KESSLER

RAPPORT DU SONDAGE SUR LES CYBERRISQUES 2019
LES CYBERRISQUES DU POINT DE VUE DE LA SUISSE

EN AVANT, SEREINEMENT.

RAPPORT DU SONDAGE SUR LES CYBERRISQUES 2019
LES CYBERRISQUES DU POINT DE VUE DE LA SUISSE

1	AVANT-PROPOS	5
2	À PROPOS DU RAPPORT	6
3	ENSEIGNEMENTS ET COMMENTAIRES	10
	3.1 LA PRISE DE CONSCIENCE DES CYBERRISQUES AUGMENTE DE FAÇON SIGNIFICATIVE	10
	3.2 L'MPORTANCE DE LA GOUVERNANCE D'ENTREPRISE	12
	3.3 LA GESTION DES CYBERRISQUES: UN INDICATEUR DE LA PRISE DE CONSCIENCE DES MENACES CYBERNETIQUES	14
	3.4 GESTION DES CYBERRISQUES ÉMANANT DES SOUS-TRAITANTS	22
	3.5 LES CONCLUSIONS DE CYBERASSURANCES SONT EN AUGMENTATION	24
4	LE RGPD RENFORCE LA GESTION DES CYBERRISQUES	28
	4.1 LES COÛTS RELATIFS AUX VIOLATIONS DE LA LÉGISLATION SUR LA PROTECTION DES DONNÉES	28
5	CONCLUSIONS	30

1 AVANT-PROPOS

L'INDUSTRIE 4.0 EST ANCRÉE DANS LA VIE QUOTIDIENNE

Dans l'industrie manufacturière en particulier, les entreprises utilisent de plus en plus fréquemment des composants de l'internet des objets (Internet of Things – IoT), ce qui a pour effet de modifier les futurs concepts de sécurité. Les dangers émanant de l'internet des objets sont sous-estimés actuellement. Les cafetières connectées, les lampes ou les photocopieurs intelligents peuvent constituer des points d'accès au réseau de l'entreprise. Personne n'ira jusqu'à affirmer que ces cafetières intelligentes sont plus sûres qu'un logiciel d'entreprise développé par des professionnels. La gestion des cyberrisques consiste notamment à connaître les failles des sociétés pour protéger les «joyaux de la couronne» de l'entreprise afin de lui permettre d'atteindre avec succès ses objectifs.

LA GESTION DES CYBERRISQUES ÉMANANT DES SOUS-TRAITANTS

La dépendance vis-à-vis des sous-traitants IT est un sujet qui a encore tendance à passer au second plan. Pour diverses raisons, les données et les processus sont externalisés. Malheureusement, nous ne pouvons pas entièrement déléguer la responsabilité afin que les données clients demeurent intègres, confidentielles et toujours disponibles. Dans le contexte international, les questions de responsabilité sont encore bien plus complexes qu'elles ne le sont déjà dans l'environnement commercial national. La chaîne de création de valeur, qui a souvent une dimension internationale aujourd'hui, exige de la part des entreprises une discipline extrême en ce qui concerne la transparence de leurs dépendances. La transparence permet de comprendre l'exposition aux cyberrisques dans le cadre la chaîne d'approvisionnement.

NOTRE SONDAGE

En septembre 2018, nous avons réalisé un sondage intersectoriel à l'échelle nationale, qui a analysé la façon dont les entreprises gèrent les cyberrisques ainsi que les dangers potentiels de ces derniers, dans les activités quotidiennes, y compris les risques que cela implique en matière de protection des données. Nous avons invité tous nos clients opérant à l'international ainsi que d'autres entreprises actives à l'international à participer au «Rapport du sondage sur les cyberrisques 2019 – Les cyberrisques du point de vue de la Suisse». Nous avons évalué pour vous les 387 réponses et commenté les principaux résultats.

LA SUISSE N'EST PAS UNE ZONE PROTÉGÉE

Les résultats du rapport ci-après le confirment une nouvelle fois: les entreprises suisses sont elles aussi une cible pour les cybercriminels. Il me semble dangereux de parier que la Suisse, longtemps épargnée par des cyberattaques aux lourdes conséquences pour la société, continuera de l'être à l'avenir également. Les cyberincidents d'ampleur mondiale sont trop difficiles à cerner, et les objectifs poursuivis sont tout autant imprévisibles.

Nous vous souhaitons une agréable lecture et serions heureux de discuter avec vous des nouvelles connaissances acquises dans le domaine du cyberespace.

Melanie Koller
Legal Counsel Cyber Risk

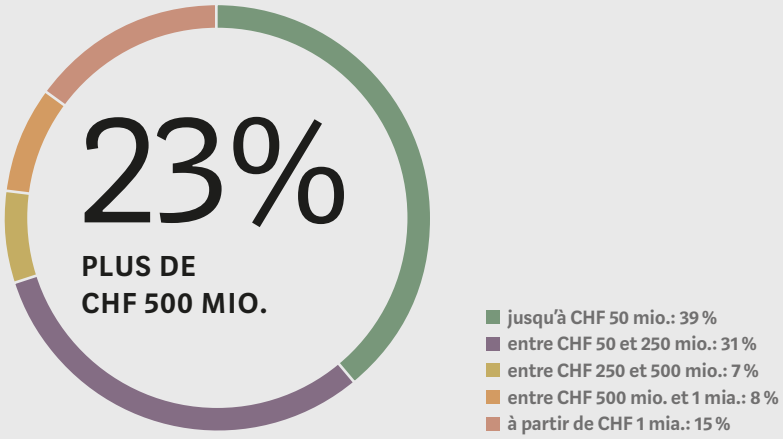
2
À PROPOS DU RAPPORT

Le présent rapport est basé sur les résultats du sondage de Kessler relatif au traitement des cyberrisques par nos clients, réalisé en septembre 2018. Les principaux enseignements du point de vue de la Suisse sont rassemblés et commentés ci-après.

387 entreprises de toute la Suisse et intervenant à l'international ont participé au sondage sur les cyberrisques. Parmi les réponses obtenues, 29 % ont été transmises par des membres de la direction ou du conseil d'administration; les 71 % restants proviennent de personnes travaillant dans le domaine de la gestion financière, de la gestion des risques, dans le domaine informatique, des ressources humaines et juridique.

70 % des entreprises interrogées génèrent un chiffre d'affaires annuel jusqu'à CHF 250 millions, alors que 7 % réalisent un chiffre d'affaires compris entre CHF 250 et 500 millions. Les 23 % restants sont des entreprises dont le chiffre d'affaires est supérieur à CHF 500 millions.

