Date : 07/04/2020
Heure : 14:51:54
Journaliste : Lucy Letellier/ Ondine Delaunay/ Aurélia

www.lja.fr
Pays : France
Dynamisme : 3

Visualiser l'article

Cyberattaque#: anticipation, gestion de crise et leçons

En 2019, 39#% des grandes entreprises européennes admettent avoir été victimes d'une cyberattaque. En France, des grands noms sont sortis dans la presse comme Edenred, Ramsay Générale de Santé, Eurofins Scientific ou encore Bouygues Construction.

Les conséquences pour l'entreprise sont importantes puisque 60#% des PME déposeraient le bilan dans les six mois d'une cyberattaque. L'exemple de Lise Charmel est le plus récent, l'entreprise ayant récemment annoncé son placement en redressement judiciaire.

L'impact sur le cours de Bourse des sociétés cotées serait également non négligeable dans près de deux tiers des cas. Et pourtant, une grande entreprise sur cinq n'aurait pas de politique stratégique en matière de cybersécurité.

Alors même que le risque cyber n'est aujourd'hui plus une hypothèse mais bien une réalité, comment les entreprises s'organisent-elles pour anticiper et gérer les attaques ? Analyse des experts du secteur.

Avec : **Etienne Drouard** , avocat associé, cabinet **Hogan Lovells** , **Nicolas Arpagian** , VP Stratégie et affaires publiques d' **Orange Cyberdefense** , Administrateur de www.cybermalveillance.gouv.fr, **Olivier Lopez** , directeur de l'Institut de statistique de l'université de Paris, Colonel **Éric Freyssinet** , chef du pôle national de lutte contre les cybermenaces, Direction générale de la **Gendarmerie nationale** , **Philippe Cotelle** , head of insurance and risk management, **Airbus Defence & Space** , administrateur de l' **AMRAE** et président de sa commission SI, co-pilote pour l' **AMRAE** du guide publié avec l' **ANSSI** « la maîtrise du risqué numérique, l'atout confiance », **Eric Barbry** , avocat associé, cabinet **Racine** et **Stanislas de Maupeou** , vice-président stratégie et marketing, systèmes d'information critiques et cybersécurité de **Thales** .

État actuel du marché

Philippe Cotelle#: Les statistiques sur les cyberattaques, sur leurs conséquences et plus largement sur le cyberrisque ne sont, à mon sens, pas tellement révélatrices de l'état actuel du marché de la cybersécurité. Notamment concernant l'impact sur les cours de bourses. Je ne suis pas certain qu'il existe aujourd'hui une étude crédible permettant d'émettre ce genre de données.

Nicolas Arpagian#: En effet, les principales études menées ne portent pas sur des volumes suffisamment significatifs d'attaques pour en tirer des principes intangibles. Tout dépendra en outre de la qualité de la réaction de la société ciblée au regard d'une multitude de critères#: la réactivité et la pertinence de sa communication, sa transparence sur les processus, sa conformité aux obligations légales ou contractuelles, sa capacité à revenir à une situation normale… Bien sûr, il en va autrement quand l'objectif de la cyberattaque est précisément de viser le cours de Bourse, comme ce fut le cas dans l'opération ayant ciblé la société Vinci. Il s'agissait alors d'une opération à des fins de spéculation sur la variation du titre.

Philippe Cotelle#: Dans tous les cas, le cyberrisque est stratégique pour la société qui doit être vigilante. C'est un risque d'entreprise, pas un risque technique. À l'heure actuelle, il n'existe aucun chiffre, aucun référentiel qui soit absolument inattaquable. Et c'est d'ailleurs un frein car nous avons besoin de statistiques objectives

permettant de chiffrer la perte de richesses en France à cause du cyberrisque. Notre seul référentiel, c'est quand l'entreprise est attaquée, s'organise et prend les mesures pour s'en prémunir. Appréhender et traiter le risque cyber, c'est aujourd'hui créer de la valeur, créer les bases de la confiance numérique, un nouvel actif immatériel. Ne parler que de coût est stupide.

Stanislas de Maupeou#: Dans les entreprises industrielles de défense, le risque cyber est pris en compte depuis des années. Mais il ne nous a pas empêchés d'être attaqués. Nous ne découvrons pas le sujet comme tel peut être le cas dans d'autres secteurs. La maturité dépend beaucoup du donneur d'ordre, selon que la régulation soit présente ou non dans le secteur, et que ce dernier ait déjà subi des attaques ou pas. Mais il est vrai de dire que la cybersécurité est encore trop souvent vue comme un facteur de coûts plutôt que comme une véritable proposition de valeur et de gestion des risques.

