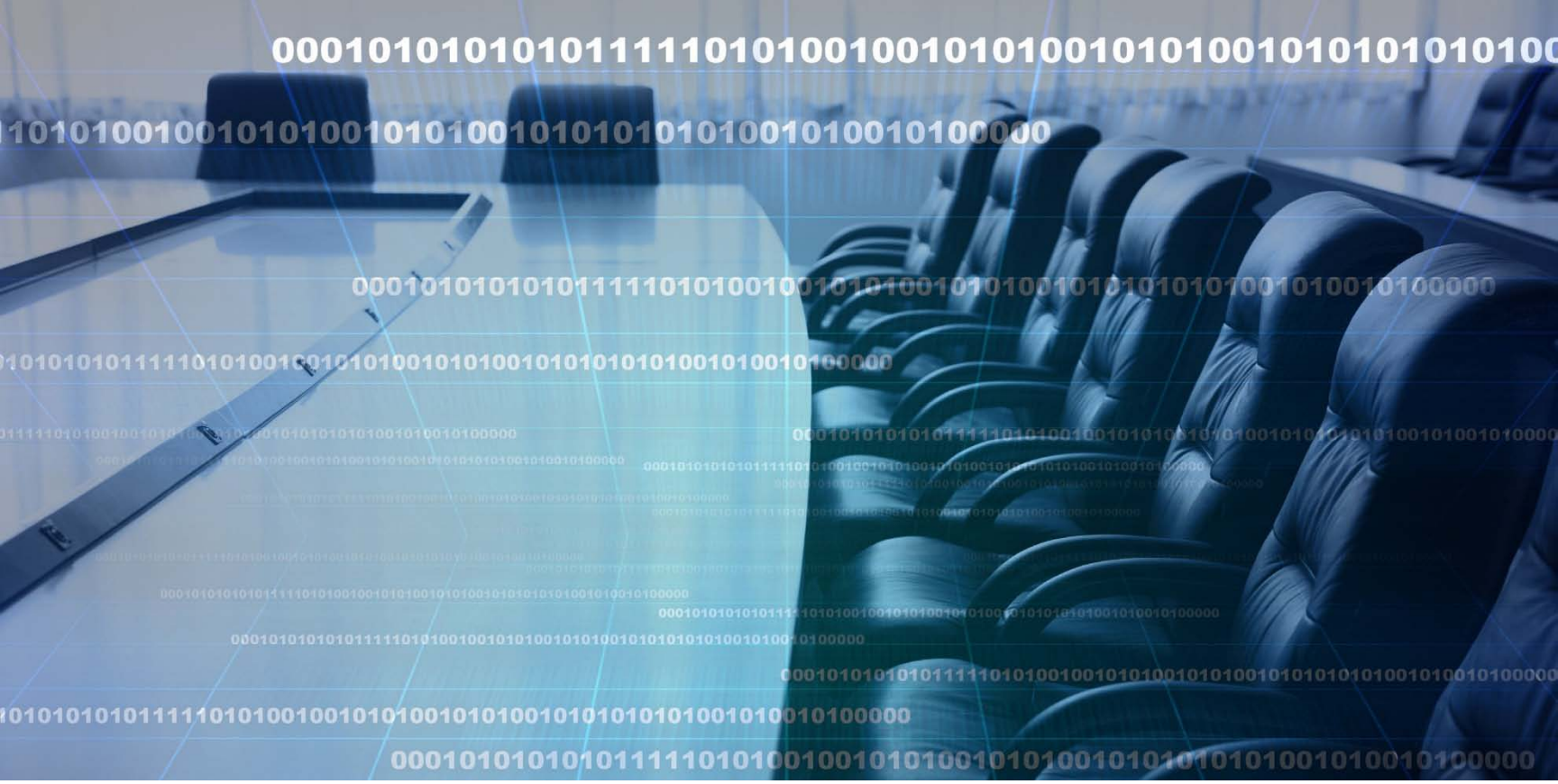


La Cybersécurité et les dirigeants

Point de vue des dirigeants et du Conseil d'administration sur la cybersécurité

IBM Institute for Business Value

Rapport de synthèse

Sécurité

Comment IBM peut vous aider

La cybercriminalité est une menace insidieuse qui a atteint des niveaux préoccupants. Bien qu'il soit difficile de le quantifier avec précision, le coût de la cybercriminalité pour l'économie mondiale est estimé entre 375 et 575 milliards de dollars par an.[1] Aucun pays, aucun secteur d'activité n'est épargné. Les pertes financières, les atteintes à la réputation et à la sécurité nationale comptent parmi les principaux risques que les dirigeants prennent au sérieux. Autrefois considérée comme un sujet technique relevant de la responsabilité du service informatique, la sécurité est aujourd'hui au cœur des préoccupations des services en charge des opérations, des dirigeants et des conseils d'administration.

IBM propose un large portefeuille intégré de logiciels et de services dédiés à la prévention, à la détection, à la gestion et à la résolution des incidents de sécurité qui peuvent aider les entreprises à anticiper et à gérer rapidement l'impact des risques liés à la cybersécurité.

Pour en savoir plus sur la manière dont IBM collabore avec les entreprises pour protéger leur infrastructure numérique, visitez le site

ibm.com/security

Pourquoi les dirigeants devraient se soucier de la cybersécurité

94 % des dirigeants pensent que leur entreprise fera probablement face à un incident de cybersécurité sérieux au cours des 2 années à venir. Et si 65 % des dirigeants sont convaincus que leurs plans de cybersécurité sont parfaitement au point, seuls 17 % des entreprises ont atteint le niveau maximal de préparation et sont réellement « cybersécurisées ». Les entreprises cybersécurisées ont effectué des progrès considérables dans la définition et la mise en œuvre de leurs stratégies de cybersécurité. Leur plan d'atténuation des risques liés à la cybersécurité est de ce fait plus efficace. Ces entreprises se distinguent par un plus grand engagement des dirigeants dans la gestion des menaces. Elles pratiquent la collaboration transversale sur les questions de cybersécurité, sont plus disposées à désigner un responsable de la sécurité des systèmes d'information (RSSI) et à lui donner les moyens d'agir et collaborent avec des entités externes pour partager les informations sur les incidents.

