l'organisation, c'est au Conseil d'administration qu'il revient en fin de compte d'étudier et de définir le niveau de risque acceptable pour son activité.

En raison de l'évolution rapide de la nature des cybermenaces, les entreprises doivent procéder à des investissements, à la fois stratégiques et financiers, afin de conserver une longueur d'avance sur les criminels. Une cybersécurité plus efficace ne passe pas forcément par la création d'obstacles supplémentaires ; il est plutôt nécessaire d'encourager une plus grande rapidité d'adaptation, en fournissant les ressources nécessaires pour palier les menaces au fur et à mesure qu'elles évoluent. Il est également important d'être capable d'identifier et prendre en charge toute violation des moyens de défense afin de limiter les dommages.

Certaines entreprises prennent cette question très au sérieux et investissent afin de comprendre les risques relatifs à la cybersécurité et d'adopter une approche pragmatique de l'atténuation de ces risques. D'autres, cependant, n'y prêtent pas d'importance et prennent par conséquent un risque considérable pour la valeur de leur entreprise au sens large, s'exposant notamment à la perte de propriété intellectuelle au profit de la concurrence, aux risques de détérioration de leur réputation aux yeux de clients fidèles et même à des pertes financières.

ÉLÉMENTS **À RETENIR**
en matière de cybersécurité pour les comités d'audit

Les cybermenaces doivent être prises en compte dans le cadre du processus de gestion des risques de l'entreprise et le comité d'audit doit vérifier que cette dernière a procédé à :

- **l'identification des informations critiques et des actifs stratégiques qu'elle souhaite protéger** d'une cyberattaque – ses biens les plus précieux – qu'il s'agisse de données financières, de données opérationnelles, de données concernant ses employés ou clients, ou encore de propriété intellectuelle ;
- **la définition des processus de renseignement** nécessaires à l'appréhension de la menace pour les actifs de la société, notamment au regard de ses activités à l'étranger ;
- **la mise en place d'une démarche pour identifier et convenir du niveau de risque** que l'entreprise peut tolérer au titre d'une information stratégique donnée ;
- **la mise en place des contrôles nécessaires pour prévenir,** se protéger et réagir face à une cyberattaque, notamment la gestion des conséquences d'un incident de cybersécurité ;
- **l'élaboration d'un processus de vérification de l'efficacité de ses contrôles** en matière de cybersécurité, y compris, le cas échéant, une procédure de test, de révision et d'audit indépendant ;
- **la mise en œuvre d'un programme d'amélioration permanente** ou, si nécessaire, de transformation, afin de s'adapter à l'évolution des cybermenaces – au moyen d'indicateurs appropriés.

Contacts

Patrick-Hubert Petit
Associé – Président de l'Audit Committee Institute France

Jean-Marc Discours
Associé – Responsable de l'Audit Committee Institute France

Jean-Marc Lefort
Associé – Forensic

Stella Vitchenian
Directeur - Audit

Site : www.audit-committee-institute.fr
E-mail : fr-auditcommittee@kpmg.fr

À propos de l'ACI

L' Audit Committee Institute, sponsorisé par KPMG, est un forum d'échanges dédié aux membres de comité d'audit. Il a été conçu pour apporter aux membres de comité d'audit des informations, outils et techniques les aidant à remplir la mission liée à leur fonction.

L' Audit Committee Institute communique à travers le monde avec les responsables de comité d'audit depuis 1999.

L' Audit Committee Institute France propose à ses membres :

- un site internet (www.audit-committee-institute.fr) conçu pour donner aux membres de comité d'audit un accès permanent aux bonnes pratiques et à des outils conçus pour améliorer le fonctionnement des comités d'audit ;
- des rencontres bi-annuelles permettant aux membres de comité d'audit d'échanger sur des sujets d'actualité avec leurs pairs ;
- des publications sur le gouvernement d'entreprise telle que l'étude internationale annuelle, « La pratique des comités d'audit en France et dans le monde », publiée chaque année depuis 2006.

À propos de cette publication

Cette publication est une traduction en français du document « Cyber Security for audit committees » publié en anglais par l'Audit Committee Institute en janvier 2014.

 Imprimé en France. Mai 2014. Conception / Réalisation : KPMG (Markets) - Studio KPMG - Xerox General Services. Crédit photos : Shutterstock.