> Stanislas de Maupeou, Vice-président stratégie et marketing, systèmes d'information critiques et cybersécurité de **Thales**

Nicolas Arpagian#: Dans tous les domaines liés à l'insécurité, que ce soient les atteintes aux biens ou aux personnes, les chiffres de la délinquance et de la criminalité sont fournis par le ministère de l'Intérieur via

l'Observatoire national de la délinquance et de la réponse pénale (ONDRP). Or, à ce jour, l'État ne dispose pas de statistiques nationales consistantes en matière cyber. Les seules données qui circulent émanent essentiellement de fournisseurs de solutions de sécurité. Ce qui n'est pas satisfaisant#: on ne demande pas à un vendeur de portes blindées d'émettre les statistiques officielles sur les cambriolages. C'est un vrai chantier pour les autorités publiques, qui pourront s'appuyer aussi sur les données collectées par le GIP ACYMA qui gère la plateforme www.cybermalveillance.gouv.fr . La mesure de la cybersécurité est d'autant plus difficile à obtenir qu'il s'agit d'un univers où vous pouvez être victime alors que vous l'ignorez. Et il ne faut pas non plus négliger la part d'entreprises qui se sont fait attaquer et ne souhaitent pas communiquer à ce propos. Donc forcément, la mesure de l'état de cyber-insécurité est donc imparfaite. Au regard de l'intensification de notre activité numérique, dans nos vies personnelles et professionnelles, on ne peut que constater un accroissement constant de notre exposition au risque cyber. De plus, l'accessibilité financière et technique de nombre de solutions de piratage en quelques clics sur le Net témoigne de l'importance de la demande dans le grand public. Ce qui désigne une forte croissance des opérations de cyberattaque.

Éric Freyssinet#: Une étude est publiée tous les deux ans par le Club de la sécurité de l'information français (Clusif) sur le thème de la cybersécurité. Elle repose sur un sondage réalisé auprès de plusieurs centaines d'entreprises. Je suis toujours surpris, en analysant ses résultats, de constater que sur les 7, 8 ou 9#%

d'entreprises victimes, on n'en voit, de notre côté, que trop peu qui ont déposé plainte pour ces faits. Il a toujours existé une importante différence entre la perception du risque par les entreprises, ce qu'est un cyberrisque, et ce que l'on peut constater dans les chiffres officiels lors de leur publication. Depuis quelques années, nous percevons une augmentation assez forte de la sollicitation des victimes. Par exemple, l'année dernière, une augmentation globale de 22#% (particuliers et entreprises) des faits de cybercriminalité nous a été rapportée ou a été détectée par nos soins. Cela veut dire que nous avons un meilleur contact avec les victimes. Cette prise de conscience est en définitive liée à une grande visibilité des cyberattaques et à l'évolution des pratiques des délinquants.

Stanislas de Maupeou#: Il existe une véritable culture de la sécurité numérique en France, qui est par exemple l'un des rares pays à avoir une cryptographie souveraine reconnue. Les moyens publics ont augmenté. La France est parmi les pays du monde qui ont le plus pris en compte ce sujet et pas simplement au gré des différentes attaques.

Nicolas Arpagian#: La France s'est dotée depuis une décennie d'une Agence nationale de Sécurité dédiée aux Systèmes d'Information (ANSSI) et d'un corpus juridique robuste pour hausser le niveau de cybersécurité des entreprises stratégiques pour la continuité d'activité du pays. Avec son homologue allemand, le BSI, elle assure le leadership en Europe sur les questions de sécurité numérique.

Etienne Drouard#: La définition américaine de la sécurité nationale inclut une dimension de conquête et de sécurité économique depuis 1974, rendant très étroits les rapports du gouvernement fédéral avec les entreprises les plus importantes pour la croissance et le PIB.
En Europe, la régulation a eu un certain effet bénéfique sur la prise en compte du risque cyber. Sans l'exigence réglementaire d'une obligation de notification, le sujet serait encore ignoré par un grand nombre de comités exécutifs. On peut regretter que les chiffres ne génèrent pas une attention plus forte et qu'une équation de la rentabilité de la prévention n'ait pas encore été trouvée par les PME et les ETI. Ce qui est certain, c'est que la culture de la sécurité numérique#-#et le rapport au secret#-#me parait historiquement plus forte en Europe qu'aux États-Unis, mais que la culture de la prévention et de la conformité réglementaire y est bien plus faible en Europe. Rappelons que le phénomène des notifications de failles provient des États-Unis, où sa vocation était exonératoire de responsabilité, sous l'influence de l'adage «#faute avouée à moitié pardonnée#». Si l'Europe avait suivi l'approche américaine sur ce point, les notifications de failles de sécurité auraient eu lieu beaucoup plus tôt. Historiquement, l'importation en Europe des mécanismes de notification s'est faite en deux vagues successives, répliquées en France avec, d'une part, la définition des Opérateurs d'Infrastructure Vitale (OIV) à partir de 2013 puis, à partir de 2018, avec la notification de certaines violations de données personnelles, inscrite dans le RGPD.

Nicolas Arpagian#: La loi de programmation militaire 2014-2019 (LPM) a qualifié près de trois cents entreprises comme étant stratégiques, ce sont les opérateurs d'importance vitale (OIV). Elles sont présentes dans 12 secteurs d'activité (banques, télécoms, énergie, alimentation, traitement de l'eau,#etc.) et doivent disposer d'une politique de cybersécurité particulièrement exigeante contrôlée par l'ANSSI. À l'échelon européen, la directive NIS a instauré, à partir de 2018, le statut d'opérateur de services essentiels (OSE) qui impose aux sociétés concernées de se doter également de capacités renforcées de protection cyber de leur activité.

