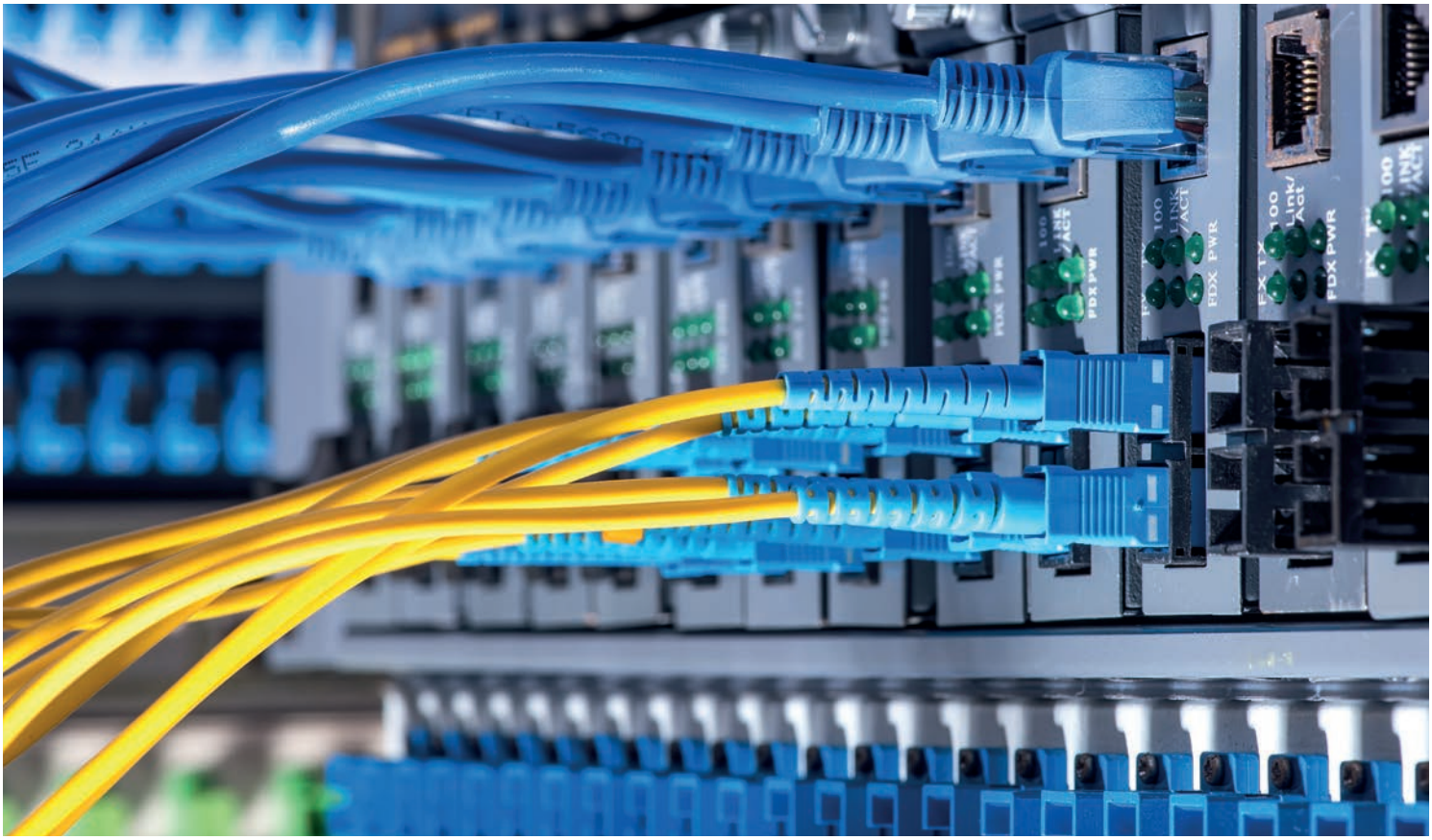
KESSLER

RAPPORT DU SONDAGE SUR LES CYBERRISQUES 2018
LES CYBERRISQUES DU POINT DE VUE DE LA SUISSE



EN AVANT, SEREINEMENT.

RAPPORT DU SONDAGE SUR LES CYBERRISQUES 2018
LES CYBERRISQUES DU POINT DE VUE DE LA SUISSE

1
AVANT-PROPOS

OPPORTUNITÉS DE LA NUMÉRISATION

La numérisation a des répercussions fondamentales sur les entreprises ainsi que sur leurs relations commerciales et leurs relations avec les clients. L'Internet des objets (Internet of Things – IoT) offre des commodités et de nouvelles interfaces numériques, mais crée également de nombreuses nouvelles failles.

La numérisation doit être considérée comme une chance, mais ne doit pas exposer les entreprises à des dangers disproportionnés. Il convient de connaître et de protéger les données précieuses et les processus d'affaires importants. Le règlement général sur la protection des données de l'UE (RGPD) soutient cette approche: la gestion des cyberrisques trouve sa légitimité dans le RGPD.

LE FACTEUR DE RISQUE GESTION DE LA CHAÎNE D'APPROVISIONNEMENT

L'utilisation croissante de services d'externalisation réduit les frais d'exploitation, mais se fait généralement au détriment de la transparence des données, en particulier en ce qui concerne l'endroit où se trouvent les données ainsi que les personnes qui y ont accès. La défaillance d'un système informatique géré de manière centrale recèle un cumul de risques difficilement calculables. Ainsi par exemple, divers secteurs ou sites de l'entreprise peuvent être touchés simultanément et de façon différente par une cyberattaque, ou bien une attaque dirigée contre un fournisseur IT permet d'accéder à l'ensemble des systèmes IT et logiciels de différentes sociétés. Ainsi que le montre le présent sondage, la dépendance vis-à-vis des sous-traitants n'est malheureusement pas encore suffisamment prise en compte dans le processus de gestion des cyberrisques.

LE SONDAGE DE MARSH

Notre partenaire réseau Marsh a réalisé en mai 2017 un sondage intersectoriel mondial, qui analyse la façon dont les entreprises gèrent les cyberrisques ainsi que les dangers potentiels de ces derniers dans les activités quotidiennes, y compris les aspects juridiques que cela implique en matière de protection de données. Nous nous y sommes associés et avons invité tous nos clients opérant à l'international à participer au sondage mondial sur la perception des cyberrisques («Global Cyber Risk Perception Survey»). Les résultats ont été publiés par Marsh fin février 2018.

LA SUISSE INTOUCHABLE?

Les menaces en provenance du cyberespace ne s'atténueront pas ces prochaines années. Le monde numérique ne s'arrête pas aux frontières suisses. Nos entreprises l'ont bien compris. Ainsi que le rapport le confirme, un certain nombre de choses sont déjà connues, mais il manque une mise en œuvre ciblée.

Nous avons évalué ci-après des résultats du sondage de Marsh pour la Suisse et commenté pour vous les principaux enseignements.

Nous vous souhaitons une lecture passionnante 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 mondial sur la perception des cyberrisques («Global Cyber Risk Perception Survey»), réalisé par Marsh en février 2018. Les principaux enseignements du point de vue de la Suisse sont rassemblés et commentés ci-après.

Plus de 1860 entreprises du monde entier ont participé au sondage sur les cyberrisques, dont 386 entreprises européennes, 178 (15 %) faisant partie de nos clients suisses.