TAILLE DES ENTREPRISES EN FONCTION DU CHIFFRE



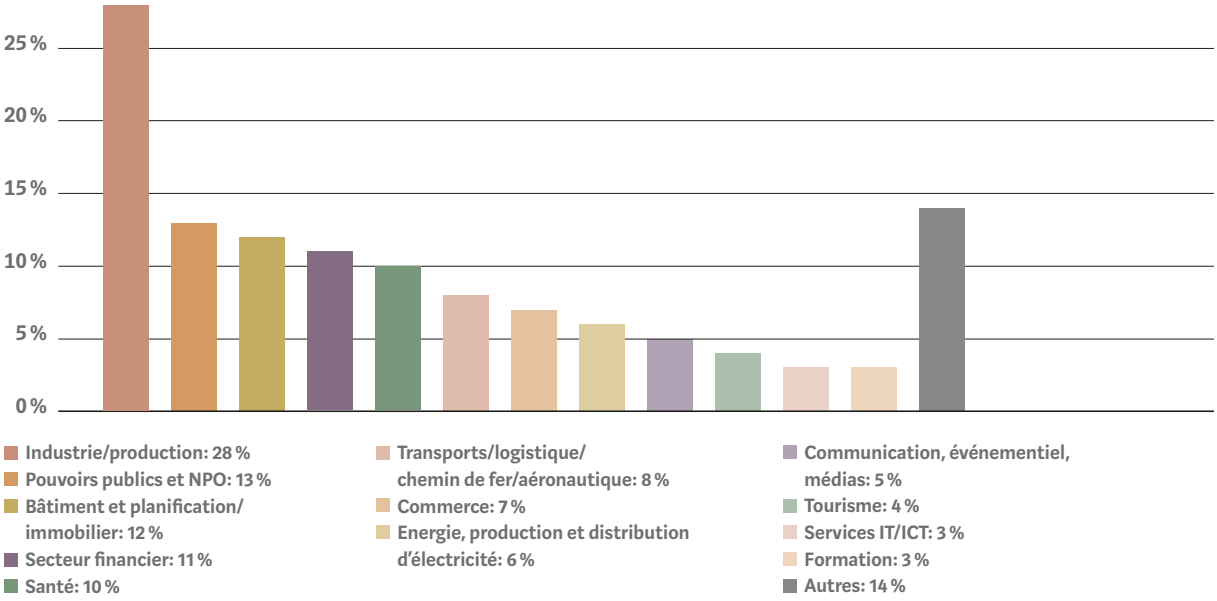
Le secteur de l'industrie et de la production, qui compte pour un quart des entreprises sondées, est le plus fortement représenté. L'intérêt manifesté par ce dernier à participer au sondage ne nous surprend pas. La perte d'exploitation consécutive à une cyberattaque, redoutée dans ce secteur, incite en effet à s'interroger profondément sur les cyberrisques.

Outre l'Europe continentale, les Etats-Unis/le Canada, l'Asie ainsi que le Proche-Orient comptent parmi les principaux marchés où opèrent les participants au sondage.

Comme c'était déjà le cas l'année dernière, la dépendance des sondés aux outils numériques et aux prestataires informatiques externes est extrêmement forte (encadré à p. 8). Comparé au sondage réalisé l'an dernier, les dépendances citées sont globalement comparables. Nous constatons cependant une nette augmentation de la prise de conscience des cyberrisques par le fait que les entreprises sont beaucoup moins nombreuses à permettre à leurs collaborateurs et à des tiers de connecter leurs propres appareils mobiles au réseau de l'entreprise. Cette évolution est confirmée lors des entretiens quotidiens que nous avons avec nos clients.

2

SECTEUR D'APPARTENANCE



DÉPENDANCE DES PARTICIPANTS VIS-À-VIS DES OUTILS ET SERVICES NUMÉRIQUES

- Un ou plusieurs ordinateurs sont reliés à Internet: 97 % (2017: 98 %)
- Traitement électronique et sauvegarde de dossiers des collaborateurs: 71 % (2017: 88 %)
- Les collaborateurs et les tiers peuvent connecter leur ordinateur portable et/ou leurs appareils mobiles au réseau de l'entreprise: 63 % (2017: 87 %)
- Sauvegarde électronique et/ou gestion de données clients: 76 % (2017: 86 %)
- Traitement électronique d'informations bancaires: 78 % (2017: 75 %)
- Sauvegarde électronique d'informations fournisseurs: 67 % (2017: 74 %)
- Services cloud: 52 % (2017: 54 %)
- Détention d'informations de santé privées, identifiables individuellement, concernant des collaborateurs ou des clients: 25 % (2017: 31 %)
- Traitement électronique de transactions par carte de crédit: 32 % (2017: 28 %)
- Saisie de données personnelles (y. c. cookies et dispositifs analogues) sur un site web: 26 % (2017: 25 %)
- Transmission de données personnelles à des fournisseurs ou à d'autres tiers: 27 % (2017: 24 %)

3 ENSEIGNEMENTS ET COMMENTAIRES

3.1 LA PRISE DE CONSCIENCE DES CYBERRISQUES AUGMENTE DE FAÇON SIGNIFICATIVE

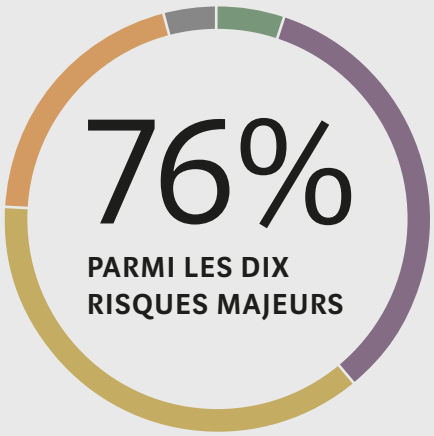
Les cyberrisques ont attiré l'attention des membres du conseil d'administration et de la direction, notamment suite à l'omniprésence depuis des mois du Règlement général de l'UE sur la protection des données (RGPD). Au vu de l'ampleur des dommages, les efforts entrepris sont toutefois insuffisants. La prise de conscience est une chose, les mesures adoptées en sont une autre.

Les résultats du sondage de cette année confirment, une fois de plus, que les cyberrisques sont considérés comme risques majeurs par les entreprises interrogées (graphique 1). Pour 76 % des participants, les cyberrisques comptent parmi les dix risques majeurs des entreprises suisses, et pour 39 % des sondés, ils font même partie des cinq risques majeurs. Cependant, les cyberrisques ne sont pas les seuls risques qui ont occupé nos clients en 2017 et 2018. Outre la guerre commerciale entre les Etats-Unis et la Chine, qui entraîne des restrictions importantes dans de nombreux secteurs économiques, le Brexit ainsi que de nouvelles dispositions législatives comme par exemple le RGPD, ont généré beaucoup d'instabilité et d'incertitudes.

Il ne suffit pas d'avoir conscience des cyberrisques pour s'attaquer à cette source de danger encore peu transparente ou d'en réduire l'impact au minimum. Pour des raisons de responsabilité au sens de l'art.

GRAPHIQUE 1

Quelle est l'importance accordée aux cyberrisques dans votre entreprise?



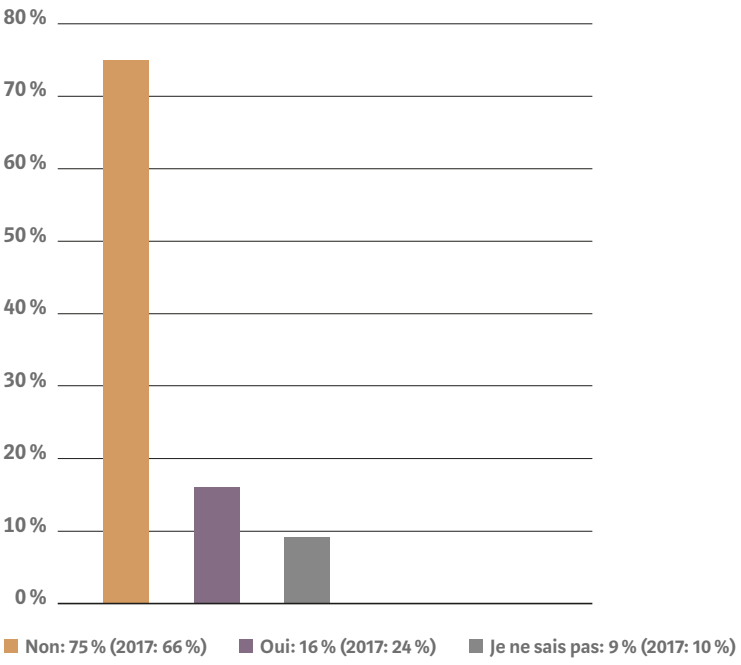
- Selon le registre des risques, les cyberrisques constituent nos plus grands risques: 5 % (2017: 3 %)
- Les cyberrisques font partie des nos 2-5 risques majeurs: 34 % (2017: 56 %)
- Les cyberrisques font partie des nos 6-10 risques majeurs: 37 % (2017: n.d.)
- Les cyberrisques ne font pas partie des dix risques majeurs: 20 % (2017: n.d.)
- Aucune importance n'est accordée aux cyberrisques: 0 % (2017: 1 %)
- Je ne connais pas l'importance des cyberrisques dans mon entreprise: 4 % (2017: 3 %)

754 CO, les entreprises non soumises à l'obligation de révision ont également intérêt à documenter dans leur rapport annuel leur exposition aux cyberrisques, conformément à l'art. 961c CO et d'engager des mesures préventives appropriées. La prise de conscience seule ne suffit pas.