Eric Barbry#: Quelles que soient les statistiques, la question n'est plus de savoir si une entreprise va être victime d'une attaque mais quand.

La sensibilisation des entreprises françaises

Éric Freyssinet#: Ces dernières années, la cyberdélinquance est devenue plus visible qu'avant, notamment avec le développement des rançongiciels. Également appelés *ransomware* , ils sont visibles sur les écrans d'ordinateurs des usagers dans l'entreprise ou de l'administrateur du serveur. Soulignons qu'il se passe toutefois beaucoup de choses avant qu'un écran n'affiche la menace, telle que l'exfiltration des données. Outre l'accroissement de sa visibilité, la cyberdélinquance touche les entreprises en plus grand nombre. Ces trois dernières années, des cyberattaques ont impacté la production de plusieurs entreprises. Ajoutons également que les pertes vécues par les entreprises ne vont pas directement dans les poches des délinquants. Certaines sont des pertes d'exploitation ou des frais de remise en service des systèmes, même si les montants liés aux rançons et à la revente de données sont élevés. Par ailleurs, je ne sais pas si les obligations de notification ont été l'un des éléments déclencheur de la prise de conscience des entreprises, mais elles ont fortement impacté la préparation de certaines sociétés qui ont revu leur stratégies. Les entreprises ont encore du mal à prendre conscience du risque et à le cerner, sauf en ce qui concerne les attaques les plus violentes. J'estime que les actions de prévention fonctionnent bien dans les organisations et sont mises en œuvre depuis longtemps, mais ne protègent pas d'une cyberattaque. Elles permettent sûrement d'en diminuer l'occurrence et de la détecter plus rapidement, mais pas de l'en empêcher. Des collaborateurs et salariés mieux sensibilisés se rendront compte plus rapidement d'un problème au sein de l'entreprise et pourront le faire remonter. Nous sommes actuellement en train de faire le tour de nos partenaires ayant mis en place des dispositifs de gestion de crise cyber spécifiques. La plupart de ces créations sont récentes. Les grands groupes bénéficient en interne, depuis longtemps, d'équipes de sécurité des systèmes d'information. Ils ont également des dispositifs de maîtrise et de gestion du risque, mais peu ont déjà créé leur dispositif de gestion de crise cyber. Cela constitue une réelle nouveauté qui est liée aux crises importantes vécues par les industriels français depuis quelque temps. Il y a un vrai besoin, parce qu'il ne faut plus laisser les techniciens de la sécurité des systèmes d'information (SSI) gérer seuls les crises. Il faut qu'il y ait un lien plus fort qui soit créé. Et il y a de plus en plus de crises qui sont très cyber dans leur gestion. L'aspect technique devient plus important pour les entreprises parce qu'elles sont de plus en plus dépendantes de leur système d'information. C'est la même chose dans les administrations et les collectivités locales. L'enjeu de ces prochaines années sera de se restructurer pour gérer ces crises cyber.

Visualiser l'article

> **Eric Barbry** Avocat associé, cabinet **Racine**

Eric Barbry#: La plupart des grands groupes (Thales, Orange, Total, Renault,#etc.) sont sensibilisés aux problèmes cyber depuis des années. Leur nouveau cheval de bataille réside surtout dans la mise en œuvre de capacité immédiate d'intervention en cas de violation. On passe d'une sécurité préventive à une sécurité préventive et réactive. Ces grandes entreprises ont les moyens de leurs ambitions. Mais le tissu économique français n'est pas fait que du CAC 40 et des grandes sociétés, il y a aussi les autres entreprises. Et, la plupart des violations dont j'ai été saisi sont pour 80#% d'entre elles des petites ou moyennes entreprises, dont beaucoup étaient fournisseurs du CAC. Or, ces sociétés ne sont pas armées pour faire face à une cyberattaque. Elles n'en ont généralement pas les moyens, ne disposent pas de directeur des systèmes d'information (DSI), ni d'une politique de sécurité adaptée et encore moins de capacité de réaction appropriée. Le problème des grands groupes, c'est celui de leurs prestataires.

Philippe Cotelle#: La prise de conscience est objective chez les grands groupes. C'est pour cette raison que ces derniers ont mis en place des politiques de prévention, de gestion de risques depuis longtemps. Mais, aujourd'hui, la plupart réalisent qu'ils sont devenus vulnérables, en étant attaqués via leur supply-chain et non plus directement. La prise de conscience du risque cyber est loin d'être parfaite chez leurs sous-traitants. Ce sont plutôt les donneurs d'ordre qui seront de plus en plus attentifs à la qualité de la gestion du risque de leurs sous-traitants, parce que ce cyberrisque fait désormais partie de leur écosystème.