Rapport de synthèse

Les problèmes de sécurité ne concernent plus uniquement le service informatique, mais chaque aspect de l'entreprise et mettent en péril la continuité de ses activités et sa réputation. Ces problèmes dépassent largement l'environnement technique et s'étendent à tout l'écosystème métier. Les solutions de cybersécurité ne doivent pas seulement apporter des réponses techniques, elles doivent aussi induire des changements des processus métier, des mesures de contrôle et du comportement des dirigeants et des employés.

Pour mieux cerner les préoccupations et les points de vue des dirigeants sur la cybersécurité, IBM a réalisé une enquête auprès de plus de 700 dirigeants représentant 18 secteurs d'activité dans plus de 28 pays. Les participants occupaient des postes de dirigeants classiques, de responsables de la conformité et de conseillers juridiques. Ce rapport permet de mieux comprendre comment les dirigeants évaluent les risques et les défis liés à la cybersécurité et de déterminer si ces évaluations sont en phase avec les menaces réelles.

La cybersécurité est importante, mais l'ennemi est parfois difficile à identifier

Deux dirigeants sur trois considèrent la cybersécurité comme un sujet prioritaire, mais ils ne sont pas assez précis sur les éléments de sécurité les plus à risque. 54 % des participants à l'enquête évoquent les risques liés à des réseaux criminels organisés. Mais bon nombre d'entre eux ont tendance à surestimer les risques émanant d'individus malveillants opportunistes et minimisent les autres sources de danger, tels que l'espionnage industriel, les gouvernements nationaux et étrangers et les membres de l'écosystème métier (employés, fournisseurs, partenaires). Une bonne connaissance de l'ennemi permet d'optimiser la gestion de ces risques et d'investir dans des solutions de sécurité appropriées.

La collaboration, élément indispensable pour rétablir un certain équilibre

Il est généralement admis que dans le domaine de la sécurité, le partage collaboratif des informations sur les incidents est une arme puissante pour combattre les « méchants ». On sait que les cybercriminels les plus doués partagent des informations sur le « dark Web », le côté obscur d'Internet sur lequel des personnes mal intentionnées peuvent communiquer de manière anonyme. Les « gentils », en revanche, sont plus réticents à collaborer. Plus des deux tiers des PDG interrogés dans le cadre de notre étude se sont déclarés réticents à

65 %

des dirigeants sont convaincus que leurs plans de cybersécurité sont parfaitement au point, mais seuls 17 % ont atteint le niveau maximal de préparation et de capacité.

68 %

des PDG sont réticents à l'idée de partager avec des organisations externes des informations sur les incidents liés à la sécurité alors que la collaboration est considérée comme un puissant outil offensif dans la lutte contre la cybercriminalité.

60 %

des DAF, des DRH et des directeurs marketing se considèrent comme les moins engagés dans la gestion des menaces de cybersécurité alors qu'ils sont responsables des données les plus convoitées par les cybercriminels.

partager avec des organisations externes des informations sur les incidents de cybersécurité de leur entreprise. Le faible niveau de collaboration transversale en interne, notamment entre les trois rôles de direction (directeur des ressources humaines, directeur marketing et directeur financier) qui sont responsables des données les plus convoitées par les cybercriminels (informations sur les employés, les clients et les finances respectivement), est tout aussi inquiétant. Ces trois rôles sont également les moins confiants concernant la mise en œuvre et l'exécution des plans de cybersécurité de leur entreprise.

Les entreprises peuvent bénéficier de l'expérience d'autres entreprises qui sont bien préparées Les entreprises cybersécurisées ont mis en œuvre un programme de cybersécurité complet pour détecter les violations de la sécurité, prévenir les incidents et gérer les risques. Fait plus parlant, ces entreprises ont mis en place un service de sécurité des informations, désigné un responsable de la sécurité des systèmes d'information (RSSI) et mis en œuvre un modèle de gouvernance transversale qui implique aussi bien le conseil d'administration que la direction et les employés. Elles sont également plus ouvertes à la collaboration et au partage avec des parties externes de leurs informations sur les incidents.

Points de vue des dirigeants

Les entreprises qui sont prêtes à renforcer leur capacité en matière de cybersécurité peuvent s'inspirer de celles qui se sont illustrées dans ce domaine. Elles doivent tout d'abord identifier clairement les acteurs qui présentent les plus grands risques et évaluer le niveau de sensibilité au risque au sein de l'entreprise. Elles doivent ensuite améliorer cette sensibilisation au risque et ancrer davantage la conscience du risque dans la culture de l'entreprise. Cela passe par la mise en place de programmes pour la gouvernance de la cybersécurité, la surveillance continue, le signalement et la gestion des incidents. Pour finir, une collaboration à la fois en interne et en externe est nécessaire pour gérer les menaces et protéger les ressources numériques les plus critiques de l'entreprise. Des normes de sécurité doivent être appliquées au niveau de l'infrastructure informatique et des processus métier.

Le point de vue des dirigeants sur la cybersécurité

C'est important

Dans le cadre de l'étude Global C-suite 2015 d'IBM, plus de 5 600 dirigeants ont été interrogés sur toute une série de sujets stratégiques et de tendances émergentes[2.] 68 % d'entre eux ont placé la sécurité informatique en tête des risques technologiques susceptibles de bouleverser leur activité au cours des 3 à 5 prochaines années (voir la Figure 1). Ce souci accru des risques liés à la sécurité informatique d'une technologie est important, mais il existe également des vulnérabilités de sécurité dans l'infrastructure existante et les points d'intégration avec les fournisseurs, les clients et les partenaires.