A la question de savoir si leur propre entreprise avait été victime d'une cyberattaque au cours des 12 derniers mois, 75 % des participants ont répondu par «Non», 16 % par «Oui» et 9 % par «Je ne sais pas» (graphique 2). Ce résultat n'est pas surprenant, car selon l'état actuel des connaissances, les logiciels malveillants (malware) ne sont généralement découverts qu'au bout de 99 jours, voire pas du tout: en Europe, ils le sont après 106 jours en moyenne, et seulement après 172 jours au Moyen-Orient, en Asie et en Afrique. On peut dès lors supposer une nouvelle fois que parmi les entreprises ayant répondu négativement en septembre 2018 (75 %), une partie d'entre elles n'avaient pas encore remarqué qu'elles avaient été piratées au cours des derniers mois. Ce problème majeur a été constaté dans le monde entier. On étudie d'autant plus intensivement les possibilités de réduire de façon drastique le temps nécessaire pour découvrir l'introduction d'un logiciel malveillant. En effet, plus la période qui s'écoule entre l'introduction et la découverte d'un malware (breach detection gap ou dwell time) est courte, plus les répercussions financières pour les entreprises sont faibles.

GRAPHIQUE 2

Votre entreprise a-t-elle été victime d'une cyberattaque au cours des 12 derniers mois?



3

3.2 L'IMPORTANCE DE LA GOUVERNANCE D'ENTREPRISE

Les organes peuvent devoir répondre personnellement des dommages liés à une cyberattaque. C'est pour cette raison qu'il incombe à la direction de l'entreprise, et non pas au service informatique, de veiller à ce que leurs systèmes d'exploitation soient capables de résister à de nouvelles cybermenaces.

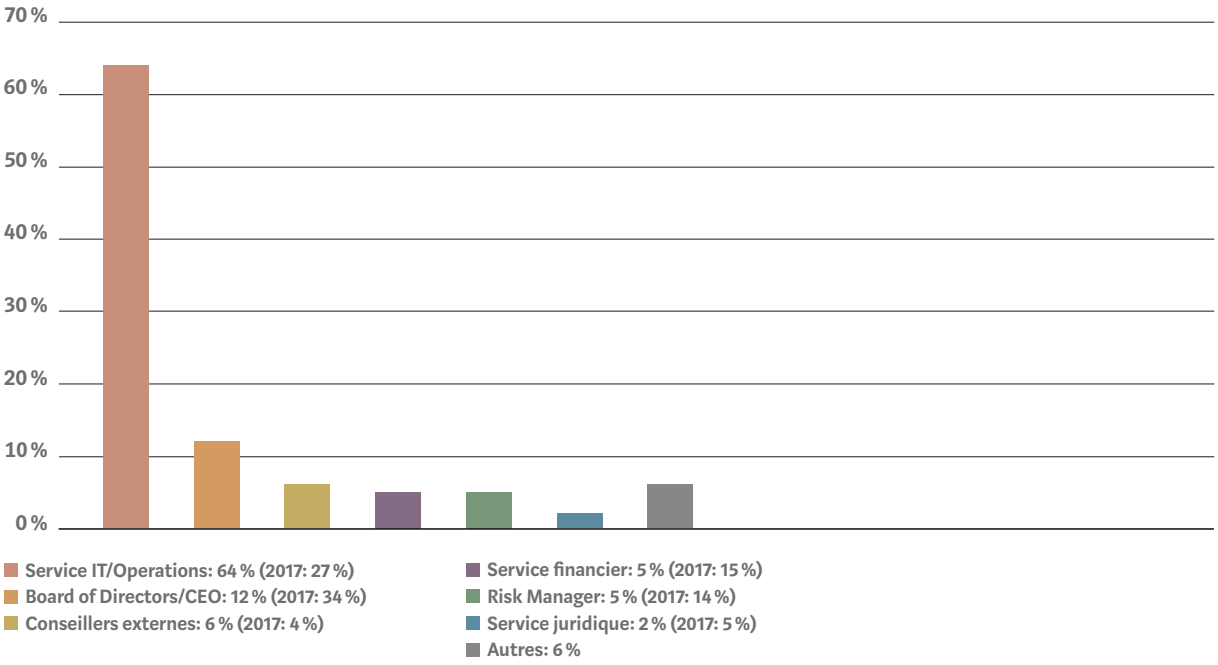
Dans le rapport de cette année, les résultats sont similaires à ceux de l'année précédente: c'est toujours le service informatique de l'entreprise qui assume en grande partie la responsabilité de la gestion des cyberrisques (64 %). La direction est responsable en matière de cyberrisques chez seulement 12 % des sondés. Ces résultats sont préoccupants.

Pour suivre l'évolution des nouvelles technologies, les entreprises doivent être innovantes. Il faut en permanence évaluer les risques et les opportunités, appliquer des mesures de sécurité appropriées et couvrir le besoin de sécurité pour la réalisation stratégique des objectifs de l'entreprise. Le RGPD a contribué à renforcer la prise de conscience des cyberrisques opérationnels. Une direction qui, à l'ère du Big Data, de l'industrie 4.0 et de l'intelligence artificielle, ne définit pas de traitement stratégique et financier réfléchi en matière de cyberrisques, sera confrontée à des problèmes importants lors d'une cyberattaque. D'un point de vue juridique, une gestion des cyberrisques absente ou insuffisante peut, dans certaines circonstances, être qualifiée de violation du devoir de diligence et de fidélité au sens de l'art. 717 CO et entraîner une responsabilité en qualité d'organe de la société en vertu de l'art. 754 CO.

Quoi qu'il en soit, la direction a tout intérêt à connaître les risques majeurs de l'entreprise et à les quantifier. En vertu de la loi de Murphy, selon laquelle tout ce qui peut aller de travers ira de travers, il faut en permanence s'attendre à des cyberincidents et par conséquent faire planifier soigneusement, avec l'aide de spécialistes, les mesures destinées à y faire face.

GRAPHIQUE 3

Parmi les domaines fonctionnels ci-après, lesquels sont responsables en priorité de la gestion des cyberrisques?



GRAPHIQUE 4

Si le comité de direction/le CEO est compétent en matière de cyberrisques, quels sont, parmi les rapports ci-après, ceux qui lui sont adressés?

- Recommandation relative à la réduction des cyberrisques: 67 %
- Mesures de sensibilisation: 48 %
- Rapport sur les problèmes ou faits survenus: 55 %
- Rapport sur les activités de contrôle (correctifs, formations, situation en matière de phishing): 36 %
- Informations sur les menaces: 21 %
- Recommandations relatives à la stratégie de financement des cyberrisques: 12 %
- Je ne sais pas: 15 %

3

3.3 LA GESTION DES CYBERRISQUES: UN INDICATEUR DE LA PRISE DE CONSCIENCE DES MENACES CYBERNETIQUES

Il n'y a pas de gestion des cyberrisques juste ou fausse: chaque entreprise a, en fonction de son cœur de métier et des objectifs stratégiques qui en découlent, une approche différente dans le traitement des cyberrisques. La seule chose à ne pas faire, c'est ne rien faire. La prise de conscience est une chose, la mise en œuvre des mesures nécessaires en est une autre. Dans la gestion des cyberrisques, cette lacune doit être comblée.