> Philippe Cotelle , Head of insurance and risk management, **Airbus Defence & Space** , administrateur de l' **AMRAE** et président de sa commission SI, co-pilote pour l' **AMRAE** du guide publié avec l' **ANSSI** « la maîtrise du risqué numérique, l'atout confiance »

Nicolas Arpagian#: Dans le Règlement général sur la protection des données (RGPD), entré en vigueur en mai#2018, c'est le responsable de traitement, c'est-à-dire celui qui possédait les données initialement, qui est responsable en cas de perte ou de vol de données, même confiées à un sous-traitant. Le donneur d'ordre ne peut s'exonérer de sa responsabilité vis-à-vis des titulaires des données en disant que c'est son prestataire qui a été défaillant. Cela incite les commanditaires à être exigeant vis-à-vis de leurs partenaires. Ce qui conduit parfois à une extension géographique du RGPD. Les sociétés de certains non européens, comme par exemple le Maroc, qui sont des sous-traitants habituels d'entreprises originaires de l'UE, se mettent en conformité avec le RGPD bien qu'elles n'y soient pas directement soumises. Elles savent que, si elles ne le font pas, tous leurs métiers de gestion de base de données marketing ou de call centers seront en péril, car elles seront considérées comme le maillon faible de la chaine numérique.

Mieux appréhender la cyberassurance

Eric Barbry#: Je pense que les entreprises devraient s'intéresser de près au sujet de la cyberassurance. Même si tout n'est pas parfait, ces assurances ont le mérite de permettre à des entreprises qui ne sont pas équipées, de pouvoir bénéficier le jour J d'équipes compétentes notamment en termes de sécurité, qu'il s'agisse d'audits de sécurité ou d'opérations de *forensic* . Nombre de ces assurances proposent une intervention «#coup de poing#» sur les premières 72#heures d'une attaque dont tout le monde sait qu'elles sont les plus critiques. Mais attention, une assurance cyber ne protège pas contre les cyberattaques ! Il est important, dans tous les cas, de mettre en œuvre une politique de sécurité adaptée au risque de l'entreprise.

Philippe Cotelle#: Rappelons que légalement, le responsable de la donnée, de ses fuites et de ses impacts est le mandataire social. L'assurance cyber, celle du mandataire social ou toute autre assurance, viennent après une solide analyse de risques et d'impacts. Un chef d'entreprise responsable sait qu'il faut mettre en balance des pertes ou coûts potentiels avec la couverture financière qui leur correspond. La période du chèque en blanc à l'assureur est terminée.

Nicolas Arpagian#: La grande entreprise cliente n'est pas toujours prête à mettre le prix pour la cybersécurité. Pourtant, les qualifications attribuées par l'ANSSI (Prestataire en audit de sécurité (PASSI), Prestataire de détection d'incidents de sécurité (PDIS) ou Prestataire de réponse aux incidents de sécurité (PRIS) exigent,

de la part de ces fournisseurs de services, des investissements qui se chiffrent en millions d'euros. Ce qui ne manquera pas de se répercuter sur les prix pratiqués. Il revient alors à l'ANSSI de faire en sorte que les entreprises désignées comme OIV ou OSE utilisent effectivement les services des experts labellisés par l'Agence nationale. Les investissements faits sur la formation et la compétence des collaborateurs doivent se retrouver dans la facturation de service à haute valeur ajoutée, forcément plus chère que des prestations standard.

> Olivier Lopez , Directeur de l' **Institut de statistique de l'université de Paris**

Olivier Lopez#:J'interviens en tant qu'universitaire porteur d'une chaire sur la cyberassurance, qui est financé par le fonds Axa, même si je ne travaille pas pour ce dernier. Après avoir rappelé mon indépendance, je voudrais revenir sur les aspects de la prise de conscience nécessaire à l'émergence de la cyberassurance et sur ce que l'on appelle l'aléa moral dans le secteur de l'assurance. Cet aléa correspond au fait de souscrire une assurance qui exonèrerait l'entreprise de prendre toutes les dispositions nécessaires pour la protéger contre le risque. C'est l'un des fondamentaux qui va avoir un impact sur le tarif d'un contrat d'assurance. Dans le tarif, il y a un élément de prévision, d'évaluation du risque, mais également un degré de confiance dans les deux partenaires. Du côté des entreprises, notamment des PME, elles sont frileuses à l'idée de

