Cybersécurité des conseils d'administration :

Remplacer les préférences à risque par une politique raisonnée

Dans un contexte où les attaques cybercriminelles se développent et sont de plus en plus sophistiquées, les membres du conseil d'administration doivent faire de la sécurité de leurs communications une priorité. Il faut que les conseils d'administration intègrent à leurs politiques des stratégies et des réglementations en matière de cybersécurité, pour bien comprendre ce qu'il est acceptable ou non de communiquer et de télécharger, avec qui et, surtout, de quelle façon. Les membres du conseil doivent donner l'exemple et veiller au respect continu des politiques de sécurité par des formations et des audits.

Le risque lié à la cybersécurité n'est pas un nouveau concept pour les conseils d'administration en 2017. La menace de voir un smartphone professionnel tomber entre de mauvaises mains ou le fait de penser, à tort, que les courriels et le stockage des données internes sont sécurisés et la protection par mot de passe synonyme de sécurité ne sont pas nouveaux non plus.[1]

Les unes des journaux se font l'écho des risques juridiques, concurrentiels ou de dégradation de la réputation des violations ou fuites de données. En octobre 2016, la fuite d'un courriel et d'une présentation du conseil d'administration de Salesforce a révélé au monde entier la liste des cibles potentielles d'acquisition de l'entreprise.[2] En mars 2017, les autorités ont arrêté un Lituanien qui a escroqué plus de 100 millions de dollars

Diligent

1 « Cybermenaces et sécurité du conseil d'administration : trois idées fausses néfastes pour la sécurité de la salle du conseil »

2 http://www.businessinsider.com/leaked-salesforce-email-adobe-acquisition-list-2016-10

à deux entreprises technologiques américaines. Son mode d'attaque : envoyer des communications électroniques qui ressemblaient aux messages d'un fabricant chinois bien connu.[3]

Les législateurs et les organismes de régulation réagissent à ces menaces qui s'intensifient. Par exemple, l'État de New York exige désormais que toutes les sociétés de services financiers exerçant leurs activités dans l'état (et toutes les entreprises faisant affaire avec elles) aient des plans de cybersécurité couvrant tout, des journaux d'audits à l'accès aux données des clients, avec approbation du conseil.[4] Récemment, des actions en justice impliquant Target et Wyndham Worldwide ont présenté comme une violation potentielle de la responsabilité fiduciaire des membres du conseil d'administration l'échec de la mise en œuvre des contrôles adéquats de protection des données.

C'est pourquoi les membres du conseil d'administration ont placé la sécurité de l'entreprise au centre de leurs préoccupation. Pourtant les communications des membres du conseil ne reflètent pas cette prise de conscience. Selon une enquête réalisée en 2017 par NYSE Governance Services, 92 % des plus de 380 membres de conseils d'administration interrogés ont exprimé leur préférence pour les courriels personnels. Près de 60 % ont reconnu qu'ils envoyaient régulièrement des communications liées aux conseils d'administration par leur messagerie électronique personnelle, notamment Google, Yahoo et Hotmail. Décuplant encore davantage les vulnérabilités de sécurité, 22 % ont répondu qu'ils avaient l'habitude de stocker les documents de conseil sur des disques durs personnels ou externes.

Malgré une sensibilisation et une formation accrues, les conseils d'administration ont des difficultés à se tenir informés des problèmes de cybersécurité et des risques, dans l'entreprise et dans leurs propres activités. Dans une enquête réalisée en 2017 par la Harvard Business School et la Women Corporate Directors Foundation, seuls 24 % des membres de conseil d'administration ont répondu qu'ils considéraient la cybersécurité de leurs propres activités « supérieure à la moyenne ou excellente ».[6]

Par où peuvent commencer les conseils d'administration pour combler ces lacunes ? En haut de la liste se trouvent les statuts et les politiques de gouvernance de l'entreprise.

INTÉGRER LES COMMUNICATIONS SÉCURISÉES À LA GOUVERNANCE DES CONSEILS D'ADMINISTRATION

Les politiques et les statuts des conseils d'administration couvrent beaucoup de choses (par exemple, les comportements financiers, l'acceptation de cadeaux, la confidentialité et les publications). Ces politiques comprennent souvent des règles en matière de communication, qu'il s'agisse de ce qui peut être communiqué entre les membres du conseil (par exemple, pas de propositions commerciales ni de sondages d'opinion) ou de la façon dont ces communications doivent s'effectuer avec la presse et le public.