42 % des participants (contre 58 % en 2017 et 41 % en 2016) ont déjà quantifié les répercussions financières d'un cybersinistre au sein de leur entreprise. Ces résultats sont réjouissants, malgré une évolution fluctuante. Ils montrent notamment que les cyberrisques sont de plus en plus fréquemment considérés comme des risques à prendre au sérieux par les entreprises (graphique 5).

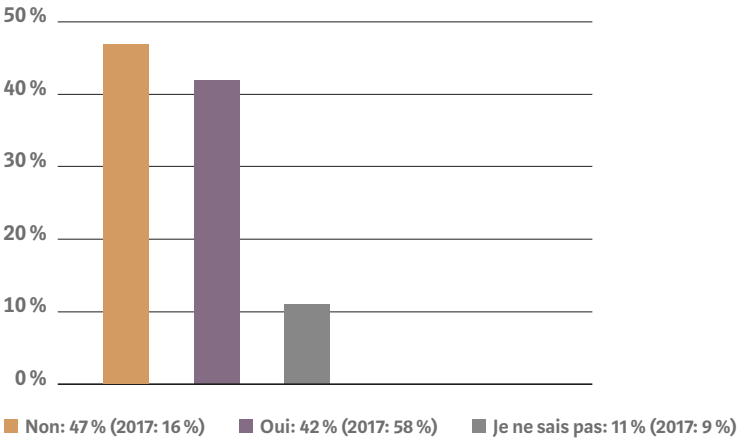
Lorsque les entreprises quantifient les cyberincidents, 34 % des sondés évaluent les répercussions financières entre CHF 1 et 10 millions (graphique 6), alors que 25 % estiment que les dommages sont supérieurs à CHF 10 millions. Nous avons constaté que parmi les entreprises qui évaluent le montant d'un cybersinistre à moins de CHF 1 million, 47% réalisent un chiffre d'affaires de CHF 100 millions au maximum.

La quantification des cybersinistres potentiels représente toujours l'un des plus grands défis dans le processus. On ne dispose toujours pas de données empiriques fiables. Il semblerait que des premiers chiffres soient disponibles, mais les assureurs restent très réticents à publier des données y compris anonymisées.

L'exemple des cyberattaques lancées contre le groupe hôtelier Marriott entre 2014 et 2018, révélé en automne 2018, montre l'importance que peut avoir une estimation approximative du cyberrisque résiduel. Les seuls frais de notification suite à un piratage de données personnelles sensibles seraient relativement faciles à calculer. Il est d'autant plus étonnant que la prétendue couverture d'assurance en vigueur ne suffise même pas à couvrir ces frais de notification.

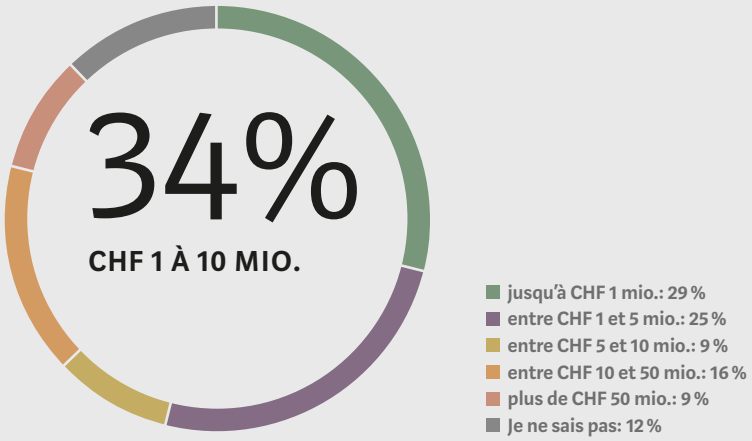
GRAPHIQUE 5

Avez-vous évalué les répercussions financières d'un cyberévénement dans votre entreprise?



GRAPHIQUE 6

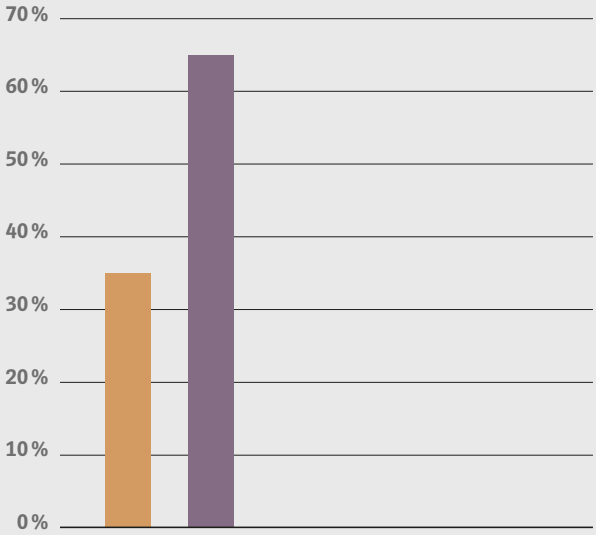
Si votre entreprise a évalué les répercussions financières d'un cybersinistre, quel est le montant maximal de la perte potentielle?



3

GRAPHIQUE 7

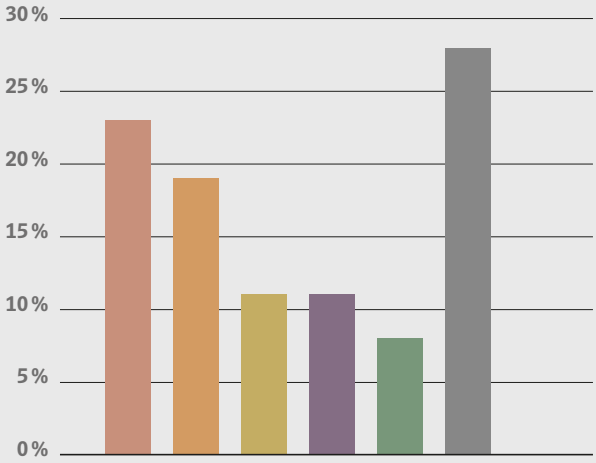
Votre entreprise a-t-elle élaboré au cours des 12 à 24 derniers mois un plan de réaction d'urgence aux cyberévénements?



- Oui: 35 % (2017: 29 %)
- Non: 65 % (2017: 61 %)
- Je ne sais pas: 0 % (2017: 10 %)

GRAPHIQUE 8

Si votre entreprise n'a pas élaboré de plan de réaction d'urgence aux cyberévénements, pouvez-vous en expliquer la raison?



- Les cyberincidents sont couverts dans d'autres plans de crise et n'exigent pas un traitement spécifique: 23 % (2017: 7 %)
- La cybersécurité/les pare-feu sont suffisants pour empêcher les cyberincidents: 19 % (2017: 18 %)
- L'organisation ne dispose pas du savoir-faire requis: 11 % (2017: 9 %)
- Le cyberrisque est trop faible pour justifier la mise en place de plans d'urgence: 11 % (2017: 4 %)
- Nous considérons qu'il ne s'agit pas d'une priorité: 8 % (2017: 7 %)
- Je ne sais pas: 28 % (2017: 16 %)

S'en remettre uniquement à de l'espoir est rarement conseillé. Les entreprises qui estiment que les cyberrisques font partie des dix risques majeurs devraient faire figurer l'élaboration d'un plan de réaction en cas d'urgence en tête de leur liste de priorités. Le traitement des cyberincidents qui menacent une entreprise doit être planifié et faire l'objet de formations. Celui qui prévoit le scénario le plus pessimiste – ce qui devrait être le cas de tous ceux qui comptent les cyberrisques parmi les risques majeurs de l'entreprise – abandonne celui-ci au fait du hasard s'il n'a pas de plan de réaction approprié en cas d'urgence. La planification d'urgence des scénarios les plus pessimistes, tout comme la planification du financement des risques, font partie du domaine de compétences de la direction stratégique de l'entreprise. L'équipe d'intervention en cas d'incident informatique (en anglais, Computer Incident Response Team ou CIRT), en revanche, travaille au niveau opérationnel et tactique et veille à garantir au mieux la sécurité des «joyaux de la couronne».