s'assurer ne percevant pas l'intérêt de la prestation. Du côté des assureurs, le fait d'avoir des interlocuteurs qui n'ont pas pris conscience du risque, qui n'ont pas réussi à s'alimenter eux-mêmes en données pertinentes pour le quantifier, va poser problème, notamment quant à la proposition d'un tarif. Le danger, outre le fait que l'assurance cyber puisse très bien ne pas se produire, est que les assureurs soient tentés, par manque d'informations, d'ajouter des clauses d'exclusion. La délimitation du périmètre du contrat est un travail nécessaire. Mais faute de pouvoir s'alimenter en informations publiques sur le sujet, mais également en informations internes pour évaluer le risque du client, les garanties risquent d'être assez pauvres, parce que l'on aura pris le soin d'exclure tout ce qu'il était possible. Prenons l'exemple du géant de l'agroalimentaire et de la confiserie Mondelez. Ce dernier a un contentieux en cours avec son assureur, qui a refusé de payer en faisant jouer une clause d'exclusion, parce qu'il s'agissait du virus NotPetya. Ce logiciel malveillant, qui apparait sous la forme d'un rançongiciel en affichant sur l'écran de l'ordinateur infecté une demande de rançon, a été interprété par l'assureur comme un acte de guerre qui entrait dans une clause d'exclusion. Cet exemple démontre que l'on peut facilement aboutir à une situation où les polices s'appauvrissent.

Eric Barbry#: Je suis d'accord avec vous. Deux éléments sont à préciser. D'abord il est bien sûr impensable de prendre une assurance en attendant de voir venir. Lorsque les entreprises sont victimes d'une cyberattaque, la question est «#comment réagir ?#». Il est toutefois évident qu'en amont, une société doit mettre en place un certain nombre de mesures, allant de la sensibilisation des collaborateurs, en passant par la mise en place d'une politique de sécurité ou encore d'audit de ses sous-traitants,#etc. Il y a beaucoup de choses que l'on peut faire en amont. Mais pour les entreprises qui n'ont pas les moyens de réagir le jour J, voilà peut-être une solution. Le deuxième point sur lequel je voudrais revenir, c'est cette guerre des exclusions dans les contrats cyber. Dans les premières politiques cyber, les assureurs, désireux de prendre des part de marché, n'imposaient pas d'obligations de sécurité ni même de questionnaires. Aujourd'hui la donne a changé. Ils sont beaucoup plus exigeants sur les mesures de sécurité préventives. Cela présente une vertu, le fait de recevoir des questionnaires permettant de mesurer le niveau de sécurité de l'entreprise l'oblige à s'auto-contrôler. Récemment, mon équipe a géré la mise en place d'une police cyber pour un grand compte, les questions posées par l'assureur potentiel étaient à la hauteur du risque qu'il allait couvrir… Il faut juste rappeler que l'assureur couvre un aléa et non pas une certitude.

Olivier Lopez#: Je suis tout à fait d'accord sur le fait que l'assureur a un rôle pédagogique de prévention qu'il faut mettre particulièrement en avant. Le nettoyage des contrats d'assurance, avec des clauses d'exclusion, est sans doute nécessaire, mais il ne faudrait pas qu'il passe en amont de cet aspect prévention qui est primordial pour faire progresser tout le secteur.

> Etienne Drouard , Avocat associé, cabinet **Hogan Lovells**

Etienne Drouard#: Une contractualisation du risque se développe, avec les prestataires informatiques et les assureurs du risque cyber, afin de constituer une alternative au rapport coût/efficacité des procédures juridiques ou judiciaires, qui sont de plus en plus nombreuses. Leur objet est le plus souvent de positionner l'entreprise en tant que victime et non d'obtenir une réparation en tant que telle. Lorsqu'une entreprise a été victime de négligence, il est préférable qu'elle porte plainte rapidement pour que la situation ne se retourne pas contre elle. Je suis, par ailleurs, d'avis de ne pas laisser la préparation des entreprises à la cyberassurance aux seules mains des assureurs et des prestataires qu'elles référencent pour assister leurs assurés dans les premier jours. Il n'y a, dans le monde, que quatre ou cinq gros assureurs et qu'une vingtaine de prestataires qui font du forensic (ndlr#: cet audit de sécurité informatique consiste à collecter et analyser les preuves d'une compromission, afin de retracer les actions menées par le pirate et les modifications potentielles qu'il aurait apportées), de la gestion de communication et de l'assistance juridique dans la cyberassurance. Même lorsqu'elle est bien assurée, si l'entreprise attaquée n'a pas librement choisi son pool de prestataires, elle va se voir imposer l'ouverture de ses systèmes d'information et de ses choix stratégiques à des inconnus, sous prétexte d'avoir été piratée. Je vais illustrer mes propos par un exemple récent. Nous avons découvert, au sein d'une société, une base de données non sécurisée sur un système, qui a été signalée de manière publique la semaine dernière. Dans les 24#heures, l'entreprise a fermé cette base de données qui n'avait pas grand intérêt -il n'y avait pas de numéro de carte bancaire, ni d'informations particulièrement sensibles.

Sous prétexte de la gestion juridique du risque cyber, qui n'a causé aucun préjudice, les boîtes mails des 18 personnes les plus stratégiques de l'entreprise ont été épluchées par une société de forensic basée aux États-Unis, qui a signé un *non-disclosure agreement* soumis au droit du Maryland. Cette entreprise d'audit de sécurité informatique devait elle-même rendre des comptes aux autorités publiques américaines sur son activité. En définitive, je conseillerai à une entreprise qui doit assurer son cyberrisque de négocier la clause «#d'intervention rapide#» afin de pouvoir choisir ses prestataires parce que, sinon, non seulement un pirate sera entré, mais des inconnus éplucheront des boites mails comme dans l'exemple que je viens de citer.