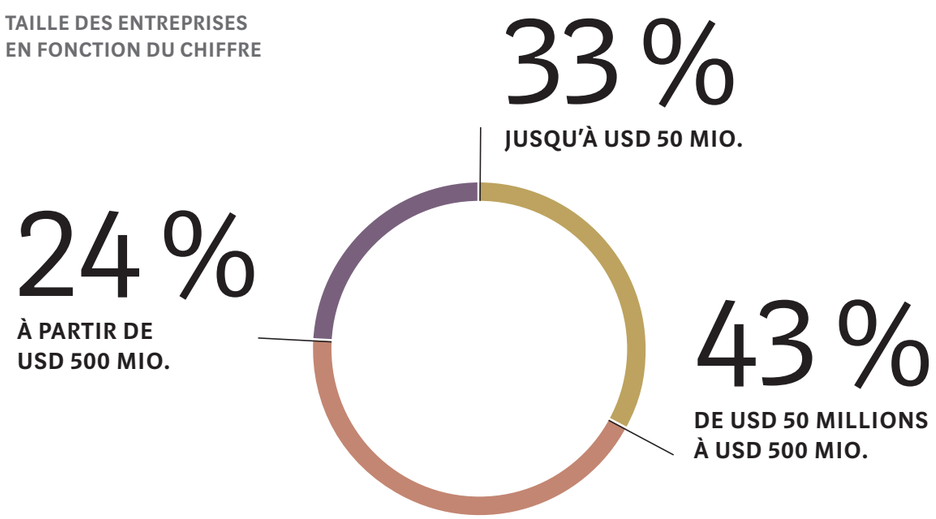
33 % des entreprises ayant participé au sondage génèrent un chiffre d'affaires annuel allant jusqu'à 50 millions de dollars, et 43 % réalisent un chiffre d'affaires compris entre 50 et 500 millions. Parmi les entreprises dont le chiffre d'affaires est supérieur à 500 millions, 24 % sont représentées dans ce sondage.

Les secteurs d'appartenance des participants suisses sont multiples. Le secteur de l'énergie, de l'électricité, de l'approvisionnement et des infrastructures, qui compte pour un quart, est le plus fortement représenté. L'intérêt manifesté par ce dernier à participer au sondage ne nous surprend pas, car compte tenu de l'état actuel de la menace, les infrastructures critiques font partie des premières cibles des cyberattaques.

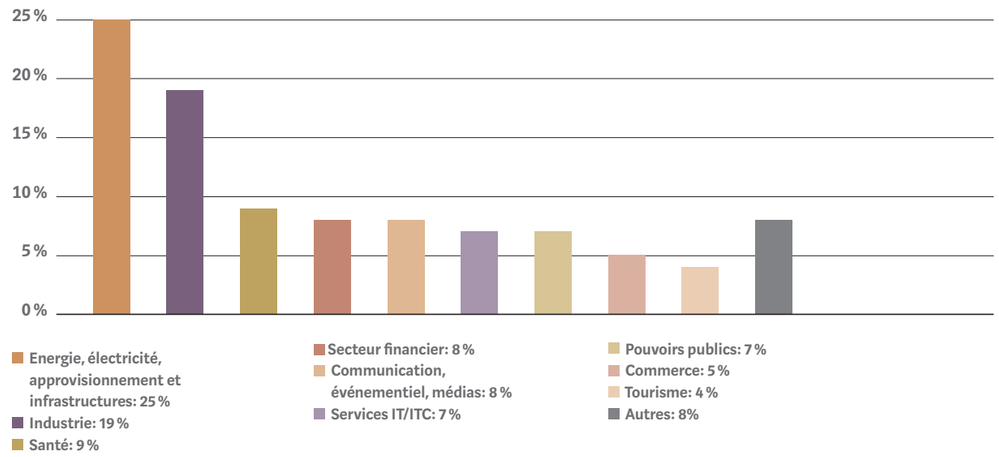
Outre la Suisse et l'Europe continentale, on compte également parmi les principaux marchés des participants au sondage les Etats-Unis/le Canada, le Royaume-Uni et l'Irlande ainsi que l'Asie.

A notre avis, la dépendance multiple et particulièrement forte des participants vis-à-vis des outils et services numériques est révélatrice (encadré à droite). Dans ce contexte, il est incontestable que le cyberrisque n'est pas un simple effet de mode, mais une conséquence de l'économie numérique d'aujourd'hui.

TAILLE DES ENTREPRISES EN FONCTION DU CHIFFRE



SECTEUR D'APPARTENANCE



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

- Un ou plusieurs ordinateurs sont reliés à Internet: 98 %
- Traitement électronique et sauvegarde de dossiers des collaborateurs: 88 %
- Les collaborateurs et les tiers peuvent connecter leurs appareils mobiles au réseau de l'entreprise: 87 %
- Sauvegarde électronique et/ou gestion de données clients: 86 %
- Traitement électronique d'informations bancaires: 75 %
- Sauvegarde électronique d'informations fournisseurs: 74 %
- Services cloud: 54 %
- Traitement électronique d'informations de santé privées de collaborateurs et de clients: 31 %
- Traitement électronique de transactions par carte de crédit: 28 %
- Saisie de données personnelles (y. c. cookies et dispositifs analogues) sur un site Internet: 25 %
- Transmission électronique de données personnelles à des fournisseurs ou à d'autres tiers: 24 %

3
ENSEIGNEMENTS ET COMMENTAIRES

3.1 LA PRISE DE CONSCIENCE DES CYBERRISQUES AUGMENTE

Du fait de leur médiatisation permanente, les cyberrisques peuvent difficilement être ignorés. Le problème ou la possibilité d'être soi-même touché semble connu dans une large mesure. Au vu des dommages potentiels des cyberincidents, force est de constater que trop peu d'efforts sont entrepris dans ce domaine.

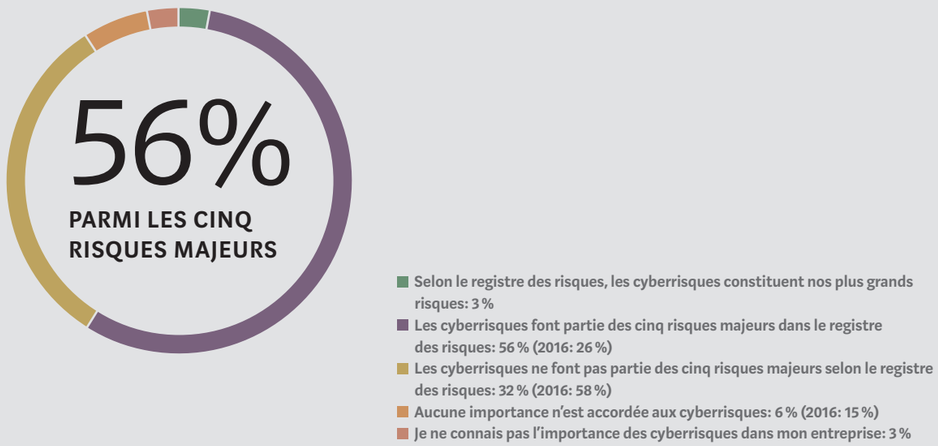
Les résultats du sondage de cette année confirment que les cyberrisques font désormais partie des risques majeurs dans le registre des risques des entreprises (graphique 1). Pour 56 % des entreprises suisses, les cyberrisques comptent d'ores et déjà parmi les cinq risques majeurs des entreprises (2016: 26 %).

Le classement des cyberrisques parmi les cinq risques majeurs des entreprises s'explique par la présence accrue dans les médias des sinistres liés à des cyberattaques, mais aussi par l'entrée en vigueur le 25 mai 2018 du RGPD de l'UE ainsi que par le constat croissant que la sécurité informatique à 100 % n'existe pas. Le sinistre majeur se produira, c'est simplement une question de temps. Pour s'y préparer, une sensibilisation accrue aux cyberrisques est largement insuffisante. Le fossé qui existe entre la perception des cyberrisques et la lutte menée pour y faire face est selon nous toujours trop important. Il existe indubitablement un besoin d'action dans ce domaine.