EN L'ABSENCE D'ENTRAÎNEMENT, LE BATEAU RISQUE DE CHAVIRER: CELUI QUI S'ENTRAÎNE À LA PRATIQUE DE LA VOILE EN CAS DE TEMPÊTE A DE BIEN MEILLEURES CHANCES DE SURVIE PAR GROS TEMPS EN PLEINE MER.

Seuls 35 % des sondés déclarent avoir élaboré de plan de réaction d'urgence au cours des 12 à 24 derniers mois (graphique 7). Et ce, bien que 59 % de ceux ayant évalué le scénario le plus pessimiste estiment à plus d'un million de francs le montant moyen des dommages suite à un cyberincident (graphique 5). L'absence de plan de crise s'explique d'une part par le fait que les cyberincidents sont déjà intégrés dans d'autres plans de crise et d'autre part - comme c'était déjà le cas l'an passé - par l'existence d'un système de cybersécurité ou de pare-feu suffisant (graphique 8).

S'agissant du plan de mesures d'urgence, le RGPD apporte une contribution indirecte non négligeable. Depuis le 25 mai 2018, les entreprises concernées sont tenues notamment de remplir leurs obligations de notification après un incident lié à la sécurité des données; l'accomplissement de cette obligation implique quasiment l'élaboration d'un plan de mesures d'urgence (voir également le graphique 16).

3

A l'instar des deux années précédentes, la plupart des entreprises suisses redoutent une perte d'exploitation liée à un cyberévénement. Le dommage de réputation constitue la seconde menace la plus importante, suivie par les dommages aux données/logiciels. Viennent ensuite la perturbation/l'interruption d'installations industrielles ou d'équipements d'exploitation, la compromission de données clients, les extorsions/ransomware, la violation du règlement général de l'UE sur la protection des données ou d'autres lois sur la protection des données, la perte/le vol de propriété intellectuelle ainsi que les dommages matériels/corporels (graphique 9).

La perte d'exploitation consécutive à une cyberattaque, tout comme les scénarios en relation avec des données personnelles, constituent à juste titre les menaces les plus redoutées; en définitive, ce sont ces sinistres qui représentent généralement les plus grands générateurs de coûts. Et ce, parce que les criminels responsables du sinistre savent parfois bien effacer leurs traces. Au final, malgré le dépôt d' une plainte contre X, ce sont les entreprises qui doivent supporter l'ensemble des frais, auxquels s'ajoute une forte augmentation d'un sentiment d'insécurité.

GRAPHIQUE 9

Quels scénarios de cyberattaque constituent la plus grande menace pour votre entreprise?

	Suisse
Perte d'exploitation	65 % (2017: 86 %)
Dommages de réputation	49 % (2017: 57 %)
Dommages aux données/logiciels	39 % (2017: 53 %)
Interruption d'installations industrielles ou d'autres équipements d'exploitation	28 % (2017: 33 %)
Compromission de données clients	25 % (2017: 52 %)
Extorsion/ransomware	25 % (2017: 37 %)
Violation du RGPD ou d'autres lois sur la protection des données	22 % (2017: n.d.)
Perte/vol de propriété intellectuelle	16 % (2017: 22 %)
Responsabilité vis-à-vis de tiers suite à une intrusion dans un système	15 % (2017: 30 %)
Dommages matériels/corporels	6 % (2017: 11 %)
Autre	2 % (2017: 34 %)
Je ne sais pas	3 % (2017: 2 %)

Des données clients et de production intègres et protégées contre l'accès de tiers ainsi que le respect des délais de livraison convenus contractuellement contribuent dans une large mesure à garantir une réputation irréprochable.

En 2018, à la suite notamment du comportement d'Uber (découverte de la dissimulation d'un piratage informatique de 2016 qui a fait 57 millions de victimes), de Swisscom (communication tardive, au bout de quelques mois, d'une perte de données intervenue en 2017 et qui a fait 800 000 victimes) et de Linked In (découverte d'une pratique de LinkedIn Europe consistant à collecter sans leur accord les adresses e-mail de 18 millions de non-utilisateurs, à traiter les données aux Etats-Unis avant de les transmettre à Facebook pour des publicités ciblées), il est apparu que les entreprises essayaient, dans la mesure du possible, de passer sous silence les problèmes liés aux données ou les utilisations frauduleuses découvertes trop tardivement. Le groupe hôtelier Marriott, en revanche, a informé ses clients de manière exemplaire, par e-mail, suite au piratage informatique découvert en automne 2018.

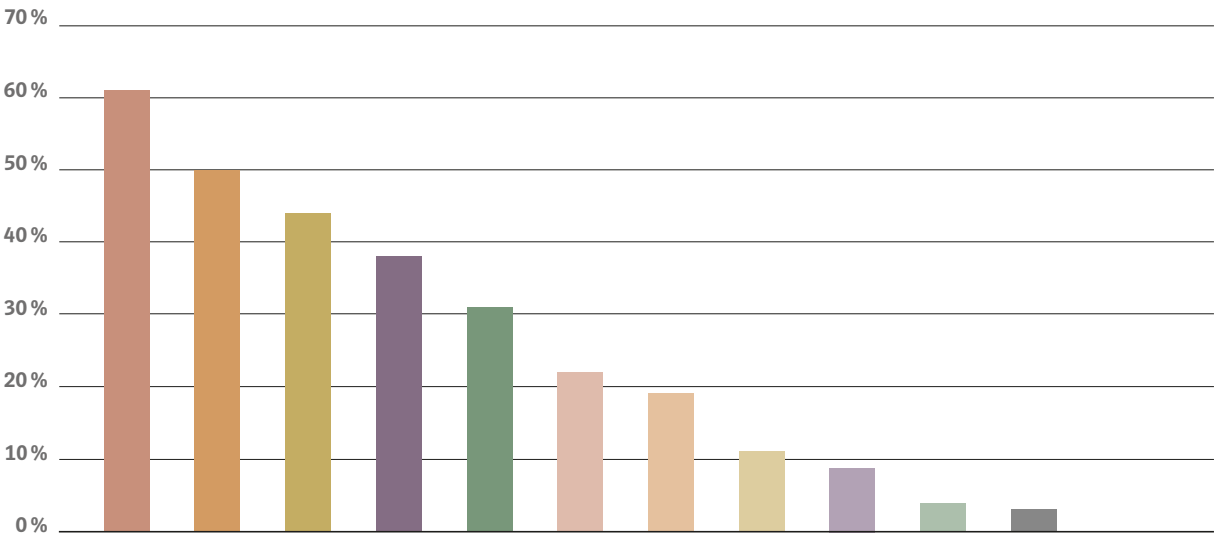
Une orientation clients transparente en cas de crise a également une influence, généralement positive, sur la réputation de l'entreprise.

A l'instar de l'année précédente, la décision coût-utilité «Pouvons-nous/voulons-nous nous permettre une amende ou un dommage de réputation?» exigera dans tous les cas de nouvelles stratégies en matière de transparence et de coûts de la part des entreprises.

3

GRAPHIQUE 10

Quelles menaces vous préoccupent le plus par rapport à une cyberattaque lancée pour installer un malware?



