Préface

Administrateurs et dirigeants sont maintenant au cœur des problématiques de cybersécurité. C'est ma conviction ; c'est mon expérience acquise en ayant lancé en 2005 une des premières sociétés de cybersécurité, et de nombreux dirigeants. C'est ma conviction de dirigeant d'une entreprise de défense particulièrement exposée à ces risques, mais aussi active dans le développement des nouvelles stratégies de protection.

Faisons de cette expertise un moteur de différenciation de nos entreprises et de la France *a safe place to do business*. C'est en cela que cet ouvrage écrit par Marie de Fréminville prend toute son importance.

Il rassemble cinq années de travaux et d'échanges entre experts et dirigeants, entre acteurs étatiques et industriels qui forgent notre conviction que la question de la cybersécurité ne peut plus rester confinée à des cercles de *geeks*, mais qu'elle est devenue un véritable enjeu de résilience économique.

La question est à l'évidence beaucoup plus large et la gouvernance de l'entreprise doit l'appréhender dans toutes ses dimensions : résilience économique, vulnérabilité des stratégies d'entreprise étendue, protection des clients, problématiques humaines, évolution des infrastructures, politique d'assurances, gestion de crise, etc.

La direction générale et son conseil d'administration doivent non seulement en prendre conscience, mais agir chacun selon sa responsabilité, pour mettre en place les organisations nécessaires, la gouvernance des risques, mais aussi les dispositifs de protection de l'entreprise. C'est cet « appel aux consciences » qui doit résonner

auprès du lecteur, chacun devant ensuite trouver des solutions adaptées : cet ouvrage vous apportera des pistes de solutions et vous éclairera sur les risques à prendre en compte pour éclairer vos décisions.

Comme on dit dans la relève de quart : maintenant, à vous le soin…

Hervé GUILLOU
Président-directeur général
Naval Group

Avant-propos

C'est l'organisation de tables rondes avec HEC Gouvernance et d'ateliers avec le cercle suisse des administratrices, qui a été le point de départ de cet ouvrage à destination des décideurs : dirigeants et administrateurs d'entreprises, d'organisations publiques, de fondations ou d'associations.

La protection des données stratégiques de l'entreprise et de ses systèmes d'information relève de la responsabilité des administrateurs et dirigeants, ainsi que des décideurs de l'entreprise, au sein des directions opérationnelles et fonctionnelles, à l'intérieur comme à l'extérieur.

Les propos des différents intervenants de ces tables rondes ont été repris dans cet ouvrage.

En octobre 2016, « Comprendre et prévenir les cyberrisques : une priorité » :

– Hervé Guillou, président-directeur général de Naval Group ;

– Alain Juillet, directeur du renseignement à la DGSE, haut responsable à l'intelligence économique au SGDSN et président du CDSE (Club des directeurs de sécurité et de sûreté des entreprises) ;

– Guillaume Poupard, directeur général de l'ANSSI (Agence nationale de la sécurité des systèmes d'information) ;

– Alain Bouillé, président du CESIN (Club des experts de la sécurité de l'information et du numérique) ;

– Alexandre Montay, secrétaire général du METI (Mouvement des entreprises de taille intermédiaire).

En juin 2017, « Le cyberrisque : un sujet à gouverner » :

– Yves Bigot, directeur général de TV5 Monde ;

– Brigitte Bouquot, présidente de l'AMRAE (Association pour le management des risques et des assurances de l'entreprise) ;

– Frédérick Douzet, professeure des universités à l'IFG (Institut français de géopolitique) de l'université Paris 8 et titulaire de la chaire Castex de Cyberstratégie ;

– Solange Ghernaouti, professeure en sécurité de l'information à l'UNIL (université de Lausanne) et directrice du Swiss Cyber Security Advisory and Research Group ;

– Philippe Gaillard, directeur risques techniques et cyber d'Axa France ;

– Alain Robic, *Partner Enterprise Risks and Services* chez Deloitte - Sécurité des systèmes d'information.

En décembre 2018, « Cybercriminalité et protection des données personnelles : quelles bonnes pratiques pour le conseil d'administration et les dirigeants ? » :

– Isabelle Falque-Pierrotin, présidente de la CNIL (Commission nationale de l'informatique et des libertés) depuis 2011, élue en 2017 à Hong Kong, présidente de la conférence mondiale des autorités de protection de données (*Conference of Data Protection and Privacy Commissioners*) ;

– Philippe Castagnac, président du conseil de gérance de Mazars, organisation internationale, intégrée et indépendante, spécialisée dans l'audit, le conseil et les services comptables, fiscaux et juridiques ;

– Annick Rimlinger, directrice générale du CDSE (Club des directeurs de sécurité et sûreté des entreprises), membre fondateur du Cercle K2 et membre du conseil d'administration de Hack Academy ;

– Éliane Rouyer, administratrice indépendante, présidente du comité d'audit et membre du comité des rémunérations de Legrand, administratrice indépendante de Vigéo Eiris.