A la question de savoir si leur propre entreprise avait été victime d'une cyberattaque au cours des 12 derniers mois, 66 % des participants ont répondu par «Non», 24 % par «Oui» et 10 % par «Je ne sais pas» (graphique 2). On peut dès lors supposer que sur ces 66%, une partie des entreprises ayant répondu par «Non» n'ont pas encore remarqué qu'elles avaient été piratées. Il n'est pas rare que des logiciels malveillants ne soient découverts qu'après des semaines ou des mois, voire pas du tout.

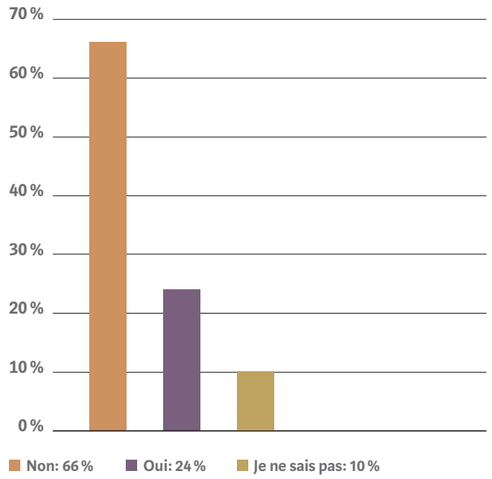
GRAPHIQUE 1

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



GRAPHIQUE 2

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



3

3.2 IMPORTANCE DE LA GOUVERNANCE D'ENTREPRISE

Nous considérons comme très positif le fait que la direction de l'entreprise ait tendance à assumer de plus en plus fréquemment la responsabilité de la gestion des risques (2017: 34 %; 2016: 13%). Néanmoins, ce sont encore principalement les domaines opérationnels qui sont responsables de la gestion des cyberrisques en Suisse. En règle générale, les inconvénients de cette répartition des responsabilités ne deviennent perceptibles que lors d'une cyberattaque.

A l'ère du Big Data et d'Industrie 4.0, il y aura un intérêt accru à voir si les dirigeants intègrent dans la planification financière d'éventuels scénarios de cyberattaques ou s'ils les négligent volontairement. Etant donné que 56 % des entreprises suisses considèrent que les cyberrisques font partie des cinq risques majeurs des entreprises (graphique 1), il faut espérer qu'à l'avenir, la responsabilité en matière de cyberrisques sera plus fréquemment assumée par l'échelon de direction stratégique.

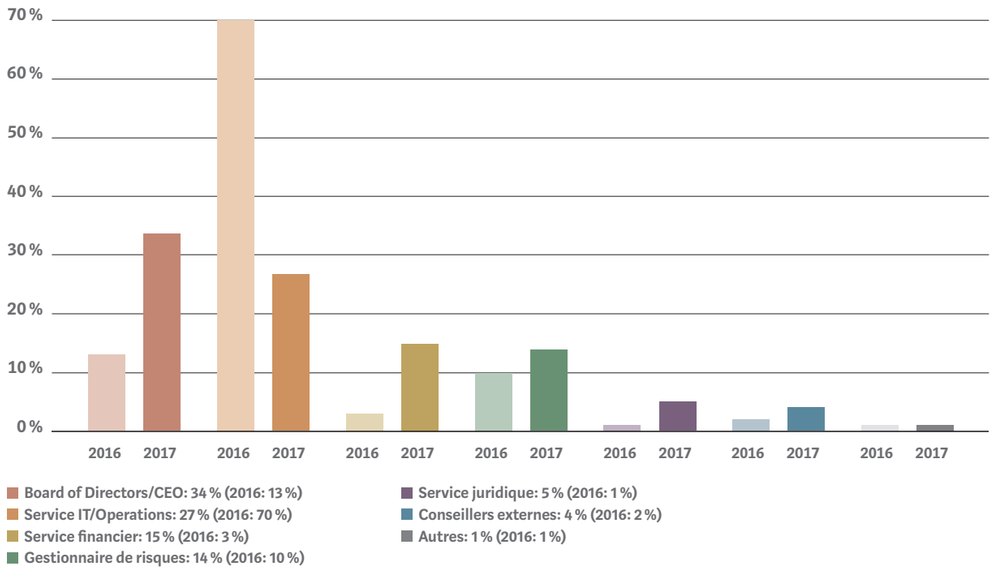
Que l'évaluation des risques constitue ou non une obligation légale dans le cadre d'un rapport annuel, la direction a tout intérêt à connaître et à budgétiser les risques de l'entreprise. En vertu de la loi de Murphy, selon laquelle tout ce qui peut aller de travers ira de travers, il faut en permanence s'attendre à des cybersinistres et par conséquent faire planifier soigneusement, par des spécialistes, les mesures destinées à y faire face.

En cas de faillite ou de cyberincident préjudiciable pour le bilan, on se retourne en priorité, en vertu de la loi, contre la direction de l'entreprise. La quantification des scénarios de cybersinistres qui n'ont pas encore eu lieu est et reste – tout au moins dans un avenir proche – le plus grand défi des entreprises et de toute l'économie mondiale. C'est précisément en raison de ces facteurs de coûts imprévisibles que la budgétisation sommaire des cyberrisques revêt plus que jamais une importance centrale. La Cyber Security Due Diligence et la Cyber Insurance Due Diligence sont également amenées à faire partie du quotidien dans le cadre du processus M&A. Plus aucun acheteur ne voudra plus se risquer à acheter les yeux fermés.

Bien que la direction de l'entreprise assume plus fréquemment que l'année précédente la responsabilité des cyberrisques, celle-ci continue d'incomber en priorité aux unités opérationnelles. Une première étape a cependant été franchie dans la mesure où aujourd'hui, ce ne sont plus les services informatiques, mais les services Finances et Risques qui sont responsables des cyberrisques au sein de l'entreprise (graphique 3). Grâce à cette redistribution des responsabilités au niveau opérationnel, on peut espérer que l'on se penchera de façon plus intensive sur la viabilité financière des cyberrisques résiduels.

GRAPHIQUE 3

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



3

3.3 GESTION DES CYBERRISQUES: QU'EST-CE QUE CELA APPORTE AUX ENTREPRISES?

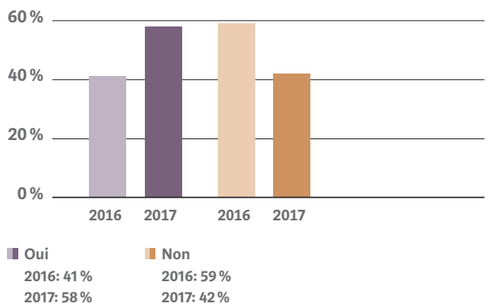
En théorie, identifier les cyberrisques et les maîtriser en connaissance de cause semble être une conséquence logique. Mais dans la pratique, lors de ce passage de la prise de conscience à l'action, la direction de l'entreprise manque de temps, de connaissances et de motivation pour aborder de façon proactive, à côté des autres risques majeurs de l'entreprise, cette grande inconnue que sont les «cyberrisques». Les cyberrisques ne disparaîtront pas au cours des prochaines années; c'est aux entreprises qu'il appartient d'être conscients de leur cyberexposition et d'améliorer la capacité de résistance de leur institution aux cyberévénements.