- Menace motivée par des raisons financières, p. ex. criminalité organisée et/ou groupes de hacktivistes: 61 % (2017: 43 %)
- Défaillance humaine de collaborateurs ou de partenaires contractuels: 50 % (2017: 21 %)
- Collaborateur ou tiers malveillant ayant un accès autorisé aux ressources IT de notre entreprise: 44 % (2017: 27 %)
- Défaillance technique/défaut de fonctionnement: 38 % (2017: 8 %)
- Incendie/événements naturels: 31 % (2017: n.d.)
- Coupure Internet: 22 % (2017: n.d.)
- Panne de courant: 19 % (2017: n.d.)
- Attaque physique contre le matériel: 11 % (2017: n.d.)
- Menace motivée politiquement: 9 % (2017: 2 %)
- Autre: 4 %
- Je ne sais pas: 3 %

Les vagues de cyberattaques de juin 2017, occasionnées par les cryptovirus WannaCry, Petya et NotPetya, soulignent de manière impressionnante la monoculture informatique qui règne en Europe, l'imprévisibilité et l'importance du facteur humain. Ces éléments jouent un rôle tout particulier, notamment lorsqu'on permet, d'un simple «clic» effectué par inadvertance, l'installation du malware dans le réseau de l'entreprise.

Une étape importante pourrait être franchie si le risque résiduel lié à des collaborateurs potentiellement criminels ou facilement manipulables était intégré de façon objective dans l'analyse des cyberrisques. Nous estimons désormais à 95 % au moins le risque résiduel émanant de l'être humain. Dans 50 à 80 % des cas, nous partons du principe qu'il s'agit d'auteurs possédant un savoir-faire interne – que celui-ci ait été acquis dans le cadre d'un emploi passé ou actuel. C'est pourquoi des mesures préventives doivent être mises en œuvre là où le dommage pourrait être le plus important. Les personnes clés du secteur informatique, qui possèdent des droits d'administrateurs étendus, ou d'autres personnes clés devraient être contrôlées en priorité selon le principe need-to-know. Il est illogique et disproportionné qu'un virement bancaire à partir de CHF 1000.– nécessite une double signature, alors que des collaborateurs IT disposant de droits d'administrateurs étendus peuvent en quelques clics paralyser l'entreprise.

3

3.4 LA GESTION DES CYBERRISQUES ÉMANANT DES SOUS-TRAITANTS

On oublie trop souvent les cyberrisques émanant des sous-traitants IT. Force est de constater que les entreprises subissent de plus en plus fréquemment des attaques par le biais de leurs sous-traitants IT. Plus la dépendance vis-à-vis de partenaires d'externalisation externes est grande, plus la défaillance de ces derniers devrait être intégrée dans la gestion des cyberrisques de l'entreprise. Dans l'idéal, l'accent devrait être mis sur l'ensemble de la chaîne de création de valeur. A l'heure actuelle, les entreprises ne peuvent plus être considérées isolément.

La responsabilité pour les dommages occasionnés par les sous-traitants IT est tout d'abord assumée par l'entreprise. Les risques de responsabilité qui peuvent en découler doivent généralement être préfinancés par les entreprises, ce qui implique de disposer de liquidités correspondantes. Parmi les autres inconvénients figurent le risque de perte de contrôle sur les données, l'absence de cloisonnement des différents traitements de données par rapport à d'autres utilisateurs du cloud, les risques de compliance, les effets «lock-in» ainsi que l'accès d'autorités étrangères aux données de l'entreprise.

LES CERTIFICATIONS ISO DES SOUS-TRAITANTS NE GARANTISSENT PAS UNE MEILLEURE CYBERSÉCURITÉ.

A présent, 47 % des entreprises évaluent leurs sous-traitants du point de vue des menaces liées aux cyberrisques, alors qu'en 2017, elles n'étaient que 33 %. Ce résultat réjouissant reflète une prise de conscience croissante pour ce sujet important.

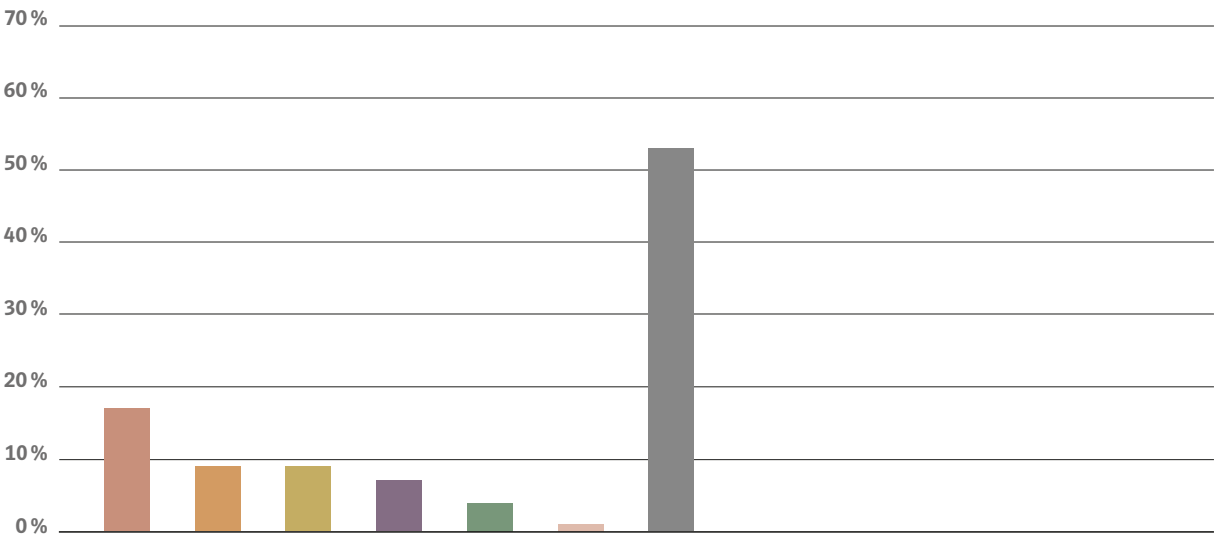
Le graphique 11 montre clairement que l'inventaire des relations avec les sous-traitants fait partie des mesures encore peu répandues. En plus de l'inventaire, les thèmes suivants devraient également être documentés: droits d'accès aux données et systèmes de l'entreprise, évaluation des sous-traitants du point de vue de la cybersécurité ainsi que demande de garanties en matière de monitoring ou autres mesures de protection, accords contractuels portant sur les limites de responsabilité pour les pertes consécutives à des cyberattaques, analyse de la capacité financière des sous-traitants et obligation pour ces derniers de souscrire eux-mêmes une cyberassurance.

L'absence d'inventaire, et par conséquent le grand manque de transparence concernant les relations quantitatives et qualitatives avec les sous-traitants IT, nous préoccupent beaucoup. Ce manque de transparence doit être assimilé à l'ignorance, et l'ignorance est dangereuse.

Une mesure préventive semble évidente en tout cas: l'existence d'une liste de sous-traitants peut apporter de la transparence et améliorer la compréhension des dépendances en cas de cybersinistre. On comprend dès lors que le cyberassureur exige de la transparence sur toute la chaîne de valeur IT externe des entreprises assurées.

GRAPHIQUE 11

Quelles mesures votre entreprise prend-elle pour évaluer et gérer le cyberrisque émanant de votre fournisseur et d'autres tiers?



- Inventaire des relations fournisseurs et des droits d'accès aux données: 17 % (2017: 31 %)
- Evaluation des sous-traitants du point de vue de la cybersécurité ainsi que demande de garanties en matière de cybersécurité: 9 % (2017: 12 %)
- Dispositions contractuelles concernant les limites de responsabilité pour les cyberpertes: 9 % (2017: 10 %)
- Surveillance régulière des fournisseurs du point de vue de leur conduite en matière de cybersécurit: 7 % (2017: 8 %)
- Analyse de la capacité financière des fournisseurs: 4 % (2017: 5 %)
- Obligation des fournisseurs de souscrire une cyberassurance: 1 % (2017: 1 %)
- Nous n'évaluons pas nos sous-traitants ou je ne sais pas: 53 %

3

3.5 LES CONCLUSIONS DE CYBERASSURANCES SONT EN AUGMENTATION

Le paysage de la cyberassurance évolue en permanence en Europe et en Suisse. Les offres d'assurance sont toujours difficiles à comprendre pour les non-spécialistes. Il est dès lors indispensable de faire appel à un conseil professionnel et d'examiner les besoins de couverture individuels. Suite à l'augmentation des risques cumulés, les garanties des entreprises liées à leurs propres normes de sécurité IT et de compliance gagneront en importance à l'avenir. Les assureurs seront à l'avenir de moins en moins disposés – à juste titre – à fournir des assurances les yeux fermés.