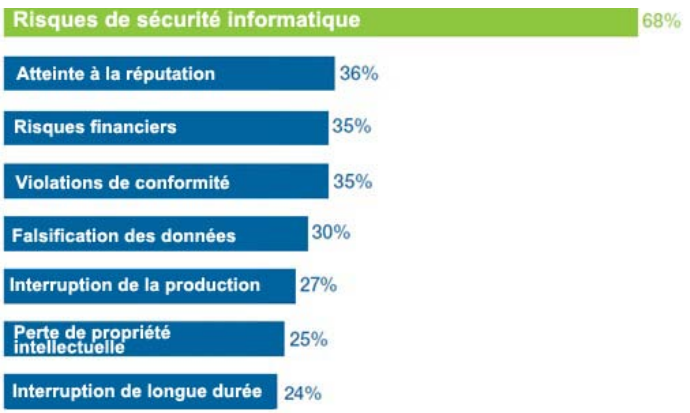
Dans ce contexte, il est essentiel de comprendre en quoi consiste un plan de cybersécurité. Une grande majorité des dirigeants interrogés s'accorde à dire que la sécurité informatique repose sur quatre éléments clés :

- Prévention (77 %) : stratégie, plan, formation et technologie pour réduire les menaces potentielles
- Détection (76 %) : systèmes et processus en temps réel pour surveiller et détecter les violations de la sécurité, combinés à des outils d'analyse pour identifier les causes principales
- Gestion des incidents (74 %) : analyse, communication, identification des responsabilités, déclarations rédigées, actions issues de l'analyse
- Résolution (78 %) : plans mis en place pour remédier rapidement aux failles de sécurité (technique, processus, formation, etc.)

… mais serai-je concerné ?

51 % des dirigeants interrogés estiment à un sur quatre le risque qu'une violation de sécurité ait un impact matériel sur leur entreprise. Ce chiffre, qui révèle une forte conscience du risque, concorde avec une étude récente qui suggère que « la probabilité d'une violation de données impliquant au moins 10 000 enregistrements est estimée à environ 22 % sur une période de 24 mois. »[3]

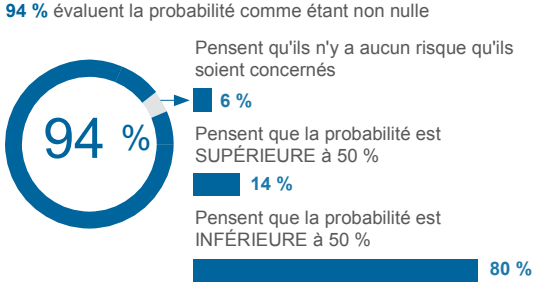
Figure 1
Point de vue des dirigeants sur les risques technologiques pour les 3-5 prochaines années.



Source : IBM Institute for Business Value.

Figure 2

Point de vue des dirigeants sur la probabilité d'une violation grave



Source : IBM Institute for Business Value.

Les 49 % restants ont des opinions très diverses sur la probabilité d'une violation. 13 % ont déjà connu une violation grave ou jugent cette situation inévitable (5 % et 8 % respectivement). Surprenant, 6 % affirment qu'une violation ne peut pas avoir d'impact matériel sur leur entreprise (voir la Figure 2).

Si les dirigeants présentent dans leur ensemble des opinions partagées sur la probabilité d'une violation, les RSSI (qui sont en première ligne en ce qui concerne la cybersécurité), sont beaucoup plus inquiets. Bon nombre d'entre eux ont d'ailleurs l'impression de perdre la bataille face à des menaces trop lourdes. L'étude menée en 2014 par IBM auprès des RSSI révélait les résultats suivants :

- 83 % des RSSI estimaient que les menaces externes s'étaient accentuées au cours des 3 dernières années (de manière considérable pour 42 % d'entre eux).
- 59 % étaient tout à fait d'accord sur le fait que la sophistication des auteurs d'attaques dépassait celle des défenses de l'entreprise.
- 40 % considéraient les menaces externes sophistiquées comme étant le défi prioritaire à relever.[4]

Il est vrai que l'évaluation de la probabilité qu'une violation de sécurité ait un impact matériel ou une retombée négative sur l'entreprise relève tout autant de l'art que de la science, notamment au vu de la diversité des acteurs et de leurs motivations, des nuances par secteur ou par région et des caractéristiques des lacunes de sécurité existantes de chaque entreprise. Le point le plus inquiétant est peut-être qu'il peut s'écouler des mois, voire des années, avant qu'un incident soit découvert. Il est alors généralement trop tard, car le mal est déjà fait.

Quels sont les risques informatiques ?

Lorsqu'ils sont interrogés sur les risques spécifiques au sein de l'infrastructure informatique, 57 % des dirigeants attribuent le niveau de risque le plus élevé aux terminaux mobiles des employés, lorsque ceux-ci utilisent des appareils personnels dans un cadre professionnel, et 54 % aux médias sociaux et aux canaux de communication, par exemple lorsque les employés utilisent Internet et répondent à des e-mails au bureau (voir la Figure 3). Les applications mobiles d'entreprise, les applications Cloud et les points d'intégration de l'écosystème métier (points d'intégration des partenaires/fournisseurs) sont également considérés à haut risque. Toutefois, l'infrastructure existante est également exposée à de nombreux risques de sécurité qui ne doivent pas être sous-estimés. Le nombre d'incidents dus aux appareils mobiles reste relativement faible par rapport à d'autres vulnérabilités. A ce niveau, les inquiétudes des dirigeants sont donc peut-être excessives.

Des violations graves survenues au cours des dernières années ont révélé le fort potentiel de risque de certains composants des infrastructures existantes, en particulier dans les conditions suivantes :

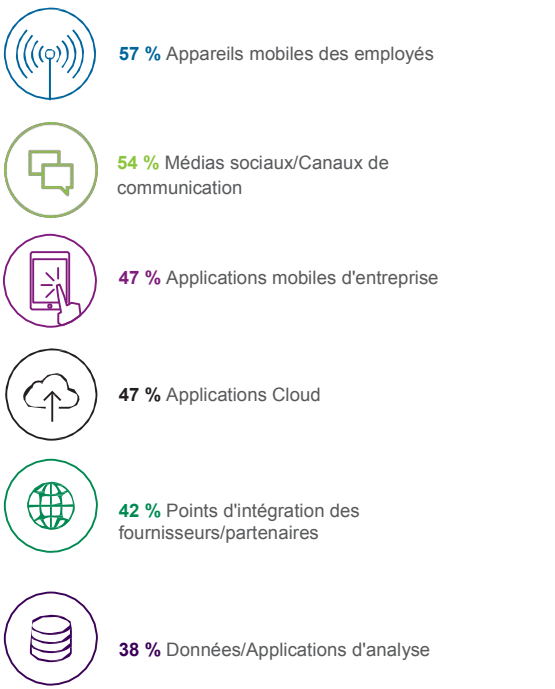
- Les employés et la direction ne sont pas suffisamment sensibilisés au problème.
- Une vulnérabilité courante n'a pas été prise en charge (les correctifs logiciels n'ont pas été installés, par exemple).
- Les protections de base ne sont pas mises en place ou mises à jour régulièrement (antivirus et détection des programmes malveillants, par exemple).