Dans le monde d'aujourd'hui où les risques et les conséquences s'intensifient, la cybersécurité doit faire partie de ces politiques. Les réglementations de l'État de New York recommandent que les politiques couvrent notamment l'accès aux données et leur confidentialité, la gestion des identités, la surveillance des systèmes et réseaux, la continuité des opérations.[7]

Que devez-vous envisager pour votre propre politique lors de votre prochain comité d'audit, de votre prochaine réunion de gouvernance ou réunion de votre conseil d'administration ? En s'appuyant sur son expérience avec des milliers de conseils d'administration dans le monde entier, Diligent recommande d'agir comme suit :

RECEVOIR ET ENVOYER DES MESSAGES

Membres du conseil, conseiller juridique, cadres supérieurs : qui devrait envoyer et recevoir des communications du conseil d'administration et qui ne devrait pas ? Précisez cela dans vos politiques, avec tous les détails nécessaires, et établissez des politiques concernant l'envoi et la réception de pièces jointes, la conservation et l'archivage des messages ainsi que l'effacement à distance des communications sur un appareil perdu ou volé. Encouragez l'adoption de technologies comme Diligent Messenger qui « boucle la boucle » contre les messages envoyés par mégarde, par exemple, le remplissage automatique de la mauvaise adresse électronique dans le champ de destinataire d'un courriel.

Étant donné la croissance des courriels de hameçonnage dans les cyberattaques, les politiques doivent également interdire explicitement les réponses de parties non autorisées. Même les applications de messagerie de conseil les plus sécurisées pourraient ne pas être 100 % inattaquables face aux techniques de piratage de plus en plus sophistiquées.

Le pirate lituanien qui a escroqué les entreprises technologiques pour se faire envoyer 100 millions de dollars n'est qu'un exemple. Une autre stratégie d'attaque récente consiste à demander aux victimes d'ouvrir un courriel en détournant « l'adresse d'envoi » d'un contact de confiance. Le destinataire est alors redirigé vers un écran de connexion à Gmail frauduleux (mais convaincant). Dans ce cas, les pirates s'emparent du nom et du mot de passe pour accéder à la boîte de réception des courriels du destinataire.[8]

Enfin, définissez précisément ce que représentent les « communications officielles du conseil d'administration ». Pour certains éléments, tels que les procès-verbaux, l'exigence de confidentialité est évidente, mais qu'en est-il des convocations aux réunions et des ordres du jour ou encore des courriels individuels échangés entre membres du conseil ? Clarifiez tous ces points dans votre politique de communications sécurisées.

GÉRER LES PIÈCES JOINTES

Lorsqu'un salarié de Boeing a transféré une feuille de calcul à son épouse pour l'aider à résoudre des problèmes de mise en page, il a en même temps exposé les noms, dates de naissance et numéros de sécurité sociale de 36 000 employés à un risque de sécurité.[9]

En plus d'établir une liste des choses à faire et à ne pas faire pour envoyer et recevoir des messages, votre politique de communications doit aborder la transmission de fichiers électroniques. Les fichiers liés aux activités du conseil ne doivent jamais être envoyés par des méthodes non sécurisées ou non chiffrées et ne doivent être transmis qu'aux utilisateurs autorisés.

3 https://www.theguardian.com/technology/2017/mar/22/phishing-scam-us-tech-companies-tricked-100-million-lithuanian-man

4 http://fortune.com/2017/03/01/cyber-regulations-new-york

5 https://iapp.org/news/a/cybersecurity-in-the-boardroom-the-new-reality-for-directors/

6 https://hbr.org/2017/02/why-boards-arent-dealing-with-cyberthreats

7 https://www.governor.ny.gov/sites/governor.ny.gov/files/atoms/files/Cybersecurity_Requirements_Financial_Services_23NYCRR500.pdf

8 http://fortune.com/2017/01/18/google-gmail-scam-phishing/

9 http://www.bizjournals.com/seattle/news/2017/02/28/boeing-discloses-36-000-employee-data-breach.html

Votre politique doit également préciser les types de fichiers que les membres du conseil peuvent et ne peuvent pas télécharger. Dans le contexte actuel des hameçonnages, logiciels malveillants et logiciels gratuits et shareware suspects, « ce qui peut apparaître comme un téléchargement inoffensif à des fins professionnelles peut facilement introduire un virus dans votre réseau et exposer des données commerciales sensibles », ont écrit des experts en cybersécurité chez Sentek Global dans le magazine *Entrepreneur*.[10] L'équipe interne chargée de la cybersécurité ou celle de votre fournisseur devrait être en mesure de vous conseiller dans ce contexte.