Une cyberassurance doit compenser les pertes d'actifs consécutives à un cyberincident. Pour cette raison, le transfert de risque ne doit pas être examiné en vertu d'un quelconque effet de mode, mais, chaque année, sous l'angle du rapport coût-utilité.

Nous considérons comme réaliste le fait que 16 % des participants au sondage disposent déjà d'une cyberassurance: 70 % des sondés appartiennent au secteur de PME, avec un chiffre d'affaires allant jusqu'à CHF 250 millions. En raison des conditions d'assurance intéressantes, ce sont les petites et moyennes entreprises qui souscrivent actuellement le plus grand nombre de polices; elles ne le font pas uniquement par l'intermédiaire d'un courtier, mais aussi directement auprès de leur assureur.

Cette année, 387 clients et non-clients de Kessler ont participé au sondage de façon anonyme. 16 % déclarent avoir conclu une cyberassurance, alors que 23 % envisagent de souscrire une assurance correspondante ou d'augmenter la somme de couverture dans les 12 prochains mois. 12 % déclarent ne pas avoir de cyberassurance, mais avoir couvert certains risques par le biais de leurs polices d'assurance conventionnelles. Et 31 % ne prévoient pas actuellement de conclure une police d'assurance contre les cyberrisques (graphique 12).

> LES CYBERRISQUES CONTINUENT D'AUGMENTER. LES CYBERRISQUES INDIVIDUELS DOIVENT ÊTRE ÉVALUÉS ET ASSURÉS AU MIEUX. UN CONSEIL PROFESSIONNEL EST INDISPENSABLE.

GRAPHIQUE 12

Quel est le positionnement actuel de votre entreprise en matière de cybercouverture?

- Mon organisation n'a pas de cyberassurance et ne prévoit pas d'en conclure: 31 % (2017: 16 %)
- Mon organisation prévoit de conclure une cyberassurance dans les 12 prochains mois ou d'augmenter la somme de couverture: 23 % (2017: 29 %)
- Mon organisation a conclu une cyberassurance: 16 % (40 %)
- Mon organisation n'a pas de cyberassurance, mais nous disposons d'une cyber-couverture dans le cadre d'autres polices: 12 % (2017: n.d.)
- Je ne sais pas: 18 % (2017: 15 %)

3

GRAPHIQUE 13

Si votre entreprise a conclu une cyberassurance ou si elle souhaite augmenter la couverture, quels sont les facteurs qui l'y ont incitée?

- Plan de gestion des cyberrisques: 51 % (2017: 44 %)
- Mandat du conseil d'administration: 14 % (2017: 26 %)
- A elle-même été victime d'une cyberattaque: 10 % (2017: 10 %)
- Exigences réglementaires comme p. ex. le RGPD: 7 % (2017: 16 %)
- Cyberattaque contre d'autres entreprises: 4 % (2017: 30 %)
- Obligation de justifier d'une assurance: 4 % (2017: 3 %)
- Autres: 7 % (2017: n.d.)
- Je ne sais pas: 3 % (2017: 13 %)

GRAPHIQUE 14

Si votre entreprise n'a pas conclu de cyberassurance, quelles en sont les raisons?

- Manque de coordination interne sur les besoins: 23 % (2017: 14 %)
- Nous n'avons pas besoin de cyberassurance car notre cybersécurité est suffisante: 21 % (2017: 17 %)
- La cyberassurance n'offre pas une couverture suffisante des coûts: 19 % (2017: 62 %)
- La couverture disponible n'est pas bien comprise: 10 % (2017: 21 %)
- La cybercouverture est intégrée dans une autre police: 10 % (2017: 14 %)
- Budget ou ressources insuffisants: 8 % (2017: 7 %)
- Nos cyberrisques sont supportés par notre captive: 1 % (2017: 3 %)
- Autres motifs: 26 % (2017: n.d.)
- Je ne sais pas: 9 % (2017: 3 %)

Plus de la moitié des sondés qui ont déjà conclu une cyberassurance ou qui envisagent d'augmenter leur somme de couverture, indiquent que c'est le plan actuel de gestion des cyberrisques qui les a poussés à agir (graphique 13). Cela est compréhensible, car celui qui ouvre la boîte de Pandore reconnaît assez rapidement son potentiel de risque.

Selon le sondage, la gestion des cyberrisques constitue, à 51 %, la principale raison, et de loin, qui incite à conclure une cyberassurance ou à procéder à une augmentation de couverture. Les sinistres survenant dans d'autres entreprises ne semblent pas faire forte impression auprès des sondés. Seuls 10 % y voient une incitation à souscrire une cyberassurance ou à augmenter la couverture. De même, la stratégie descendante (top-down) de financement des cyberrisques ne constitue actuellement un incitateur que pour un faible pourcentage de sondés (14 %): nous considérons le conseil d'administration comme un futur moteur important pour lancer la discussion sur les cyberrisques. Et ce, déjà par le seul fait de son obligation légale d'opter en connaissance de cause pour une stratégie de financement des cyberrisques, si le cyberrisque devait être considéré comme un risque majeur dans l'entreprise (voir également le graphique 1).

43 % des entreprises suisses n'ont pas de cyberassurance, n'ont pas l'intention d'en souscrire une, ne disposent pas d'un plan correspondant ou déclarent ne pas avoir de cyberassurance parce que certaines composantes de couverture ayant trait aux cyberrisques sont couvertes dans d'autres polices d'assurance (graphique 12). Les principaux motifs invoqués cette année sont l'absence de concertation interne sur le besoin de cyberassurance ainsi que le bon niveau de cybersécurité existant dans l'entreprise. La couverture insuffisante des coûts est toujours invoquée, mais ne constitue plus le principal motif comme c'était le cas l'année dernière (graphique 14).

4
LE RGPD RENFORCE LA GESTION DES CYBERRISQUES

4.1 LES COÛTS RELATIFS AUX VIOLATIONS DE LA LÉGISLATION SUR LA PROTECTION DES DONNÉES

Les coûts des violations de la législation sur la protection des données sont calculables et en grande partie assurables. La décision de mettre en œuvre le RGPD de manière judicieuse doit dès lors faire partie des mesures prises par la direction. Le RGPD renforce la gestion des cyberrisques.

On peut considérer que les sinistres liés à des cyber-attaques en Europe feront à l'avenir l'objet d'un nombre de prétentions de plus en plus élevé dans le cadre des assurances D&O et des cyberassurances; cela aura des conséquences sur la prise en compte des risques cumulés, qui doivent déjà être pris en considération dans le processus de souscription des assureurs et des réassureurs.

Les développements juridiques actuels dans le domaine de la protection des données renforcent la sensibilisation des entreprises en matière de gestion des cyberrisques et de cyber-résilience. En effet, le RGPD oblige pratiquement la direction de l'entreprise à se pencher sur les problèmes de gestion des cyberrisques et de protection des données. Les coûts risquent d'être élevés. Par ailleurs, le droit de recours des associations, autorisé par le RGPD et déjà en vigueur en Allemagne, sera inscrit à l'ordre du jour des séances des conseils d'administration en Suisse également dans le cadre de la prochaine révision du CPC. La possibilité de recours prévue aura pour effet d'augmenter encore de façon significative la sensibilisation aux cyberrisques et à la protection des données.