Qui est l'ennemi ?

Pour identifier son ennemi, il faut connaître les différents auteurs des menaces, leurs modes opératoires et leurs niveaux de sophistication, afin d'évaluer le degré de risque. Les experts de la sécurité connaissent bien les différents acteurs grâce à la surveillance et à l'analyse des incidents. Divers auteurs ayant des motivations diverses sont constamment à la recherche de vulnérabilités à exploiter. Leurs profils peuvent aller de l'« auteur par inadvertance » sans intention malveillante à la « menace ciblée», menée par un auteur habile et plein de ressources disposant d'un financement confortable et dont l'impact potentiel est beaucoup plus sérieux.

Figure 3

Point de vue des dirigeants sur les zones de l'infrastructure informatique les plus à risque



Source : IBM Institute for Business Value.

Nous avons demandé aux participants d'indiquer quels auteurs représentent selon eux les trois principales menaces pour leur entreprise. 70 % des dirigeants ont cité les individus malveillants, dont 38 % en première position. Les réseaux criminels organisés occupent la deuxième place, ce qui suggère que les dirigeants sont conscients des risques que ces auteurs représentent réellement. La protection de la propriété intellectuelle est manifestement un sujet de préoccupation, puisque les concurrents sont considérés comme la troisième source de menace.

La perception du risque des dirigeants ne correspond pas forcément à l'impact potentiel de chaque type d'auteur. Le profil de menace de chaque auteur dépend de son intention, de son niveau d'expertise et de la proportion d'incidents qui lui est attribuée. Certains individus externes représentent une menace relativement faible, car leur niveau de sophistication et de financement est limité et ils s'attaquent principalement à des vulnérabilités connues qui peuvent plus facilement être sécurisées. Si les entreprises s'intéressent trop à ce groupe, les résultats risquent de ne pas être à la hauteur en termes de réduction des risques, par rapport à des auteurs plus experts, tels que les gouvernements nationaux, les espions industriels et les réseaux du crime organisés. Des individus internes ou des agents externes malveillants (employés, fournisseurs, partenaires) peuvent représenter un risque beaucoup plus sérieux.

Le rapport IBM 2015 « Cybersecurity Intelligence Index » présente des chiffres inquiétants tirés d'une analyse d'incidents : 31,5 % des violations de données sont imputables à des individus malveillants internes à l'entreprise et 23,5 % à des erreurs et au non-respect des processus et politiques qui entraînent des violations ou des divulgations involontaires de données.[5] Seuls 32 % des dirigeants interrogés ont cité les employés ou anciens employés et 8 % les fournisseurs ou anciens fournisseurs parmi les trois principales menaces. L'analyse de données d'incident peut fournir des informations utiles sur le profil des auteurs, ce qui permettra aux dirigeants de prendre des décisions plus avisées sur l'orientation de leurs stratégies de sécurité.

Gouvernance et collaboration

La transparence, la collaboration et le partage en interne et en externe d'informations sur les incidents constituent des armes efficaces contre la cybercriminalité. Les analyses des violations permettent de mettre au jour les méthodes, pratiques et origines des intrusions. Le partage transversal de ces informations au sein de l'entreprise et avec des organisations externes contribue à la création d'une base de connaissances collective des auteurs et de leurs méthodes, qui facilite la mise en place de solutions.

Les dirigeants doivent s'engager et collaborer en interne sur la cybersécurité. Les entreprises doivent si nécessaire impliquer d'autres parties de leur écosystème, tels que les fournisseurs, les partenaires et les concurrents. Les cybercriminels échangent sur le dark Web des informations sur les vulnérabilités qu'ils découvrent. L'absence de collaboration handicape les entreprises par rapport aux cybercriminels qui ont pour habitude de collaborer et de partager des informations.

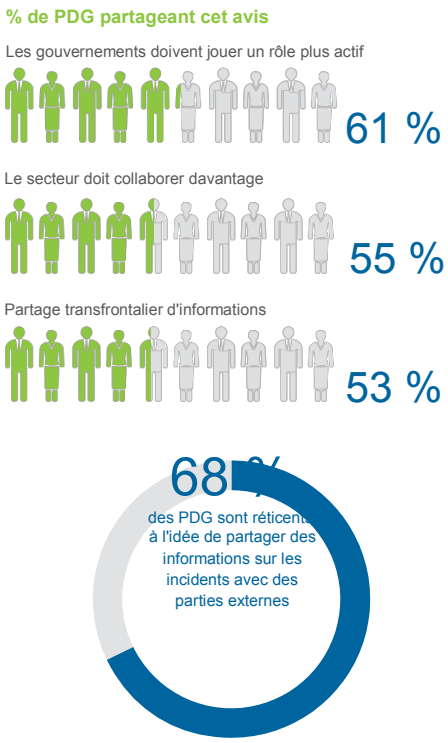
La dichotomie du PDG

Les PDG semblent hésitants à l'idée de partager avec des parties externes des informations sur les incidents. La décision peut être difficile à prendre, mais si les mesures de contrôle appropriées sont mises en place, le partage des informations sur les incidents peut rétablir un certain équilibre.

Face à une série d'affirmations sur le rôle d'une partie externe dans la lutte contre la cybercriminalité, 61 % des PDG conviennent que les gouvernements doivent jouer un rôle plus actif, 55% pensent qu'une collaboration plus poussée au sein du secteur est nécessaire et 53 % considèrent que le partage transfrontalier d'informations est nécessaire (voir la Figure 4).

Figure 4

Importance accordée par les PDG au soutien externe par rapport à la volonté de collaboration avec l'extérieur



Source : IBM Institute for Business Value.