Je remercie l'ensemble de ces intervenants pour leurs contributions et leur soutien, ainsi que Marc Triboulet (mon coéquipier d'HEC Gouvernance, avec lequel ce cycle de tables rondes a été initié).

La formation que j'ai développée au sein du groupe Airbus pour les administrateurs et dirigeants de filiales, les travaux réalisés pour ces conférences, ainsi que les échanges à l'occasion de ces tables rondes, ont été complétés par des travaux de recherche menés depuis cinq ans, la participation à des groupes de travail (la stratégie

cybersécurité de la Suisse, par exemple), l'accompagnement de plusieurs start-up dans le domaine de la cybersécurité, la mise en place de formations, l'intervention auprès d'universités, d'entreprises, ou de prestataires de services, la mise en place de cartographies des risques, la définition et le déploiement de dispositifs pour améliorer la conformité au RGPD (Règlement général sur la protection des données), sans oublier la mise en œuvre de programmes cyber au travers d'entreprises, associations, fondations et organismes publics.

Introduction

Performance financière et performance cyber

Pourquoi ne pas évaluer la performance cyber des entreprises, comme le sont la performance financière et la performance extra-financière (gouvernance et RSE – responsabilité sociale et environnementale) ?

Pourquoi ne pas certifier la performance cyber des entreprises, comme l'est la performance financière de l'entreprise *via* les commissaires aux comptes, dont l'intervention est obligatoire pour les entreprises d'une certaine taille ?

Malgré quelques évolutions, la grande majorité des actionnaires, et donc le conseil d'administration et les dirigeants, s'intéressent en priorité à la performance financière de l'entreprise.

Pourtant, l'ère numérique introduit des bouleversements dans l'entreprise, et au sein de son écosystème. En effet, le « tout numérique » concerne toutes les parties prenantes, l'administration, les services publics et les infrastructures nationales et internationales, la défense et les services de renseignements.

Nous sommes arrivés à un stade de non-retour, qui offre d'importantes opportunités, mais qui est également une source de fragilité et de risques majeurs, notamment parce que les acteurs de la menace cyber se professionnalisent et disposent de moyens importants pour frauder, espionner, saboter.

Les risques pour l'entreprise sont systémiques : les actionnaires sont exposés financièrement et les administrateurs, en charge de définir sa stratégie et de veiller à sa pérennité, sont exposés juridiquement, s'ils ne s'informent pas sur la qualité de la sécurité des données et de la protection du système d'information et s'ils ne s'assurent

pas de la mise en place d'une organisation, de procédures et d'outils pour une cybersécurité de bon niveau.

Le risque zéro n'existe pas, mais la négligence d'un conseil d'administration lui serait reprochée, si aucune action n'était engagée dans le domaine de la cybersécurité de l'entreprise et si les attaques avaient des conséquences significatives pour son bon fonctionnement, sa rentabilité et sa réputation.

La performance financière ne devrait donc plus être la seule priorité. La performance financière et la performance cyber devraient être maintenant les deux priorités des organes de gouvernance des entreprises.

Faut-il par conséquent réinventer l'organe de gouvernance désigné par les actionnaires, à savoir ses compétences, son fonctionnement, son agenda et ses partenaires ?

Depuis cinquante ans, nous vivons un tsunami technologique :

– 1970 : *mainframe* ;

– 1980 : PC (ordinateur personnel) et client/serveur ;

– 1990 : Internet et e-commerce ;

– 2000-2010 : mobile et *e-Cloud* ;

– 2010-2020 : Internet des objets et intelligence artificielle ;

– 2020-2030 : *quantum computing* et *blockchain*.

Le monde numérique est sans frontières, immatériel, les menaces sont invisibles.

Le digital et les nouvelles technologies associées transforment le fonctionnement des entreprises et les *business models*.

Les principaux risques cyber sont des risques de dysfonctionnement du processus industriel ou commercial, des risques financiers mais aussi des risques de perte d'informations confidentielles considérables (informations stratégiques, informations personnelles) et touchent différents secteurs : hôpitaux, voitures autonomes, banques, opérateurs télécoms, énergie, etc., avec des conséquences humaines potentielles.

Selon une étude menée aux États-Unis par la *National Archives and Records Administration* en 2018, 93 % des entreprises ayant perdu leurs données pendant dix jours ou plus ont déclaré faillite dans l'année de la catastrophe et la moitié (50 %) ont déposé leur bilan immédiatement après l'attaque.

La question n'est pas « quand serons-nous attaqués ? », mais « que faire pour protéger l'entreprise au maximum, que faire en cas d'attaque, que faire pour restaurer les systèmes aussi rapidement que possible ? ».

Le cyberrisque fait partie intégrante de l'entreprise et également des organisations personnelles (chacun est concerné à titre individuel et en tant que membre d'une organisation). Il ne s'agit pas seulement d'un risque technique.

L'homme est le maillon faible (et le maillon fort) de toute la chaîne de sécurité.