Philippe Cotelle#: Toutes les entreprises sont sous la menace d'une cyberattaque, mais elles ne peuvent pas entièrement se protéger car ce serait financièrement inefficace. Donc, par bon sens, elles ajoutent à ces processus de gestion de risque interne, un outil de transfert d'une partie du risque à l'assurance. Elles doivent néanmoins savoir utiliser cet outil. Or j'ai constaté, aux Assises de la cybersécurité, que nombreuses étaient encore les personnes à être convaincues que l'assurance cyber ne servait à rien. Le problème porte d'abord sur l'information de souscription. Les entreprises reçoivent une multitude de questionnaires très techniques de la part des assureurs. Elles ne les comprennent souvent pas et ne saisissent pas non plus les conséquences de leurs réponses. Mais les assureurs, eux, font valoir que, sans réponses précises, ils ne peuvent pas évaluer le risque et être en mesure de faire des propositions financières intéressantes. Autre source de frustration#:

les offres d'assurance qui sont totalement disparates. L'assureur, lui, explique qu'il propose un contrat qui couvre, pour un même événement donné, le dommage et la perte d'exploitation. Au sein de FERMA, qui est la fédération européenne des associations nationales de risk management, nous avons donc travaillé avec les courtiers et les assureurs à clarifier ce dialogue pour tenter de comprendre quelles données ont du sens et comment elles sont interprétées. On a aussi travaillé sur les offres d'assurance, avec quatre piliers qui sont la prévention, l'assistance, le dommage et la responsabilité. Des modules ont été définis pour que le risk manager puisse identifier les options qui l'intéresseront, le choix de ses prestataires en cas de gestion de crise, pour ensuite avec ce cahier des charges clair, solliciter une offre de la part des assureurs.

Etienne Drouard#: Les PME qui ne veulent pas d'assurance cyber se répartissent entre celles qui n'ont pas la maturité suffisante dans la gestion et le partage du risque et celles qui n'ont pas le budget suffisant, souvent en raison de leur manque d'anticipation des risques à couvrir. Il est urgent que le seuil de maturité soit atteint par le plus grand nombre d'entreprises, car une assurance cyber, quand elle est utilisée avec les préparations et les souplesses nécessaires, est particulièrement rentable en termes de retour sur investissement.

Philippe Cotelle#: Il faut être capable de démystifier cet outil, de combattre les craintes sur l'affaire Mondelez, car ce n'est pas de l'assurance cyber de gérer les questions de prestataires. Ensemble, nous devons être encore plus pédagogues, expliquer les pertes économiques après une attaque, les conséquences sur l'emploi, sur la réputation. Et montrer ce qu'aurait permis d'atténuer l'assurance. Demain, si la démonstration de l'efficacité des assurances cyber n'est plus contestée, les assureurs avec celles et ceux qui pilotent la gestion des risques pourront, ensemble, coopérer efficacement sur une vraie politique interne de gestion des cyberrisques. Faute de quoi ils n'assureront pas.

Éric Freyssinet#: J'avais examiné quelques questionnaires#: est-ce que vous avez un anti-virus, une politique de mots de passe ? etc. Mais, les premières questions à se poser sont#: quel est mon système d'information, quelles sont mes données, qu'est-ce que je cherche à protéger ? Or, c'est difficile à mettre dans un questionnaire. Autre question légitime#: est ce que les assureurs travaillent également avec les prestataires de terrain qui font du conseil en sécurité des systèmes d'information ? Tous ne pourront pas être Prestataires d'audit de la sécurité des systèmes d'information (PASSI). Il faut que les assureurs travaillent avec des prestataires ayant une certaine démarche et que celle-ci colle à leurs attentes.

Olivier Lopez#: Même pour l'assureur, je ne suis pas sûr que le questionnaire ait un véritable sens puisqu'il doit pouvoir traduire les réponses données en un coût économique. Pour le moment il n'a pas d'historique. C'est la création d'une base qui va lui permettre progressivement de faire ce lien. Il y a également une interrogation sur la façon de définir les questions pour savoir si elles sont adaptées.

Nicolas Arpagian#: Il faut garder à l'esprit la singularité de la cybersécurité. En effet, dans la vie quotidienne, la victime d'une agression suscite généralement de la compassion. Or, en cas de perte ou de vol de données personnelles, la société attaquée pourra faire l'objet de sanctions financières, pouvant représenter jusqu'à 4#% de son chiffre d'affaires mondial globalisé. Ce qui vient s'ajouter aux coûts des éventuels dégâts techniques, aux opérations de communication et de restauration du système d'information incriminé. L'entité victime peut donc être sanctionnée en sus du préjudice immédiat de l'attaque.