Mais lorsque nous avons demandé aux PDG dans quelle mesure ils étaient prêts à transmettre des informations sur les incidents de cybersécurité à diverses parties prenantes (internes et externes), 68 % d'entre eux ont exprimé leur réticence à l'idée de partager ces informations avec des parties externes. Une plus grande collaboration externe entre les entreprises pourrait pourtant accélérer le développement d'une base de connaissances et d'informations sur les auteurs des menaces et leurs stratégies. Les dirigeants doivent surmonter leur réticence pour le partage responsable d'informations avec les organisations externes appropriées. Ils pourront ainsi utiliser l'analyse et appliquer des méthodes cognitives de plus en plus évoluées pour renforcer et automatiser les solutions de sécurité et limiter les risques.

Le paradoxe de la confiance

65 % des dirigeants interrogés affirment être convaincus que les plans de cybersécurité de leur entreprise sont parfaitement au point. Cet avis n'est cependant pas partagé par tous les dirigeants. 77 % des directeurs de la gestion des risques et 76 % des directeurs des systèmes d'information affirment que les plans de cybersécurité de leur entreprise sont au point. Ce chiffre tombe à un peu plus de 50 % chez les PDG. Ils forment le groupe le moins confiant avec les directeurs marketing, financiers et des ressources humaines (voir la Figure 5). Ces résultats sont significatifs, car ces trois rôles sont responsables des données sur les clients, les finances et les employés, des informations très convoitées par les cybercriminels.

Les DSI et les Directeurs de la Gestion des Risques (DGR) peuvent avoir un degré de confiance supérieur du fait de leurs rôles spécifiques. Puisque la cybersécurité a toujours relevé historiquement de la responsabilité des services informatiques, il est possible que les DSI pensent avoir géré les aspects techniques et mis en place des défenses solides sur le réseau de l'entreprise, au sein des applications et pour les accès distants depuis des ordinateurs portables et des appareils mobiles. Si l'on considère que c'est suffisant sans engager l'entreprise, on risque d'omettre des domaines des processus métier, de la gestion des informations et des solutions tierces. Le Cloud illustre bien ce problème et peut expliquer les divergences d'opinion des dirigeants sur les risques de sécurité. Si l'entreprise décide de s'appuyer sur des offres Cloud tierces,

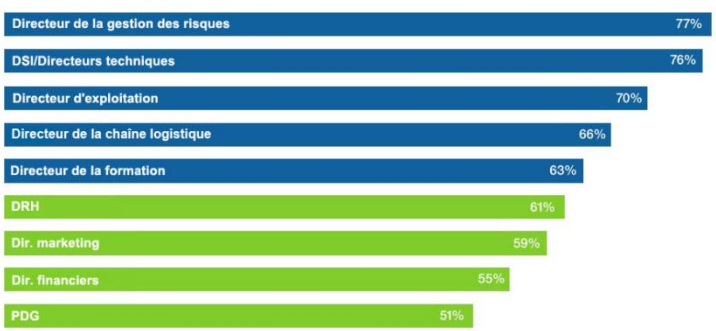
sans engager les services en charge de l'informatique et de la cybersécurité ou sans tenir compte de la capacité du fournisseur à gérer les risques liés à la cybersécurité, elle s'expose à un risque supplémentaire.

De même, les DGR étant chargés de l'évaluation et de la planification des risques de l'entreprise, ils ont pu intégrer les risques liés à la cybersécurité à leur modèle de gestion des risques d'entreprise (ERM). Mais cela ne se traduit pas nécessairement par une véritable protection contre les risques. L'ERM est orienté plan de réponse aux incidents après un événement induisant un risque. Les plans doivent comporter des étapes tactiques spécifiques destinées à limiter les risques en améliorant la sécurité. Le DGR peut être confiant par rapport au plan et aux actions développés, mais les dirigeants de l'entreprise doivent gérer concrètement les risques spécifiques.

Figure 5

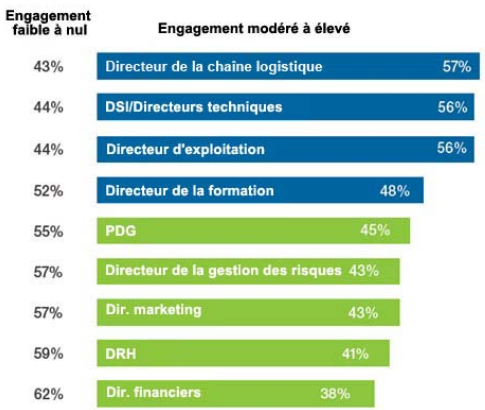
Efficacité des plans de cybersécurité par rôle

% de dirigeants affirmant que la stratégie de cybersécurité de leur entreprise est au point



Source : IBM Institute for Business Value.

Figure 6 *Degré d'engagement des dirigeants dans les activités de gestion des menaces de cybersécurité par rôle*



Source : IBM Institute for Business Value.

Collaboration entre dirigeants – De l'informatique à l'opérationnel

Il est de plus en plus important que les dirigeants, en particulier entre les responsables informatiques et les responsables de services dédiés, soient sur la même longueur d'onde pour mettre en place un dispositif de sécurité mature. Nous avons étudié les réponses à des questions spécifiques de l'enquête pour déterminer si les différents rôles étaient en phase.

Les directeurs des systèmes d'information sont pratiquement deux fois plus confiants que les PDG et les directeurs financiers, marketing et ressources humaines dans la capacité des plans de cybersécurité à favoriser la collaboration entre dirigeants.

Cette confiance peut être due au fait que les services informatiques ont une meilleure compréhension des mesures à prendre pour sécuriser les domaines à plus haut risque. Les directeurs des systèmes d'information se soucient davantage des systèmes informatiques existants tels que le réseau, le système d'exploitation et le système financier que du marketing, des ressources humaines et de l'écosystème de fournisseurs/partenaires.

Si les directeurs des systèmes d'information ont exprimé leur confiance, 69 % des dirigeants ont indiqué que les plans de cybersécurité n'intégraient pas d'éléments de collaboration entre dirigeants. Pratiquement trois PDG, directeurs des ressources humaines, directeurs marketing et directeurs financiers sur quatre estiment que les plans de cybersécurité ne les incluent pas dans une approche transversale.