Cet ouvrage ne traite pas des outils (matériel, logiciels, serveurs, architecture), mais des organisations, des processus et des comportements, sans lesquels l'entreprise ne peut améliorer sa performance, sa sécurité, la gestion des incidents ou des crises, et sa résilience.

Il s'agit pour l'entreprise d'exercer sa responsabilité numérique et de maintenir ou d'améliorer la confiance de ses parties prenantes : clients, fournisseurs, partenaires et investisseurs.

Il y a trente ans seulement, j'ai vécu l'arrivée des ordinateurs individuels (les ordinateurs et le traitement de texte existaient, mais n'étaient pas déployés dans l'entreprise), la numérisation des opérations financières (comptabilité, comptabilité analytique, relations banques et gestion de trésorerie, déclarations fiscales, outils de reporting et consolidation comptable et de gestion, relations financières avec les clients et fournisseurs), mais aussi la numérisation de la gestion des ressources humaines (paies, déclarations sociales, recrutement, formation), de la communication interne et externe, notamment avec l'arrivée des réseaux sociaux, de la production (usines connectées et entreprise étendue), du marketing et des ventes bien sûr, comme de la logistique.

Toutes les fonctions de l'entreprise sont maintenant concernées, ainsi que les relations avec l'ensemble des parties prenantes : clients, fournisseurs, prestataires de services, sous-traitants, actionnaires (investisseurs individuels, fonds d'investissements), conseil d'administration, auditeurs, employés, filiales, *proxy advisers* (conseillers en gouvernance qui commentent publiquement les propositions faites par les sociétés en vue de leurs assemblées générales).

L'entreprise est entièrement numérisée : ses données, ses opérations, ses comptes, ses processus sont immatériels ; ses communications internes et externes, ses produits sont connectés.

Les organisations et habitudes de travail se sont modifiées, les compétences ont évolué, les outils se sont transformés, la classification des documents et des personnes est parfois (souvent ?) tombée dans les oubliettes.

L'entreprise a pu s'internationaliser, grâce aux moyens de communication ultra-rapides. Nous parlons aussi bien à l'entreprise d'en face qu'à celle des États-Unis ou de la Chine : seul le décalage horaire est incompressible.

L'entreprise partage ses données avec ses clients, fournisseurs, employés, actionnaires, filiales, etc. Le tout numérique donne des opportunités aux entreprises de créer de nouveaux business, de nouveaux produits et services et de nouveaux clients, d'optimiser leurs organisations, de réduire leurs coûts, d'améliorer leurs processus internes et externes, avec leurs fournisseurs, prestataires, sous-traitants, investisseurs, clients, en fonction du secteur d'activité dans lequel elles opèrent.

L'entreprise est jugée sur sa performance financière : ses comptes, ses résultats, son bilan, sa trésorerie, son cours de bourse, son potentiel de croissance et de résultats, sa performance extra-financière (sa gouvernance et sa performance sociale et environnementale), mais…

Quid de sa performance cyber ? La gouvernance des données, la sécurité de ces données : intégrité, confidentialité et accessibilité, la protection des données personnelles qu'elle collecte, utilise, archive, la protection des systèmes informatiques qui permettent d'échanger, stocker, modifier ces données.

Une entreprise peut être performante financièrement, mais une défaillance de son système informatique ou de la sécurité numérique peut atteindre gravement sa capacité à vendre ou produire, à payer ses fournisseurs, à échanger avec ses sous-traitants et donc dégrader ses résultats financiers, sa réputation, la confiance des actionnaires et des parties prenantes.

Les cyberrisques ne sont pas l'apanage d'une poignée de spécialistes dans l'entreprise mais touchent à la gouvernance d'ensemble. Outre les obligations règlementaires en matière de sécurité des données, il s'agit de protéger l'entreprise contre des risques de pertes de valeur, liées par exemple à la diffusion d'informations confidentielles.

« Tous connectés, tous engagés, tous responsables », est le mot d'ordre communiqué par Guillaume Poupard, directeur général de l'ANSSI au FIC 2019[1], de haut en bas et de bas en haut des organisations privées ou publiques : le conseil d'administration, le comité exécutif et l'ensemble des équipes.

La guerre commerciale entre grandes puissances est plus médiatique que la guerre cyber, qui est pourtant une arme largement utilisée par les États, les organisations

1. 11e édition du Forum international de la cybersécurité (FIC).

terroristes et criminelles, ou les entreprises (espionnage). Par ailleurs, la collecte des données est au cœur de l'économie numérique du XXI^e^ siècle, construite autour de la valorisation des données. Cette économie est actuellement dominée par les géants d'Internet, américains et chinois. Enfin, les cybercriminels exploitent les nombreuses failles des outils numériques, les failles humaines générées par des organisations qui ne se sont pas adaptées, des processus qui n'ont pas été mis à jour, et des collaborateurs qui n'ont pas été formés.

Il y a des cybermorts parmi les victimes. La cyberomerta est un frein à la prise de conscience. Enfin, les cyberautruches sont trop nombreuses parmi les dirigeants et administrateurs.