Déjà 58 % (contre seulement 41 % en 2016) des participants au sondage ont quantifié les répercussions financières d'un cyberévénement au sein de l'entreprise. Ces résultats sont réjouissants et montrent, une fois de plus, que les cyberrisques sont de plus en plus fréquemment considérés comme des risques à prendre au sérieux par les entreprises (graphique 4).

Lorsque les entreprises quantifient les cyberincidents, plus de la moitié d'entre elles évaluent les répercussions financières entre USD 1 et 10 millions (graphique 5). Dans le segment des PME, des dommages à partir de CHF 1 million peuvent déjà menacer l'existence des entreprises. Au vu du potentiel de dommages évoqué, il est d'autant plus surprenant que les mesures de cyberprévention aient pris un tel retard et qu'en dépit d'offres de couverture et de primes attrayantes, la demande de solutions de cyberassurance ait tendance à progresser lentement (graphique 6).

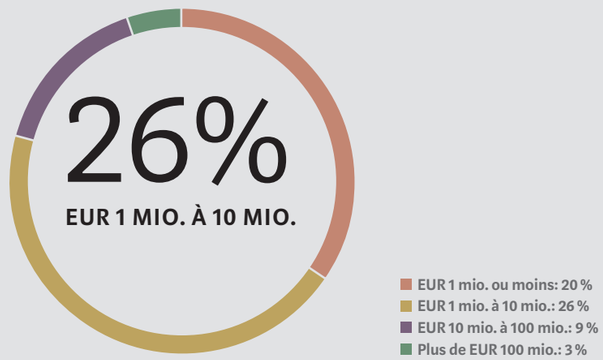
GRAPHIQUE 4

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



GRAPHIQUE 5

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



3

GRAPHIQUE 6

Parmi les mesures suivantes du processus de gestion des cyberrisques, lesquelles ont été mises en œuvre par votre entreprise au cours des 12 à 24 derniers mois?

ÉVALUER ET ANALYSER
- Estimation des répercussions financières des cyberincidents: 58 %
- Analyse des lacunes en matière de cybersécurité réalisée: 46 %
- Modélisation des scénarios potentiels de cyberpertes: 25 %

SÉCURISER ET ASSURER
- Cryptage des ordinateurs de bureau et des ordinateurs portables de l'entreprise: 54 %
- Authentification à facteurs multiples pour l'accès à distance au réseau de l'entreprise: 45 %
- Test de pénétration réalisé: 41 %
- Cyberassurance conclue: 40 %
- Mise en œuvre de mesures de prévention en cas de perte de données: 39 %
- Gestion des failles et des correctifs améliorée: 31 %
- Mise en réseau de systèmes externes réduite: 26 %
- Restructuration de la cyberassurance existante ou augmentation de la couverture: 14 %

RÉAGIR ET RÉTABLIR
- Introduction et amélioration de la sensibilisation à l'ingénierie sociale pour les collaborateurs: 69 %
- Elaboration d'un plan de réponse aux cyberincidents: 29 %
- Améliorations concrètes dans l'identification de risques de cyberévénements: 25 %
- Organisation de services d'assistance externes (droit, RP, IT-Security): 12 %

Quel que soit le ressenti subjectif des sondés, il a dans tous les cas des répercussions sur la gestion des cyberrisques, essentiellement sur la mise en œuvre ou non de mesures de prévention.

Il est frappant de constater que près de 40 % des participants au sondage déclarent avoir conclu une cyberassurance (graphiques 6 et 12). Au vu du marché relativement récent de la cyberassurance et des volumes de primes actuels en Suisse, nous estimons que le pourcentage de polices de cyberassurance placées est nettement plus faible. Nous considérons plutôt que ces 40% de sondés n'ont soit pas conclu de cyberassurance, mais pensent à tort que les risques sont couverts dans les polices existantes, soit ont estimé que certaines composantes de couverture ayant trait aux cyberrisques offraient une protection suffisante. De nombreuses entreprises sont dans une illusion de sécurité et ont tendance à négliger les mesures de réaction et de rétablissement (graphique 6).

En outre, les résultats obtenus dans le domaine des mesures de réaction amènent à penser que 69 % des entreprises ont pris des mesures préventives d'ingénierie sociale. Etant donné que la plupart des cyberrisques sont déclenchés par le facteur humain, ce résultat serait très réjouissant.

Mais si l'on se réfère à nos discussions quotidiennes avec les clients, cette information doit toutefois être prise avec circonspection. Ainsi par exemple, des cours d'introduction ponctuels à l'informatique ou l'information occasionnelle des collaborateurs au sujet de tentatives actuelles de phishing sont fréquemment considérés comme des formations de sensibilisation à l'ingénierie sociale. Malgré les chiffres, nous constatons que les entreprises font beaucoup plus d'efforts pour aborder de manière proactive le facteur humain comme le maillon le plus faible de la chaîne de cybersécurité. Les qualités humaines, la serviabilité, la crédulité et la curiosité constituent les plus grands points faibles des collaborateurs, et par conséquent les plus grands risques. C'est pourquoi il est indispensable de réaliser chaque année une formation récurrente, car les formations ponctuelles ne donnent généralement pas de résultat à long terme.

3

L'investissement dans un plan de réaction d'urgence fait aujourd'hui partie des mesures de prévention absolument essentielles et qui offrent le plus d'avantages à long terme. Au moins 61 % des sondés déclarent cependant ne pas avoir élaboré de plan de réaction d'urgence au cours des 12 à 24 derniers mois (graphique 7). Et ce, bien que la plupart de ceux ayant évalué le scénario le plus pessimiste estiment à plus d'un million de dollars le montant moyen des dommages suite à un cyberincident (graphique 5). L'absence de plan de crise s'explique en grande partie par l'existence d'un propre système de cybersécurité/pare-feu ainsi que par le manque de savoir-faire (graphique 8).

Les mesures techniques IT sont encore souvent surévaluées en matière de cybersécurité: à l'ère de la mise en réseau numérique croissante et de dépendances vis-à-vis de tiers, ni une cybersécurité/sécurité IT/un pare-feu conçus selon les règles de l'art ni le manque de savoir-faire ne justifient l'absence de plan de réaction d'urgence.

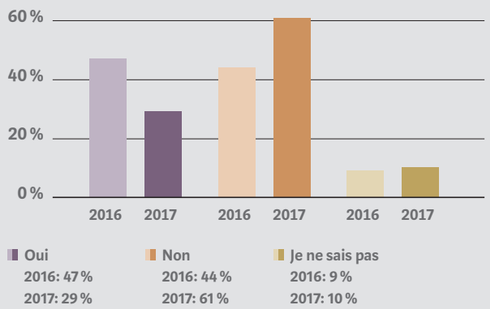
Peu de personnes sont conscientes du fait que les cyberrisques occasionnent autant de préjudices économiques que les catastrophes naturelles. Ainsi par exemple, la neutralisation d'un fournisseur de services cloud peut occasionner un préjudice économique total de 50 à 120 milliards de dollars, ce qui correspond à l'ampleur du sinistre occasionné par les ouragans Sandy ou Katrina (rapport WEF 2018). La dépendance vis-à-vis de données intègres et de systèmes disponibles est élevée, tout comme les dommages, et malgré tout, on investit peu dans les mesures préventives. L'attaque NotPetya dont a été victime l'armateur Maersk en juin 2017 a fait office de signal d'alarme qui a coûté cher: la perte d'exploitation de dix jours a en effet entraîné une perte de chiffre d'affaires de 20 %, ce qui correspond à un montant des dommages d'au moins 250 millions de dollars. Avec un plan de reprise après sinistre (Recovery Plan) élaboré au préalable, les coûts auraient été sensiblement moins élevés.