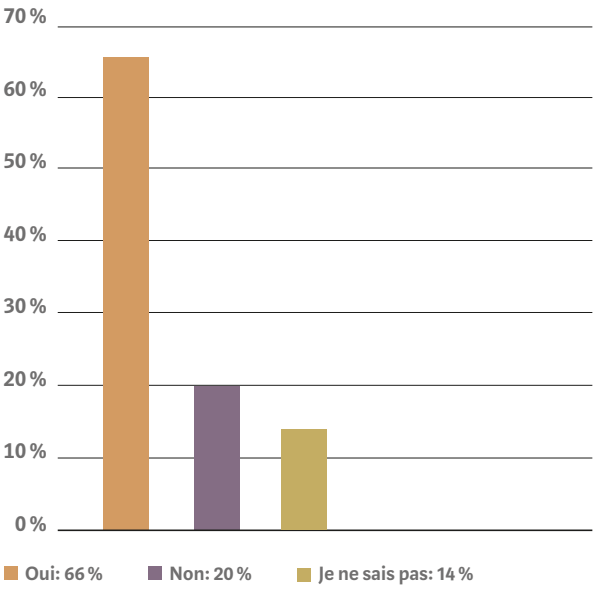
Si vous connaissez les lois applicables en matière de protection des données, vous pouvez remplir les obligations requises en cas de fuite de données et mettre en œuvre des mesures opérationnelles ciblées pour éviter des procédures officielles relatives à la protection des données, des amendes et d'autres frais consécutifs. Certains secteurs voient dans la cyberassurance un intérêt car les coûts encourus en cas de violation de la protection des données sont en grande partie couverts.

Parmi les entreprises interrogées, 66 % entrent dans le champ d'application du RGPD, 20% ne sont pas concernées et 14 % ne savent pas (graphique 15).

Parmi les entreprises soumises au RGDP, 49 % ont déclaré à l'automne 2018 disposer d'un plan de réaction en cas de violation des dispositions sur la protection des données (graphique 16). Cette évolution est réjouissante. L'année précédente, elles étaient seulement 23 %. Il est frappant de constater qu'à l'heure actuelle, 35 % d'entre elles ne disposent toujours pas d'un plan de réaction approprié, bien que le RGPD soit applicable depuis le 25 mai 2018 aux pays de l'UE et depuis le 30 juillet 2018 aux pays de l'EEE. Le RGPD n'impose pas de plan de réaction en cas de cyberincidents, mais demande que les autorités de surveillance soient informées dans les 72 heures suivant la constatation d'un incident lié à la sécurité des données. Il est évident que ce délai a plus de chances d'être respecté avec un plan de réaction que sans.

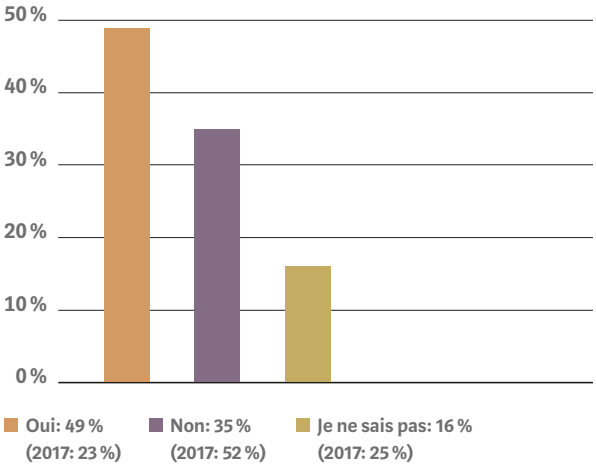
GRAPHIQUE 15

Votre organisation est-elle soumise au RGPD?



GRAPHIQUE 16

Si votre entreprise est soumise au RGPD, avez-vous élaboré un plan de réaction aux violations de la protection des données, qui prévoit notamment l'annonce dans les 72 h d'une violation du RGPD à l'autorité de surveillance au sein de l'UE?



5 CONCLUSIONS

ENSEIGNEMENTS

Les cyberrisques sont sur toutes les lèvres. La prise de conscience a eu lieu. Mais elle ne suffit pas à elle seule pour atteindre les objectifs de l'entreprise. Des mesures doivent être adoptées et un changement de mentalité est nécessaire: dans le quotidien numérique, il est indispensable d'avoir des données intègres, disponibles et protégées contre l'accès de tiers.

Les cyberrisques sont imprévisibles et entraînent divers coûts qui sont difficiles à anticiper. Et ce, notamment en raison du manque de transparence de la chaîne d'approvisionnement IT et du maillon le plus faible dans la chaîne de sécurité IT, à savoir l'être humain, avec ses caractéristiques typiques comme la serviabilité, la crédulité, la rancune, l'avidité, la fierté, l'égoïsme et la peur. Tous ces facteurs peuvent influencer le comportement humain et transformer un collaborateur motivé en criminel. Ce sont les attaques ciblées, associées à du savoir-faire interne, qui ont le potentiel de dommages le plus important.

Le catastrophisme systématique est destructeur, mais il en faut une petite dose pour protéger l'entreprise contre les cyberrisques et mettre en œuvre les mesures de prévention adaptées. Les failles de sécurité les plus critiques au sein du système et de l'organisation sont sans doute identifiées si l'on adopte l'état d'esprit d'un criminel.

BESOIN DE CONSEIL

Le traitement des cyberrisques résiduels est et restera une tâche complexe et exigeante. Nous estimons qu'il existe également un besoin de conseil pour l'attribution de la responsabilité en matière de cyberrisques et pour la quantification de ces derniers dans l'entreprise et, de façon accrue, pour la mise en œuvre de mesures de prévention diversifiées et appropriées. L'argument majeur en faveur d'un transfert des cyberrisques réside dans l'imprévisibilité du facteur humain, qui est aujourd'hui considéré comme la principale cause des cyberrisques. Les cyberrisques sont des risques d'entreprise, qui doivent faire l'objet d'un examen annuel sur la base du principe coûts-utilité afin de déterminer dans quelle mesure ils doivent être assurés.

Vous avez des questions? Demandez un entretien-conseil personnel:

Pascal Schweingruber
Membre du Comité de direction
pascal.schweingruber@kessler.ch
T +41 44 387 87 65

Melanie Koller
Legal Counsel Cyber Risk
melanie.koller@kessler.ch
T +41 44 387 88 39

KESSLER EN BREF

Kessler est l'entreprise suisse leader dans le domaine du conseil en matière de risques, d'assurances et de prévoyance. Grâce à notre savoir spécialisé, à l'expérience de nos collaborateurs et à notre force d'innovation, ainsi qu'à notre position sur le marché, nous offrons une valeur ajoutée durable à nos clients des secteurs des services, du commerce et de l'industrie. Notre excellente réputation ainsi que notre réussite économique assurent notre pérennité en tant qu'entreprise familiale indépendante. Fondée en 1915, Kessler emploie actuellement 275 collaborateurs à son siège de Zurich et dans ses succursales à Aarau, Bâle, Berne, Genève, Lausanne, Lucerne, Neuchâtel, Saint-Gall et Vaduz. En tant que partenaire suisse de Marsh, nous faisons partie d'un réseau de spécialistes issus de tous les domaines de la gestion des risques et disposons d'une grande expérience dans le suivi des programmes d'assurance mondiaux. Marsh est le courtier en assurances et le conseiller en risques leader dans plus de 100 pays et fait partie de Marsh & McLennan Companies dont les actions sont négociées sur les Bourses de New York, Chicago et Londres (sigle boursier: MMC).

Vous trouverez des informations complémentaires sur www.kessler.ch, www.marsh.com, www.mmc.com.

KESSLER & CO SA
Forchstrasse 95
Case postale
CH-8032 Zurich
T +41 44 387 87 11
www.kessler.ch

Marsh Network