Dans une question étroitement liée à l'exécution tactique des plans de cybersécurité, nous avons demandé aux participants dans quelle mesure les responsables fonctionnels participent aux activités de gestion des menaces de sécurité lors des réunions de direction (voir la Figure 6). Près de 60 % ont répondu qu'ils n'avaient pas l'impression d'être inclus dans la discussion ou qu'ils n'y participaient pas lors des réunions de direction. 57 % des directeurs marketing, 59 % des directeurs des ressources humaines et 62 % des directeurs financiers ont indiqué qu'ils n'étaient pas impliqués dans ces discussions avec les autres dirigeants.

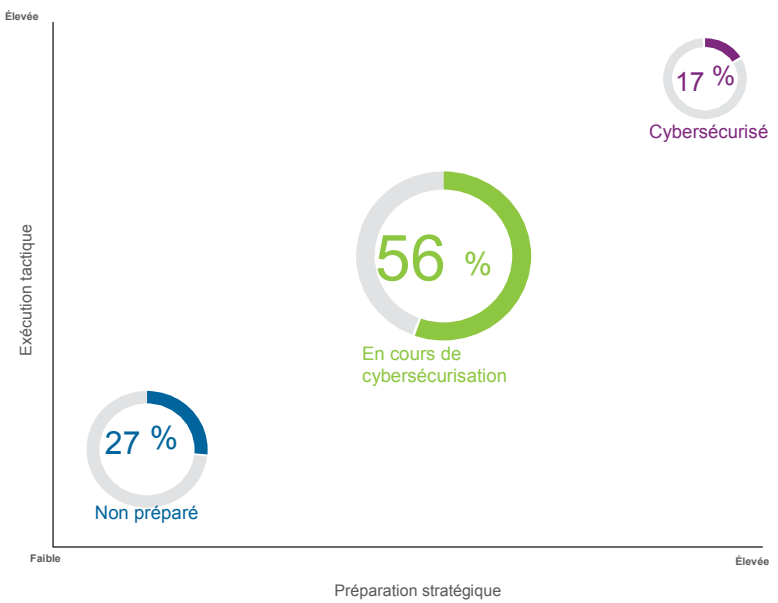
L'interaction entre dirigeants est le principal environnement dans lequel les dirigeants interrogés ont affirmé collaborer avec leurs pairs sur les questions de cybersécurité. Dans ces conditions, le faible niveau d'engagement de ces trois rôles clés a de quoi inquiéter.

Etre cybersécurisé

Nous avons analysé les réponses aux questions sur la préparation tactique et stratégique de la cybersécurité. Cette analyse a généré trois profils. Un groupe que nous avons qualifié de « cybersécurisé » fournit des informations utiles sur la préparation stratégique et l'exécution tactique des plans de cybersécurité de ces entreprises. Ce groupe qui réunit 17 % des participants présente des facteurs distinctifs clés (voir la Figure 7).

Figure 7

Modèle de capacité des dirigeants en matière de cybersécurité



Source : IBM Institute for Business Value.

Modèle de capacité en matière de cybersécurité

Un groupe de participants s'est distingué par la capacité et la préparation des dirigeants en termes de cybersécurité. Nous avons qualifié ce groupe de « cybersécurisé ». Il affiche la vision la plus optimiste des risques et un besoin de gouvernance transversale et intègre davantage ces risques à ses plans d'ERM que les autres groupes. L'élément le plus important est que les dirigeants de ce groupe présentent l'engagement le plus équilibré et le plus collaboratif.
L'analyse a porté sur plusieurs questions de l'enquête afin de tenir compte du plan de cybersécurité dans son intégralité et du degré d'exécution tactique de ce plan. A chaque question, le participant était invité à noter son entreprise sur une échelle de 1 à 5, 1 signifiant « pas du tout efficace » et 5 « extrêmement efficace ».

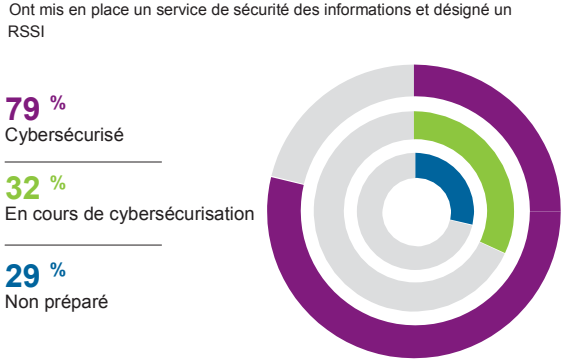
La dimension stratégique du modèle de maturité nécessite une progression dans trois domaines clés :

1. Etablir un modèle de gouvernance pour la sécurité, y compris la sécurité à l'échelle de l'entreprise.
2. Identifier et protéger les données et les applications critiques.
3. Développer et mettre en œuvre un plan d'intervention efficace.

La dimension tactique du modèle de maturité tient compte du degré d'efficacité mentionné par les participants pour chacun des quatre éléments du plan de cybersécurité.

Figure 8

Prévalence du rôle de RSSI par groupe de capacité



Source : IBM Institute for Business Value.

L'équipe de Cybersécurité comme UN seul homme derrière son RSSI

Un facteur important de développement des capacités en matière de cybersécurité est directement lié à l'instauration d'un service de sécurité des informations et à la désignation d'un RSSI. Les entreprises cybersécurisées sont 2,5 fois plus susceptibles d'avoir suivi ce processus (voir la Figure 8).

Les dirigeants des entreprises cybersécurisées travaillent en équipe

Les dirigeants des entreprises cybersécurisées comprennent l'intérêt d'une approche globale et transversale de la cybersécurité. Conscients de l'importance d'engager l'aspect opérationnel, ils sont cinq fois plus susceptibles d'intégrer la collaboration entre dirigeants à leurs plans de cybersécurité que ceux des entreprises qui ne sont pas préparées. La collaboration entre les dirigeants est beaucoup plus susceptible d'être intégrée à la gouvernance de la cybersécurité au sein des entreprises cybersécurisées (voir la Figure 9).

Ces dernières ont d'ailleurs une gouvernance de la cybersécurité plus efficace que les autres, avec 61 % des personnes interrogées qui évoquent régulièrement le sujet lors des réunions de direction contre seulement 31 %. Plus important, le niveau d'engagement moyen est beaucoup plus élevé dans ces entreprises, notamment en ce qui concerne les directeurs marketing, des ressources humaines et financiers.