> CELUI QUI S'ATTEND A UNE ATTAQUE ET QUI Y EST PRÉPARÉ POSSÈDE LES MEILLEURS ATOUTS.

Les mesures contre les cyberrisques ne doivent pas entraver l'exploitation, mais assurer une protection particulière des points sensibles dans l'entreprise. Celui qui est formé à la gestion des tempêtes a les meilleures chances de les maîtriser intelligemment et avec tout le calme requis.

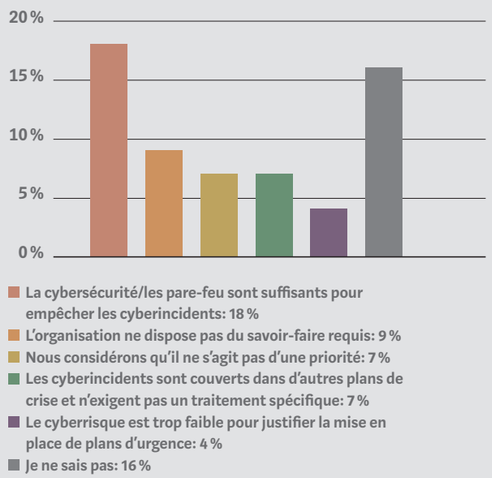
GRAPHIQUE 7

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



GRAPHIQUE 8

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



3

A l'instar de l'année précédente, la plupart des entreprises suisses redoutent une perte d'exploitation. Le dommage de réputation constitue la seconde menace la plus importante, suivie par les dommages aux données/logiciels ainsi que la perte de données clients. Viennent ensuite les extorsions/ransomwares, l'arrêt d'installations industrielles ou d'autres équipements d'exploitation, la responsabilité vis-à-vis de tiers suite à une intrusion dans un système, la perte/le vol de propriété intellectuelle, la perte d'exploitation chez des fournisseurs importants ainsi que les dommages matériels et corporels (graphique 9).

La perte d'exploitation consécutive à une cyberattaque constitue à juste titre la menace la plus redoutée dans toute l'Europe (graphique 9); le montant des dommages et les divers scénarios sont totalement imprévisibles et dépendent entre autres de la façon dont les systèmes IT sont implantés (implantation centralisée ou décentralisée), du nombre de prestataires informatiques impliqués et de la façon dont ils le sont, du concept de sauvegarde appliqué, etc. Le for judiciaire et le droit applicable peuvent également avoir une grande incidence sur les coûts des dommages propres ou des dommages causés à des tiers.

En matière de réputation, l'obligation de déclarer jouera un rôle intéressant dans le cadre du RGPD. Au vu du montant «abordable» des amendes infligées en matière de protection des données en Suisse et en Europe, les entreprises victime d'un piratage informatique des données clients préféraient se taire et s'acquitter d'une amende afin de préserver leur réputation. Il reste à voir comment les amendes élevées prévues dans le RGPD seront conçues dans la pratique juridique. Une chose est claire: la décision coût-utilité «Pouvons-nous/voulons-nous nous permettre une amende ou un dommage de réputation?» exigera de la part des entreprises de nouvelles stratégies en matière de transparence et de coûts.

S'agissant de l'ampleur du sinistre, la perte de données clients devrait, dans l'optique du RGPD et d'autres lois européennes sur la protection des données ou de lois en relation avec la loi sur la protection des données, devenir une deuxième grande inconnue. Et ce, non seulement en raison de la perte de données clients et, le cas échéant, des obligations de notification aux personnes ou entreprises touchées ou aux autorités, mais surtout en raison d'autres menaces d'amendes élevées (jusqu'à 4 % du chiffre d'affaires annuel mondial consolidé ou 20 millions d'euros; art. 83 RGPD) en cas de violation du RGPD. En outre, une procédure d'examen de la protection des données, initiée par une autorité européenne, peut générer d'autres coûts dans le domaine des dommages propres, qui à l'heure actuelle sont difficiles à quantifier.

GRAPHIQUE 9

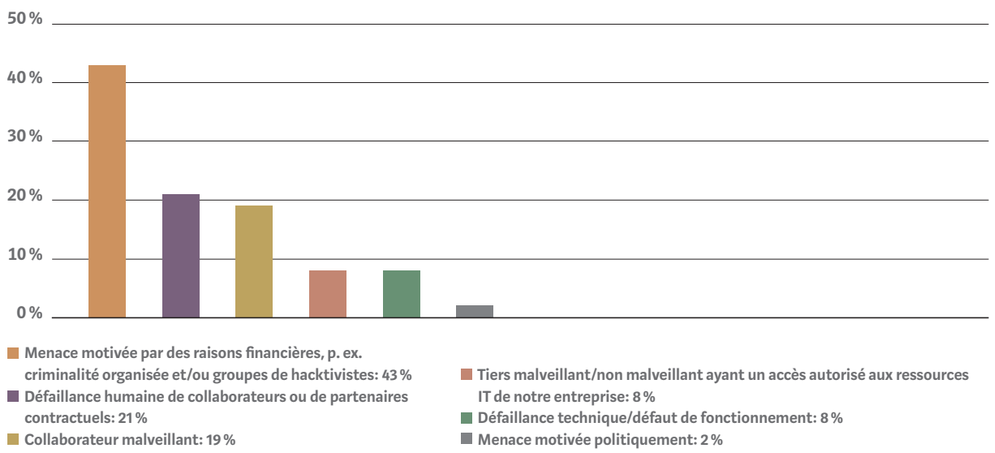
Quels scénarios de cyberattaque constituent la plus grande menace pour votre entreprise?

	Italie	France	Espagne	Portugal	Allemagne	Suisse	Roumanie	Belgique	Benelux
Perte d'exploitation	69 %	83 %	84 %	81 %	75 %	86 %	82 %	60 %	63 %
Dommages aux données/logiciels	71 %	83 %	53 %	54 %	17 %	53 %	59 %	47 %	52 %
Dommages de réputation	46 %	42 %	53 %	51 %	25 %	57 %	41 %	60 %	63 %
Perte de données clients	40 %	42 %	32 %	49 %	33 %	52 %	47 %	47 %	52 %
Responsabilité vis-à-vis de tiers suite à une intrusion dans un système	34 %	42 %	37 %	27 %	17 %	30 %	29 %	13 %	24 %
Interruption d'installations industrielles ou d'autres équipements d'exploitation	34 %	33 %	32 %	41 %	33 %	33 %	29 %	27 %	33 %
Extorsion/ransomware	31 %	33 %	42 %	51 %	25 %	37 %	29 %	43 %	41 %
Perte/vol de propriété intellectuelle	26 %	17 %	21 %	24 %	50 %	22 %	47 %	37 %	33 %
Perte d'exploitation chez des fournisseurs importants	20 %	33 %	32 %	35 %	25 %	17 %	29 %	30 %	30 %
Dommages matériels/corporels	6 %	25 %	16 %	5 %	8 %	11 %	12 %	13 %	9 %
Autre	34 %	33 %	32 %	41 %	33 %	34 %	29 %	27 %	33 %
Je ne sais pas	3 %	0 %	5 %	0 %	0 %	2 %	0 %	0 %	0 %

3

GRAPHIQUE 10

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



Un malware est un logiciel malveillant développé dans le but de provoquer un dommage à l'utilisateur d'un ordinateur. Les outils de piratage, aujourd'hui moins coûteux, ainsi que la tendance croissante au partage de connaissances («Let's Share Knowledge») favorisent la propagation de malware par des non-spécialistes de l'informatique. Les vagues de cyberattaques de juin 2017, occasionnées par les cryptovirus WannaCry, Petya et NotPetya, révèlent non seulement les dangers provenant de cybercriminels, mais soulignent une fois de plus la monoculture informatique qui règne en Europe et qui favorise la cybercriminalité. La tendance des entreprises à utiliser des logiciels, des programmes de sécurité ainsi qu'une infrastructure IT similaires ouvre, en cas de cyberattaques fructueuses, la porte à d'autres organisations (Sigma Report 1/2017, SwissRe).