ARCHIVER ET CONSERVER LES COMMUNICATIONS

L'enregistrement des procès-verbaux ou d'un document de fusions-acquisitions sur le disque dur d'un ordinateur portable ou la conservation d'archives importantes de courriels sur plusieurs années peuvent représenter des « piratages de commodité » rapides pour un membre du conseil en déplacement. Néanmoins cette pratique expose votre conseil d'administration à une vulnérabilité importante si jamais les appareils sont perdus ou volés ou si jamais une boîte de réception de courriels est compromise par des personnes malveillantes.

Précisez dans votre politique de conseil d'administration les types de documents que les membres du conseil sont autorisés à télécharger, ainsi que les smartphones, tablettes, ordinateurs et logiciels qu'ils peuvent utiliser. Étant donné que les appareils et boîtes de réception personnels sont désormais soumis à l'administration de la preuve électronique, et qu'un membre du conseil risque une citation à comparaître personnelle si la société va devant la justice, les réglementations sur les communications du conseil doivent couvrir tous les angles pertinents. Comment ces appareils doivent-ils être sécurisés ? Les membres du conseil devront-ils supprimer les fichiers ou les anciens courriels après un certain temps ?

Cette partie de votre politique devra également apporter des conseils dans le cas où les choses tournent mal. Dans le cas de Boeing, la société a mené une enquête scientifique sur les deux appareils pour vérifier que toutes les copies connues du fichier avaient été détruites, puis a transmis une lettre de notification à toutes les parties concernées (avec une proposition de deux années de surveillance gratuite de solvabilité) et une formation supplémentaire des employés sur la gestion des données personnelles.

À qui doivent être signalés les incidents ? Par quels moyens les données et les appareils doivent-ils être « effacés » et comment pourrez-vous prouver que ces mesures ont été appliquées ?

Votre équipe interne chargée de la cybersécurité ou celle de votre fournisseur doit être en mesure de vous guider sur les détails techniques spécifiques, tels que le stockage sécurisé, le chiffrement des données, la vérification d'identité et le contrôle d'accès des administrateurs.

ENCOURAGER L'ADHÉSION

La mise en place des règles adéquates est la première étape et peut être effectuée lors de votre prochaine réunion du comité ou du conseil. Leur bonne application sera ensuite un processus continu.

Pour augmenter vos chances de réussite, adoptez une solution technologique prête à fonctionner qui tienne compte de vos politiques. Diligent recommande un système de messagerie en boucle fermée, sécurisé et contrôlé qui s'intègre à un système existant de portail pour conseils d'administration sécurisé. Recherchez un chiffrement des données et une authentification multifacteur (renforçant les mots de passe par une méthode secondaire pour confirmer l'identité) sur tous les appareils.

« Ce que les membres du conseil d'administration risquent de perdre d'un point de vue pratique en n'utilisant plus leur messagerie personnelle, ils le récupèreront au niveau de la cybersécurité, de l'atténuation du cyber-risque et de la limitation de la responsabilité personnelle» déclare Dottie Schindlinger, évangéliste des technologies de gouvernance chez Diligent.

Pour aider les membres du conseil à éviter de céder à la tentation des solutions de contournement, faites en sorte que les solutions technologiques que vous proposez soient simples et sans stress. Elles doivent :

- avoir une installation intuitive, par exemple, télécharger une application plutôt que de nécessiter plusieurs étapes inhabituelles ;
- être facile à utiliser ;
- permettre la synchronisation entre les smartphones, tablettes et ordinateurs portables utilisés par les membres du conseil pour accéder à leurs informations en déplacement.

Quelle que soit la solution que vous choisissez, son utilisation régulière et correcte sera la clé de sa réussite. Prenez le temps de former les membres du conseil aux nouvelles technologies par des formations pratiques. (Dans l'étude réalisée par NYSE auprès de membres de conseil d'administration d'entreprises cotées en bourse, seulement 9 % des personnes interrogées ont déclaré qu'elles avaient dû suivre la même formation à la cybersécurité que les employés.) Renforcez l'adoption grâce à des remises à niveau, ainsi que des audits et des vérifications qui impliquent les directeurs généraux chargés de la sécurité des informations, de la conformité et de l'informatique.

Dans un contexte où l'on s'attend à ce que le hameçonnage ciblé soit de plus en plus précis et perfectionné, où le sabotage de données augmente comme une menace et où les attaques des États-nations et de « l'Internet des objets » compliquent la situation dans l'ensemble,[11] la cybersécurité poursuit son ascension pour devenir une priorité organisationnelle. En même temps, les conséquences de l'incapacité à rester au niveau, sur la réputation et la compétitivité, sont de plus en plus préoccupantes. Selon Matteo Tonello de The Conference Board, la déficience des processus de gestion des risques et du contrôle ainsi que de la sécurité informatique est « de plus en plus perçue comme de simples symptômes d'une « mauvaise » ou « insuffisante » culture du risque. »[12]

Faire preuve de diligence en matière de cybersécurité est impératif et commence au domicile. Étant donné les menaces et les risques grandissants dans l'environnement professionnel d'aujourd'hui et le rôle croissant des conseils d'administration dans la surveillance de la cybersécurité, les membres du conseil ne peuvent pas se permettre d'attendre pour veiller à ce que leurs propres communications respectent les meilleures pratiques de cybersécurité. Ajouter une messagerie sécurisée à leurs recommandations et à leurs politiques relatives aux communications est un point de départ.