La cybersécurité est près de deux fois plus susceptible d'être à l'ordre du jour des réunions du conseil d'administration des entreprises cybersécurisées (56 %) que des autres organisations (27 %). Les membres du conseil ne doivent pas nécessairement devenir des experts de la cybersécurité, mais ils doivent s'informer suffisamment sur les risques associés pour pouvoir :

- Demander aux dirigeants d'informer le conseil d'administration des mesures de contrôle appropriées mises en place.
- Surveiller régulièrement les mesures de contrôle pour s'assurer qu'elles fonctionnent comme prévu.
- Demander le signalement rapide des incidents sérieux.

Les entreprises cybersécurisées collaborent davantage avec des organisations externes

Sachant que les cybercriminels les plus doués collaborent, il est évident que la collaboration des entreprises sur la gestion de la sécurité et les incidents contribuerait à réduire les risques. Entre cybercriminels, cette collaboration consiste pour un des leurs à découvrir une vulnérabilité et à vendre l'information aux autres pour qu'ils l'exploitent. Les PDG des entreprises cybersécurisées sont beaucoup moins réticents à partager des données sur les incidents avec des organisations externes. Ils sont trois fois plus disposés que les autres à collaborer avec des concurrents de leur secteur industriel et deux fois plus à collaborer avec des prestataires de services de sécurité tiers et des fournisseurs et partenaires. Pour rétablir l'équilibre, les dirigeants doivent considérer la collaboration extérieure comme une puissante tactique offensive. Le volume des données d'incident sur les cybercriminels, les origines et les stratégies des attaques augmente rapidement. Plus les entreprises collaborent pour mieux connaître les cybercriminels et leurs activités, mieux elles sont préparées à mettre en place des solutions qui réduisent des risques.

Figure 9

Prévalence de la collaboration et de la transparence du conseil d'administration par groupe

Collaboration entre dirigeants intégrée au plan de cybersécurité (gouvernance)

La cybersécurité est régulièrement à l'ordre du jour des réunions du conseil d'administration

Rôle central des ressources humaines dans la cybersécurité

Seuls 57 % des directeurs des ressources humaines ont indiqué avoir mis en place une formation à la cybersécurité pour les employés. En tant que responsables d'informations personnelles sensibles sur les employés très convoitées par les pirates informatiques, les directeurs des ressources humaines doivent être en première ligne des efforts de cybersécurité déployés par l'entreprise, parmi lesquels :

Protection des informations personnelles sensibles sur les employés
Le service des ressources humaines doit s'approprier la gouvernance de la protection de ces informations et des processus métier liés à l'utilisation et à la gestion de données pendant toute la durée des contrats des employés.

Formation à la cybersécurité et renforcements des mesures
Les terminaux mobiles personnels accédant aux systèmes des entreprises sont de plus en plus nombreux et génèrent de nouvelles vulnérabilités. Les ressources humaines peuvent instaurer des politiques de sécurité et des mesures disciplinaires qui s'appliquent aux employés et peuvent aller jusqu'au licenciement.

Pratiques sur toute la durée du contrat de travail
Les ressources humaines peuvent aider les parties prenantes à établir clairement les rôles et les parcours professionnels, puis contribuer au processus de recherche et de sélection, y compris à l'évaluation des candidats par rapport aux risques de sécurité pour ne pas recruter par inadvertance un candidat qui constituera une menace interne. Les ressources humaines doivent participer à l'évaluation de la sensibilité des rôles et procéder à des vérifications plus détaillées lors de recrutements à ces postes.

A l'attention des dirigeants : Conseils de cybersécurité pour 2016 et au-delà

Comprendre les risques

- Evaluer les risques liés à votre secteur, à votre zone géographique et à votre écosystème métier et partenaires.
- Procéder à une évaluation des risques de sécurité ou à la mise à jour de toute évaluation de plus d'un an.
- Déterminer quels domaines représentent des cibles de choix pour les cybercriminels et investir dans des moyens de défense appropriés.
- Intégrer l'évaluation de la sécurité au plan de risque de l'entreprise.
- Développer des supports d'éducation et de formation obligatoires pour les employés, les mettre à jour régulièrement et appliquer de manière rigoureuse les règles de conformité.

Collaborer, éduquer et responsabiliser

- Mettre en place un modèle et un programme de gouvernance de la sécurité pour favoriser la collaboration à l'échelle de l'entreprise.
- Confier au RSSI la gestion des risques liés à la sécurité des informations de l'entreprise et diriger l'initiative.
- Accorder plus d'importance à la cybersécurité, aborder régulièrement le sujet lors des réunions de direction et du conseil d'administration et impliquer au moins les directeurs de la gestion des risques, du marketing, des ressources humaines et de la chaîne logistique.
- Inciter le développement des supports de base pour l'éducation des cadres dirigeants.
- Impliquer les dirigeants dans l'élaboration d'un plan de réponse aux incidents et soumettre ce plan au conseil d'administration avant de l'appliquer.

Gérer les risques avec vigilance et rapidité

- Mettre en œuvre une solution de surveillance continue de la sécurité et créer des services de sécurité ou s'appuyer sur des services tiers pour analyser les incidents.
- Partager les données sur les incidents avec les parties externes concernées, telles que des concurrents, des fournisseurs/partenaires et des experts de la cybersécurité et tirer profit de l'analyse des menaces pour poursuivre la sécurisation de l'environnement.
- Identifier les ressources numériques de l'entreprise (données, applications, systèmes et infrastructure) et développer un plan de protection pour chaque ressource, en fonction du niveau de risque et de la tolérance au risque.

- Développer et appliquer des politiques de cybersécurité, y compris sur le comportement sur le lieu de travail des employés, des sous-traitants et des fournisseurs et la gestion des terminaux mobiles, notamment des appareils personnels des employés (BYOD).

- Intégrer la cybersécurité aux processus et décisions métier.

Quel est le rôle du RSSI ?

La désignation d'un RSSI ou d'un rôle équivalent est désormais une pratique courante au sein des organisations commerciales, gouvernementales et à but non lucratif. Le RSSI occupe aujourd'hui un rôle essentiel dans les grandes entreprises, car la sécurité est devenue trop sensible pour être une activité parmi d'autres du périmètre du DSI.