Lors de nos entretiens avec les clients, le débat au sujet des auteurs de menaces les plus redoutés dans le cadre d'une infection par un malware (graphique 10) donne fréquemment lieu à des discussions à forte charge émotionnelle. Quelle en est la raison? L'accès illicite à des systèmes de l'entreprise s'effectue fréquemment par l'intermédiaire des collaborateurs. Ils constituent le maillon le plus faible de la chaîne de cybersécurité. En raison de son corps émotionnel, l'être humain est difficilement prévisible (voir également le commentaire du graphique 6). Des collaborateurs de longue date, jeunes ou moins jeunes, des collaborateurs bien ou mal établis peuvent, sans signes avant-coureurs, développer une énergie criminelle contre leur employeur, ou des collaborateurs bien formés peuvent se faire piéger par un e-mail de phishing adapté à leurs besoins. Cette problématique est bien connue. Cependant, nos clients ont souvent du mal à intégrer dans l'analyse des cyberrisques résiduels leurs collaborateurs comme la cause la plus fréquente, active ou passive, d'un cyberrisque. Nous sommes d'avis qu'une étape importante pourrait être franchie si le risque résiduel lié à des collaborateurs potentiellement criminels ou faciles à manipuler était intégré de façon objective, sans connotation émotionnelle, dans l'analyse des cyberrisques. Nous estimons à 50 % au moins le cyberrisque résiduel émanant de l'être humain.

3

3.4 ÉVALUATION DES RISQUES ÉMANANT DES SOUS-TRAITANTS IT

Pour se concentrer sur leurs compétences-clés, de plus en plus d'entreprises externalisent leur technologie de l'information et leurs systèmes d'information. A côté des avantages évidents offerts par l'outsourcing, celui-ci implique toujours des risques. Les données et les processus d'affaires précieux doivent être en de bonnes mains, c'est pourquoi le fournisseur IT doit être choisi avec soin. L'outsourcing est une question de confiance.

L'outsourcing informatique signifie que des tâches internes de l'entreprise sont déléguées sur la base d'une relation contractuelle, par exemple applications, infrastructure, processus, personnel ou tâches de maintenance informatique. Les gains d'efficience et d'efficacité ainsi que les faibles coûts sont autant d'avantages offerts par l'outsourcing. Les inconvénients tels que la 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 ont généralement un poids plus important, mais sont curieusement acceptés assez facilement dans de nombreux cas (les établissements financiers, qui ont moins de possibilités de choix en raison de prescriptions plus strictes de la BaFin ou de la FINMA, constituent une exception).

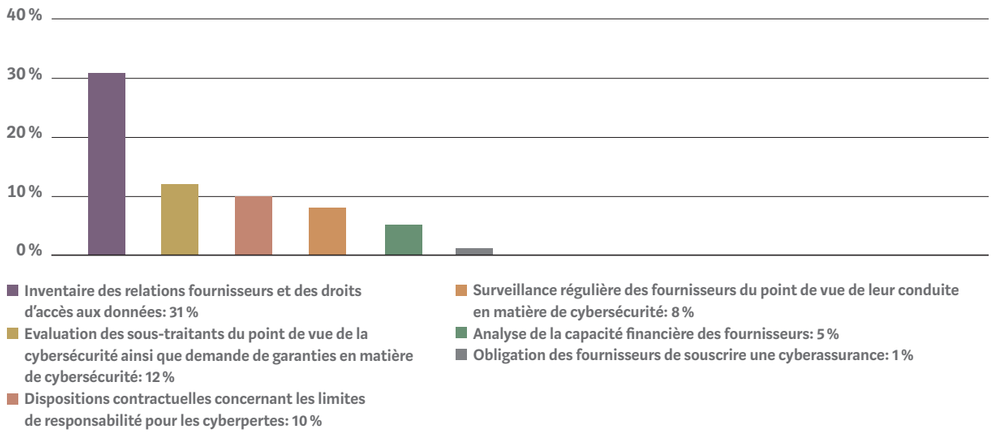
L'attaque ciblée d'une chaîne de logistique IT est lucrative. Par le biais du fournisseur IT contre lequel l'attaque est dirigée, on essaie par exemple d'obtenir simultanément le contrôle de diverses organisations, ce qui peut provoquer des dommages considérables. Les risques de responsabilité sont généralement répercutés sur le client dans le cadre de ce qui est légalement possible. Il faut dès lors faire comprendre à ce dernier que même des entreprises de télécommunications leader du secteur et qui proposent un niveau de service optimal n'offrent qu'une sécurité IT/cybersécurité limitée et ne sont pas en mesure de protéger une entreprise contre une perte de liquidités voire une faillite. Plus la dépendance vis-à-vis de prestataires externes est grande, plus leur défaillance devrait être intégrée dans la gestion des cyberrisques opérationnels. Le graphique 11 fournit des chiffres intéressants à ce sujet.

33 % ÉVALUENT LEURS SOUS-TRAITANTS DU POINT DE VUE DES MENACES LIÉES AUX CYBERRISQUES. 46 % Y RENONCENT. 21 % NE SAVENT PAS.

A présent, 33 % des entreprises évaluent leurs sous-traitants du point de vue des menaces liées aux cyberrisques, alors qu'en 2016, elles n'étaient que 20 %. Ce résultat montre une progression importante. Le graphique 11 fait toutefois apparaître que l'évaluation qualitative des entreprises concernant leurs fournisseurs IT présente un potentiel d'amélioration. Ainsi, l'évaluation des sous-traitants du point de vue de leur cybersécurité, la demande de garanties pour une cybersécurité et une cybersurveillance durables, les accords contractuels portant sur les limites de responsabilité pour des pertes consécutives à des cyberattaques, l'analyse de la capacité financière des fournisseurs ainsi que l'obligation des fournisseurs de conclure eux-mêmes une cyberassurance figurent encore parmi les rares mesures prises.

GRAPHIQUE 11

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



3

3.5 LES CONCLUSIONS DE CYBERASSURANCES CONTINUENT DE PROGRESSER

Le marché de la cyberassurance évolue en permanence suite à de nouveaux cyberrisques, alors les entreprises sont elles-aussi en mutation permanente. Mieux les entreprises identifient leurs failles et leurs besoins dans le domaine de la cybersécurité, plus la décision relative à la stratégie de financement sera facile à prendre: une cyberassurance ne remplacera jamais des mesures de prévention, mais doit empêcher, en cas de sinistre, la mise en péril du bilan et du compte de résultat ainsi que la perte de liquidités.

Depuis la vague de cyberattaques qui a eu lieu à la mi-2017, les grandes entreprises et, de plus en plus de PME, manifestent un intérêt croissant pour les polices de cyberassurance. Chez nos clients suisses, les cyberassurances sont toujours axées sur la couverture des pertes d'exploitation consécutives à un cyberévénement. A l'heure actuelle, c'est-à-dire avant que le RGPD n'ait un effet direct à partir du 25 mai 2018, il est difficile, du fait de l'absence de jurisprudence européenne et en raison des questions ayant trait à l'exécution des peines d'amende qui ne sont pas totalement clarifiées, d'évaluer si le RGPD, suite à la hausse des risques de coûts assurables dans les domaines des amendes pour violation de la protection des données, des coûts de notification ainsi que des coûts des procédures réglementaires, aura une influence perceptible sur l'augmentation du nombre de cyberassurances conclues en Suisse.