Etienne Drouard#: En matière de données personnelles, l'entreprise détient «#les affaires des autres#» -leurs données personnelles. Elle est perçue par les régulateurs comme souvent coupable et parfois victime. Les grandes sanctions prononcées sous l'empire du RGPD ne portaient pas tant sur les failles de sécurité elles-mêmes, que sur le constat d'une sécurité tellement insuffisante, qu'une faille était survenue sans besoin d'atttaques sophistiquées. Les 230#millions d'euros infligés par l'ICO (la CNIL britannique) à British Airways ont été justifiés surtout par la négligence de l'entreprise avant l'attaque. Le maximum des sanctions appliquées à une entreprise qui a subi une faille tout en ayant démontré que sa sécurité antérieure était raisonnablement sérieuse, est 100 000#euros.

Eric Barbry#: Le nombre de notifications a explosé du fait du RGPD, mais je ne sais pas combien de contrôles CNIL ont eu lieu à la suite d'une notification de violation de sécurité. Proportionnellement, sans doute très peu.

Etienne Drouard#: Il y en aurait une vingtaine en ce moment, à ma connaissance. Mais dans les autres pays européens, les «#droits de suite#» des régulateurs sont manifestement plus conséquents.

Rendre publique l'information

> Nicolas Arpagian , VP Stratégie et affaires publiques d' **Orange Cyberdefense** , Administrateur de www.cybermalveillance.gouv.fr

Nicolas Arpagian#: Au-delà des autorités de contrôle technique comme l'ANSSI ou ses équivalents étrangers, l'influence des marchés financiers est de plus en plus prégnante. Prenons l'exemple de la société Saint-Gobain, qui s'est fait pirater le 27#juin#2017. Son système d'information n'est revenu à la normale que le 10#juillet. Le groupe étant coté en bourse, il a été dans l'obligation de révéler les détails de cette cyberattaque. Et sans délai, puisque son communiqué fournissant les éléments chiffrés sur l'impact de l'attaque est publié dès le 26#juillet, à l'occasion de l'annonce de ses résultats semestriels. Un agenda particulièrement serré pour fournir à la communauté financière le montant des pertes subies, le chiffrage de la perte d'exploitation et les mesures de prévention qui ont été prises. C'est un exercice contraignant d'introspection, d'analyse et de chiffrage qui est imposé dans un délai très court. Aux États-Unis, la SEC, l'autorité des marchés financiers, prévoit qu'une société ayant subi une cyberattaque doit rendre des comptes en expliquant ce qu'elle a fait pour se prémunir contre de possibles intrusions. Les autorités gouvernementales ne sont plus les seules à la manœuvre puisque les marchés et les agences de notation demandent des comptes au nom de la transparence de l'information financière. L'exemple emblématique de 2019 est Equifax, une super base de données de profilage de la population américaine permettant de s'assurer de leur capacité d'emprunt. Après la cyberattaque de l'entreprise, les agences de notation ont dégradé sa note au motif de la piètre qualité de sa cybersécurité.

Etienne Drouard#: Dans cette affaire, ce sont les actions de groupe qui ont entrainé la dégradation de la note financière. Le matin de l'annonce de la cyberattaque, une vingtaine d'actions de groupe étaient déjà rédigées et déposées. En France, il faut reconnaître que la décision de rendre publique l'information tient compte d'avantage du risque réputationnel que du risque juridique, n'en déplaise au régulateur. En matière de RGPD, le risque financier de cyberattaque n'est «#que#» de 2#% du chiffre d'affaires de l'entreprise. Les juristes ont pour tâche de retarder le plus tard possible le jour de l'information au marché. Sur le plan réputationnel, la clé du bon moment pour informer les marchés est juste avant qu'on ne vous reproche de ne pas l'avoir fait. Cela peut être au moment des résultats financiers semestriels, ou juste avant que le pirate ne communique lui-même. Ce n'est donc pas une science exacte, pas davantage que l'application des critères du point de départ d'une notification requise par la RGPD. C'est à cette analyse que les conseils juridiques sont utiles dans les premiers instants de la gestion de crise.

Philippe Catelle#: Quand l'entreprise arrête de travailler, l'information fuite forcément.

Etienne Drouard#: Pour la notification à la CNIL, le point de départ est flexible. Le texte prévoit 72#heures à compter de «#la connaissance effective d'une violation entrainant… une perte de confidentialité#». «#Entrainant#» ne signifie pas «#susceptible d'entraîner#» -#les débats législatifs ont tranché ce point. Dans les faits, le point de départ peut être repoussé, mais l'évaluation du risque de «#fuite#» sur l'existence d'une violation reste le point-clé.

Stanislas de Maupeou#: C'est aussi une forme de maturité d'informer le marché et cela peut constituer une stratégie active de dire que l'entreprise a conscience d'être exposée, d'être attaquée, de réagir et de l'annoncer. Il n'y a rien d'étonnant d'être attaqué dans un monde massivement interconnecté et où les systèmes d'information prennent de plus en plus de valeur compte tenu des informations traitées !