10 https://www.entrepreneur.com/article/272847

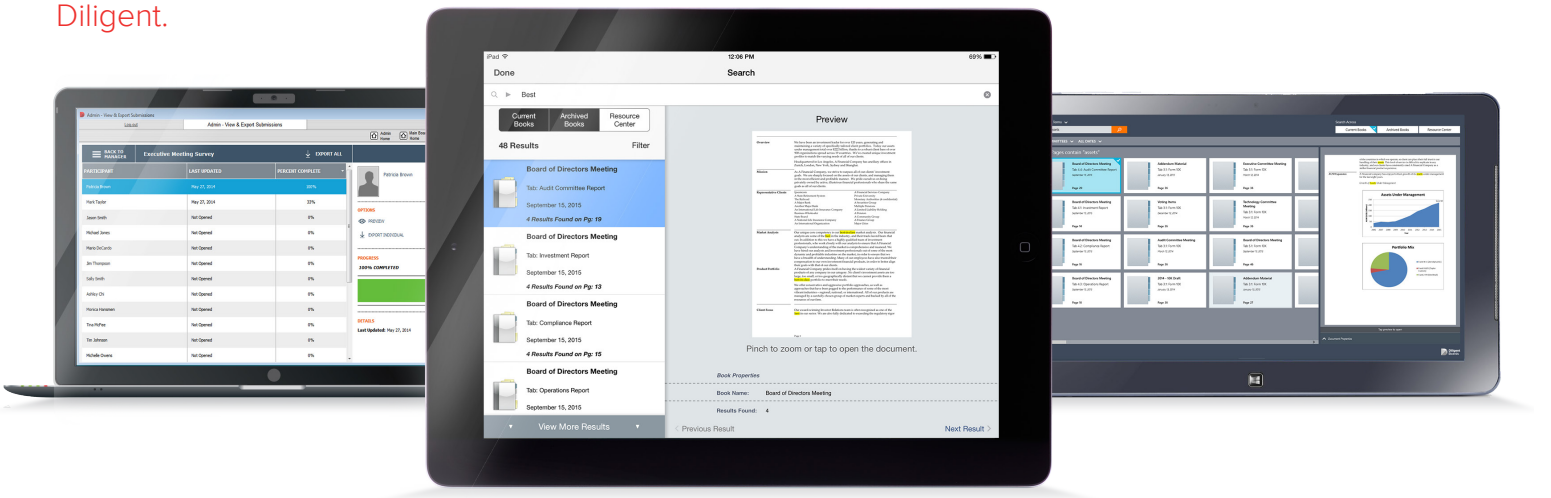
11 http://www.insurancejournal.com/news/international/2017/01/11/438549.htm

12 https://corpgov.law.harvard.edu/2017/02/15/risk-management-and-the-board-of-directors-4/

Diligent

Exploiter la puissance de l'information. En toute sécurité.

Pour aider les organisations les plus puissantes du monde à exploiter en toute sécurité le pouvoir de l'information et de la collaboration, Diligent fournit aux conseils d'administration et équipes de gestion tout pour leur permettre de prendre de meilleures décisions. Plus de 4 700 clients dans plus de 70 pays comptent sur Diligent pour accéder sans délai aux informations les plus urgentes et confidentielles et aux outils pour en discuter, collaborer et les examiner avec les principaux décideurs. Diligent Boards accélère et simplifie la création et la distribution des documents de conseil sur les iPad, les appareils Windows et les navigateurs. Parallèlement, Diligent Boards offre des avantages pratiques comme la réduction des coûts de production, une contribution au développement durable et l'accélération des procédures administratives et informatiques pour les leaders du monde entier. Rejoignez les plus grands. Choisissez Diligent.



Télécharger dans l'App Store · Obtenir sur Microsoft · DISPONIBLE SUR Google Play · AICPA SOC · ISO 27001 CERTIFIED BY BRIGHTLINE

Pour de plus amples informations ou pour obtenir une démonstration, contactez-nous aux coordonnées suivantes :

Tél. : +33 (0)1 56 60 58 58
Courriel : info@diligent.com
Visitez : www.diligent.com