Le nombre d'entreprises ayant un RSSI a augmenté régulièrement depuis 2006 de 10 % par an environ. 22 % des entreprises affirmaient avoir un RSSI en 2006, contre 80 % en 2011.[6] En moyenne, 71 % des participants ont déclaré que leur entreprise avait désigné un RSSI. Près de 80 % des entreprises cybersécurisées (voir l'encadré Modèle de capacité en matière de cybersécurité, page 11) ont un RSSI, dont la durée moyenne du contrat a augmenté de près de deux ans.

Le conseil d'administration attend du RSSI qu'il l'aide à mieux identifier et valoriser les risques pour l'entreprise. Les dirigeants demandent au RSSI de développer et de mettre en place un cadre complet de cybersécurité destiné à réduire les risques.

Pour plus d'informations
Pour en savoir plus sur cette étude de l'IBM Institute for Business Value, contactez-nous à l'adresse iibv@us.ibm.com. Suivez @IBMIBV sur Twister, et pour obtenir le catalogue complet de nos travaux de recherche (ou pour vous abonner à notre lettre d'informations mensuelle), visitez le site suivant : ibis.com/iibv

Vous pouvez accéder aux rapports de synthèse de l'IBM Institute for Business Value sur votre appareil mobile, en téléchargeant gratuitement l'application « IBM IBV » pour votre téléphone ou tablette dans votre magasin d'applications.

Le partenaire idéal dans un monde en perpétuelle évolution
Chez IBM, nous collaborons avec nos clients en associant les données professionnelles, la recherche avancée et la technologie. Ainsi, ils disposent d'une réelle longueur d'avance dans l'environnement actuel en perpétuelle évolution.

IBM Institute for Business Value
IBM Institute for Business Value, au sein de l'IBM Global Business Services, élabore des analyses stratégiques factuelles destinées aux cadres supérieurs et concernant des sujets sensibles des secteurs public et privé.

A propos des auteurs
Diana Kelley est conseillère exécutive pour la sécurité d'IBM Security et directrice de l'IBM Security Newsroom. Forte de plus de 25 années d'expérience au poste de conseillère exécutive pour la sécurité, elle dispose des compétences en informatique nécessaires pour conseiller et guider les RSSI et les professionnels de la sécurité. Elle a contribué au rapport IBM X-Force et publie régulièrement des articles consacrés au leadership sur le blog Security Intelligence. Elle est actuellement membre de la faculté de l'institut de recherche IANS et siège au conseil consultatif d'InfoSec World et au comité du programme du Executive Women's Forum. Diana intervient régulièrement lors de conférences sur la sécurité et a été citée comme experte en sécurité par The New York Times, TIME, MSNBC.com, Information Security Magazine et The Wall Street Journal. Elle a participé à la rédaction de l'ouvrage Cryptographic Libraries for Developers. Il est possible de la contacter à l'adresse suivante : drkelley@us.ibm.com.

Carl Nordman est Directeur de recherche en cybersécurité et finances à l'IBM Institute for Business Value. Il est responsable de la recherche primaire dans ces deux domaines. Il mène des études afin de mettre au jour les tendances actuelles et des perspectives sur des sujets stratégiques d'actualité. Carl a 25 ans d'expérience dans le risque financier et la fraude. Il a auparavant travaillé pour les services de conseil d'IBM, où il a accompagné les directeurs financiers d'entreprises du Fortune 1000 et assuré des services BPO de finance et de comptabilité en tant que responsable de compte pour plusieurs clients. Il est possible de le contacter à l'adresse suivante : carl.nordman@us.ibm.com.

Contributeurs
John Lainhart, Partenaire, Service public GBS, $$$Directeur régional, Cybersécurité et confidentialité ; Gretchen Marx, Directrice de programme, Stratégie du portefeuille de sécurité IBM, IBM Security ; Lisa van Deth, Directrice de programme marketing, Stratégie de campagne et de leadership, IBM Security.

Remerciements

Peter Allor, Stratège principal en sécurité, IBM Security ; Michelle Alvarez, Chercheuse spécialisée dans les menaces, Editrice et relectrice, Services de sécurité gérés ; Chuck Carney, Vice-Président des services de sécurité, IBM Security ; David Jarvis, Directeur, IBM Center for Applied Insights, Market Insights ; Bob Kalka, Vice-Président des comptes stratégiques et des programmes d'habilitation, IBM Security ; Charles Kolodgy, Stratège en sécurité IBM, IBM Security ; Jason Kravitz, Spécialiste technique IBM pour les systèmes et services de sécurité Internet ; Christopher Poulin, Stratège en recherche-X-Force, IBM Security ; Michaela Santa Barbara, Directrice de programme, Conseils en sécurité et intégration de systèmes.

Notes et sources

1 « Net Losses: Estimating the Global Cost of Cybercrime », juin 2014. Center for Strategic and International Studies. http://www.cyberriskinsuranceforum.com/sites/default/files/pictures/ rp-economic-impact-cybercrime2.pdf

2 « Redefining Boundaries: Insights from the Global C-suite Study ». IBM Institute for Business Value. Novembre 2015. http://www-935.ibm.com/services/c-suite/study/study/

3 2015 Cost of Data Breach Study: Global Analysis. Analyse comparative sponsorisée par IBM, menée de manière indépendante independently par Ponemon Institute LLC, mai 2015. Page 20, Figure 15. http://www-01. ibm.com/common/ssi/cgi-bin/sialias?subtype=WH&infotype=SA&htmlfid=SEW03053 WWEN&attachment=SEW03053WWEN.PDF

4 « Fortifying for the future: Insights from the 2014 IBM Chief Information Security Officer Assessment. » IBM. Décembre 2014. www.ibm.com/ibmcai/ciso

5 IBM 2015 Cyber Security Intelligence Index - https://securityintelligence.com/ economic-espionage-the-global-workforce-and-the-insider-threat/

6 Enquête annulle de PricewaterhouseCoopers sur la sécurité de l'information, 2011, 2006

IBM Global Business Services
17 avenue de l'Europe
92275 Bois Colombes Cedex

Imprimé en France
Février 2016

GBE03738-FRFR-0