Eric Barbry#: Dans certains cas, l'entreprise n'a parfois pas le choix de communiquer. Quand les données volées sont sensibles, comme des numéros de carte bancaire par exemple, l'entreprise est obligée de prévenir ses clients dans un temps extrêmement court. Si elle les prévient, c'est tout le marché qu'elle prévient. Donc, il faut en premier lieu vérifier si les données personnelles volées emportent suffisamment de risques pour les personnes concernées pour imposer à la société de les informer ou non. Cette étape est capitale et se tromper dans l'analyse peut avoir des conséquences désastreuses.

> Colonel Éric Freyssinet , Chef du pôle national de lutte contre les cybermenaces, Direction générale de la Gendarmerie nationale

Éric Freyssinet#: La communication en temps de crise présente plusieurs dimensions auxquelles il faut être préparé#: les explications techniques et juridiques qu'on devra développer au service des communicants, cela dans un temps où la priorité est donnée à la gestion de l'événement technique lui-même, et la sensibilité des informations communications, voire leur secret si une enquête judiciaire est déclenchée, ou en tous cas la nécessité de coordonner la communication avec l'autorité judiciaire.

Communiquer avec les autres acteurs du secteur

Éric Freyssinet#: Il me semble important de souligner que dans le cas d'une cyberattaque portant sur des systèmes d'information très ouverts ou concernant des vulnérabilités partagées dans un secteur, l'entreprise victime a un intérêt déontologique à partager avec les autres acteurs du secteur, avec les sous-traitants,#etc. C'est l'attitude qu'on attendra en retour de ses propres interlocuteurs s'ils sont eux-mêmes d'abord touchés. Mais il faut un juste équilibre et en tant que service d'enquête, nous conseillons de conserver le maximum d'informations confidentielles pour que, par exemple, dans l'hypothèse où une rançon est demandée, les négociations soient plus équilibrées et qu'il y ait le moins de pressions possibles. Cependant, nous sommes d'accord avec l'ANSSI pour communiquer des éléments techniques vers les autres acteurs du secteur. Il faudra néanmoins faire les bons choix pour éviter les fuites dans la presse.

Philippe Cotelle#: La confiance est un actif. L'ANSSI et l'AMRAE le proclament et l'ont publié. Dans un monde du tout numérique, on a besoin aujourd'hui de rétablir la notion de confiance entre les parties, entre les acteurs économiques et avec l'ensemble du public. La confiance est clé. Il est de notre responsabilité collective de faire en sorte qu'il n'y ait pas de dette de sécurité nuisant à cette confiance et, au final, au développement économique de la nation.

Stanislas de Maupeou#: De bonnes pratiques venant du monde de la sureté pourraient être appliquées au monde de la cybersécurité, par exemple au travers de l'obligation de déclaration de vulnérabilité à une autorité de régulation -bien évidement sans diffuser d'informations de contexte. Les *computers emergency*

response team (CERTs) sont dans cette approche mais il faudrait plus structurer et organiser ce partage. C'est le propre d'un écosystème de confiance et je partage votre avis#: collectivement, nous serons plus forts.

Nicolas Arpagian#: Le principe des CERTs est sans équivalent dans le monde économique car, dans ces cénacles, des concurrents partagent des informations de manière confidentielle pour échanger sur les éléments techniques des attaques de manière à éviter la propagation du risque. Il y a quelques années, nous avions été contactés par un opérateur télécoms espagnol qui avait subi une cyberattaque. Il avait alors appelé ses alter egos européens pour nous permettre de documenter nos systèmes de détection et les adapter au logiciel malveillant en cause. L'idée étant que si l'attaque suivante nous concernait en premier, nous informerions à notre tour nos homologues. Il y a peu de domaines où il y a de tels échanges d'informations entre compétiteurs. Ce système fonctionne sur la cooptation des experts des CERTs et sur la confiance entre lesdits experts.

Etienne Drouard#: Nous évoquions tout à l'heure le risque des prestataires externes. Or, le premier réflexe de «#couverture juridique#» des entreprises entre#2015 et#2018, quand elles ont cartographié leurs prestataires pour se mettre à jour avec le RGPD, a été de tenter de déplafonner toutes les responsabilités du prestataire comme si ces derniers allaient devenir leur assurance-vie-RGPD, alors même qu'un raisonnement serein sur

l'exclusion des dommages indirects pouvait rendre ces déplafonnement inefficaces en pratique. Comment ensuite instituer un rapport de confiance ? Dans la sécurisation contractuelle du risque, il y a un rapport de force qui doit rester rationnel pour rester efficace.

Philippe Catelle#: Quand le sous-traitant est Amazon, le rapport de force est inverse !

Etienne Drouard#: Si les entreprises ont conclu des contrats avec de gros prestataires sans avoir la possibilité de modifier une virgule, cela ne rend pas pour autant utile la forme de défoulement qu'elles peuvent vouloir appliquer à des prestataires européens de moindre taille, car cela s'avérera inefficace lorsque surviendra le cyberrisque. Se préparer à le partager permet d'en accélérer la résilience. Le repousser excessivement rend le contentieux et ses délais inévitables.