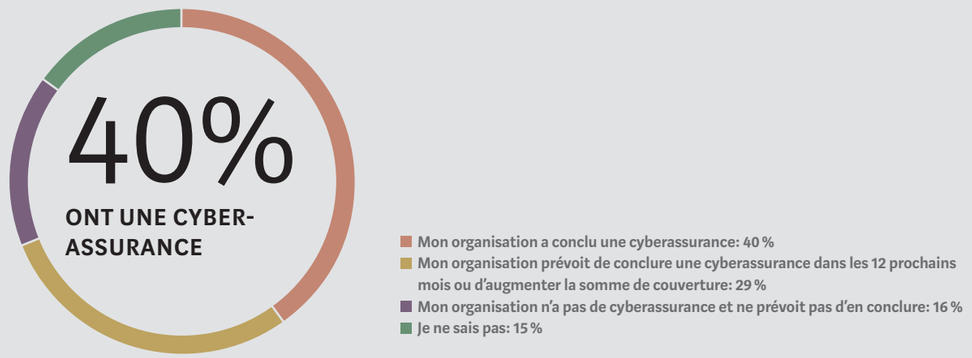
Selon le présent sondage, 40 % de nos clients ont conclu une cyberassurance, alors que 29 % envisagent de souscrire une assurance correspondante ou d'augmenter la somme de couverture dans les 12 prochains mois (graphique 12).

LE TRAITEMENT DU RISQUE D'AMENDE EST INSCRIT À L'ORDRE DU JOUR DE LA DIRECTION AU MÊME TITRE QUE LA DÉCISION ÉCLAIRÉE CONCERNANT LA STRATÉGIE DE FINANCEMENT DU RISQUE.

Au vu des contrats de placement de cyberassurances qui nous sans confiés en tant que courtier et compte tenu de la situation actuelle du marché pour les cyberassurances indépendantes, le taux de conclusion élevé de 40 % a de quoi nous surprendre. Nous supposons que la notion de cyberassurance est interprétée différemment et que certains sondés considèrent par exemple qu'il s'agit d'une cybercouverture tacite dans le cadre d'un produit standard ou que des composantes de couverture individuelles dans des produits d'assurance traditionnels sont interprétées comme une cybercouverture.

GRAPHIQUE 12

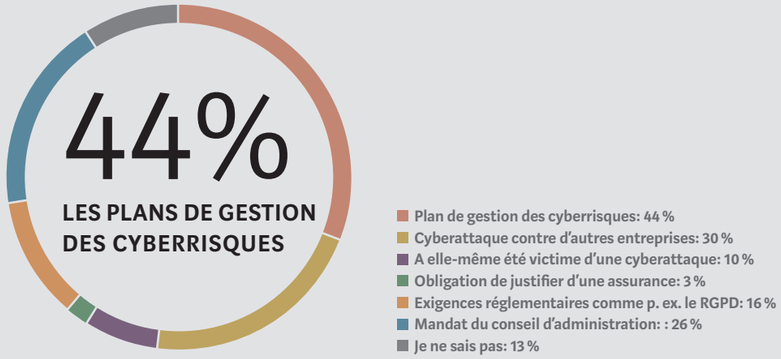
Quel est le positionnement actuel de votre entreprise en matière de cybercouverture?



3

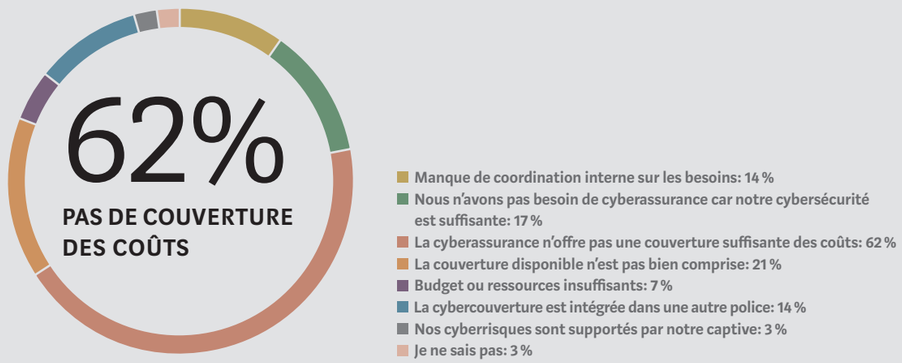
GRAPHIQUE 13

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



GRAPHIQUE 14

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



Le fait que sur plus de 40 % des sondés qui ont déjà conclu une cyberassurance ou qui envisagent d'augmenter leur somme de couverture, près de la moitié indiquent que c'est le plan actuel de gestion des cyberrisques qui les a poussés à agir, est compréhensible (graphique 13). Car si l'on se penche de façon plus intensive sur les cyberrisques et leurs conséquences potentielles, on s'aperçoit assez rapidement qu'une perte d'exploitation de plusieurs heures peut entraîner des pertes financières considérables.

Tant que les scénarios potentiels les plus pessimistes en matière de cyberrisques ne seront pas quantifiés, les cyberattaques resteront une grande inconnue pour la direction de l'entreprise. Lorsqu'il s'agit d'empêcher que la responsabilité des organes de direction ne soit engagée – par exemple en raison de l'insuffisance des mesures de sécurité IT ou de la surveillance, l'espoir est mauvais conseiller. Il n'est donc guère étonnant que pour la stratégie de financement des cyberrisques, les conseils d'administration imposent de plus en plus fréquemment, dans leur propre intérêt, une stratégie descendante (top-down) (voir également le graphique 13).

31 % des entreprises suisses n'ont pas de cyberassurance, n'ont pas l'intention d'en souscrire ou ne disposent pas d'un plan correspondant (graphique 12). Le principal motif invoqué est la couverture insuffisante des coûts (62 %) (graphique 14).

Compte tenu des résultats du graphique 14, nous estimons qu'il existe un besoin de conseil dans ce domaine. Pour les non-spécialistes, il est en effet difficile de différencier les différentes composantes de couverture des assureurs ainsi que les critères demandés dans les évaluations de risque divergentes. Chaque assureur parle sa propre langue. C'est pourquoi il est déconseillé de conclure une police standard sans faire appel à un cyberspécialiste et sans procéder à une étude de marché approfondie. Les besoins de chaque client doivent être déterminés. Chaque cyberpolice est dès lors unique. Le scénario le plus pessimiste ne devrait pas être exclu de la couverture.

4
LE RGPD, UNE OPPORTUNITÉ POUR RENFORCER LA GESTION DES CYBERRISQUES

4.1 CAUSES ET EFFETS DE LA CONFORMITÉ AVEC LE RGPD

Considéré par de nombreuses entreprises suisses comme coûteux en temps et en argent, et donc comme un obstacle à la marche des affaires, le RGPD a au moins un effet positif: les entreprises sont quasiment obligées de se pencher sur les cyberrisques et d'optimiser leur gestion.

Les coûts des violations de la loi sur la protection des données sont calculables et en grande partie (encore) assurables. La décision éclairée relative à un degré de mise en œuvre judicieux du RGPD doit, à notre avis, être inscrite à l'ordre du jour de la direction au même titre que celle concernant la stratégie de financement des risques majeurs. Parmi les entreprises interrogées qui sont soumises au RGPD, seules 6 % ont indiqué à la mi-2017 être en totale conformité avec ce dernier, tandis que 51 % prévoient de respecter le RGPD en fonction de leur exposition au sein de l'UE. Le fait est que 43 % des entreprises suisses n'ont soit pas encore de plan pour l'intégration du RGPD dans l'entreprise, soit ne savent pas où elles en sont dans la mise en œuvre du RGPD (graphique 15).

Compte tenu des efforts nécessaires pour respecter à peu près les dispositions du RGPD, il est probable qu'au cours des dernières semaines précédant l'entrée en vigueur du RGPD (d'ici le 25 mai 2018) ou au plus tard à partir du moment où les premiers jugements infligeant le paiement d'une amende deviendront exécutoires, on assistera à une grande vague de mise en œuvre supplémentaire de la part des entreprises pour se mettre en conformité avec le RGPD. Il est clair que les menaces de sanctions prévues à l'article 83 du RGPD peuvent faire peser des risques de responsabilités considérables sur les entreprises suisses.

On ne peut toutefois pas nier l'effet positif du RGPD: les entreprises seront quasiment obligées d'améliorer leur capacité à maîtriser les risques et à réagir face aux risques survenant dans le paysage des cyberrisques, en constante évolution, afin d'assurer également une meilleure protection des données personnelles. Ainsi par exemple, le RGPD comporte l'obligation de traiter les données personnelles de manière à garantir une sécurité appropriée, y compris d'empêcher l'accès ou l'utilisation non autorisé des données à caractère personnel et des appareils utilisés pour le traitement. L'entreprise responsable du traitement ou le sous-traitant (p. ex. le fournisseur IT) devrait par conséquent évaluer les risques liés aux données à caractère personnel et prendre des mesures destinées à réduire ces risques (article 32 du RGPD). En cas de violation de diverses prescriptions, le RGPD définit en outre des règles claires sur les conditions d'application de sanctions administratives. A l'avenir, de lourdes amendes pourront être infligées aux entreprises si elles n'ont pas informé leurs clients par exemple au sujet de la compromission de données à caractère personnel, ou si la notification n'a eu lieu qu'après une pression extérieure.

Chacun sait qu'un plan de réaction d'urgence pour un risque défini fait partie des mesures les plus efficaces de réduction des coûts (on peut prendre comme comparaison les exercices pratiqués généralement par les sapeurs-pompiers avec l'ensemble du personnel). Il est dès lors surprenant que seulement 23 % des sondés aient élaboré un plan de réaction en perspective de violations des données à caractère personnel (graphique 16).

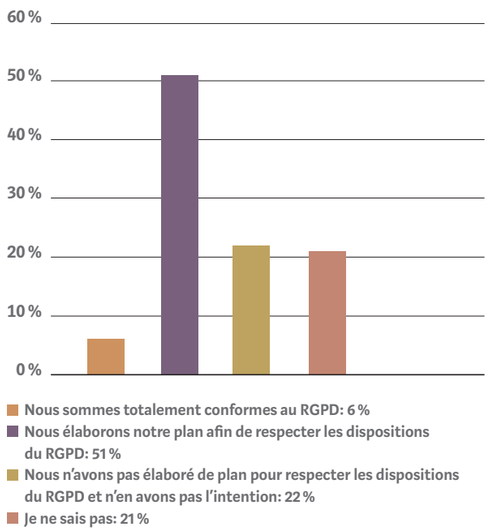
Le RGPD n'impose pas de plan de réaction d'urgence en cas de cyberincidents, mais demande que les autorités de surveillance soient informées dans les 72 heures suivant la constatation d'un incident ayant trait à la sécurité des données.

Il est évident que cette notification dans les délais réussit plutôt avec un plan de mesures d'urgence que sans. Si les coûts liés à ces cyberincidents doivent être limités dès le départ, la décision coût-utilité (charges financières/charge de travail interne versus réduction de l'ampleur du dommage en cas d'urgence) doit être prise avant le premier cyberincident.

Mais en dépit de toute raison, rien n'empêche la direction de l'entreprise d'adopter une ligne de conduite à risque et donc d'omettre volontairement d'éventuelles dispositions en matière de sécurité IT. Il est important que le traitement du risque d'amende en vertu du RGPD soit inscrit à l'ordre du jour de la direction de l'entreprise au même titre que la décision éclairée au sujet de la stratégie de financement des risques majeurs. En raison du montant jusqu'ici abordable des amendes liées à la protection des données, on peut considérer que pour préserver leur réputation, les entreprises suisses préféraient jusqu'ici s'acquitter d'une amende pour garder secret un piratage des bases de données clients plutôt que de le révéler aux victimes ou aux autorités. Avec l'introduction du RGPD et, le cas échéant, suite à la 2e révision de la loi fédérale sur la protection des données, cette pratique est amenée à changer.

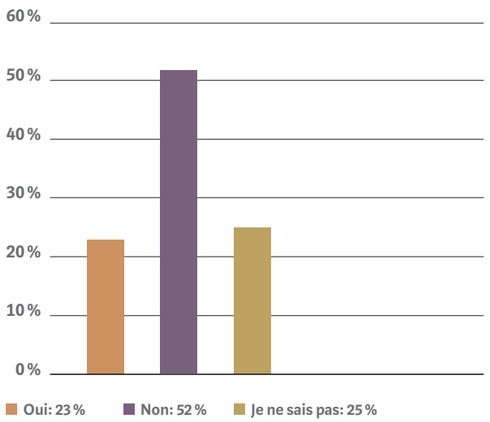
GRAPHIQUE 15

Quels progrès votre organisation a-t-elle réalisés dans sa volonté de mise en conformité avec le 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

L'évolution des modèles d'affaires numériques donne lieu à un trafic de données difficilement évaluable, à un volume de données numériques considérable et par conséquent à une hausse des cyberrisques. De nombreuses entreprises ne disposent pas du savoir-faire pratique nécessaire pour faire face à ces défis et les maîtriser de manière judicieuse.

Les cyberrisques sont complexes et susceptibles d'entraîner des dommages cumulés considérables. Dès lors, les propres cyberrisques tout comme ceux des fournisseurs IT, des fournisseurs de matières premières ou de sous-composants devraient également être pris en considération dans la gestion des risques opérationnels. Le travail initial nécessaire pour un traitement judicieux des cyberrisques exige beaucoup de temps, génère des coûts et est incontestablement fastidieux, si l'on tient compte des autres risques d'entreprise qui doivent également être pris au sérieux.

Au vu des progrès de la numérisation, il est évident que nous ne pourrons pas éliminer les cyberrisques. Il est d'autant plus important de mettre en place une gestion ciblée des cyberrisques, qui n'entrave pas l'activité, mais qui renforce la cyberrésistance des entreprises et celle de l'économie suisse.

En outre, il est clair que le traitement opérationnel des cyberrisques est individuel et largement tributaire de la propension au risque de la direction.

Enfin, celui qui considère le RGPD comme une opportunité de repenser la gestion du cyberrisque opérationnel se penchera de façon plus constructive sur la thématique de la protection des données et ne la considérera pas seulement comme une obligation fastidieuse.

BESOIN DE CONSEIL

Le traitement des cyberrisques résiduels est une tâche exigeante. Nous estimons qu'il existe également un besoin de conseil pour l'attribution de la responsabilité en matière de cyberrisques au sein de l'entreprise, pour l'identification et l'analyse des cyberrisques dans l'entreprise et, de façon accrue, pour la mise en œuvre de mesures de prévention diversifiées et appropriées. Outre les mesures de prévention diversifiées, la gestion des cyberrisques comporte également d'autres stratégies de financement du risque adaptées à la capacité financière et à la politique en matière d'assurance du risque.

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

Helmut Studer
Membre du Comité de direction
helmut.studer@kessler.ch
T +41 44 387 87 17

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