La cybersécurité, un risque difficile à identifier

Amanda Marechal
Souscripteur

Avec des facteurs techniques et réglementaires en constante évolution, les cyber-risques sont difficiles à anticiper. Néanmoins, de meilleurs outils, alliés à une expérience accrue, peuvent faciliter la gestion de ces menaces.

Résumé

La cybersécurité est l'une des plus grandes menaces jalonnant le paysage des risques actuels. D'après un récent sondage[1] interrogeant des dirigeants à échelle mondiale, la cybersécurité figure parmi les risques les plus élevés, aux côtés de l'instabilité géopolitique et du changement climatique. Un panel de Risk-Managers européens a même classé la cybersécurité comme étant leur première inquiétude.

800 millions

de postes existants pourraient disparaître d'ici à 2030

Comme le montre l'Indice d'Imprévisibilité de QBE, la technologie est un moteur important pour les changements politiques et économiques, qui constituent les deux principales causes de l'augmentation de l'imprévisibilité dans les entreprises. Alors que les réseaux sociaux transforment le débat politique, de nouvelles technologies telles que la voiture autonome, la robotique et l'intelligence artificielle devraient avoir un impact considérable sur notre vie au quotidien. Selon McKinsey, l'automatisation devrait toucher environ 60% des professions, et jusqu'à 800 millions de postes existants pourraient disparaître d'ici à 2030.

Désormais au cœur de la plupart des organisations, la technologie est au cœur des opérations, la chaîne logistique et la distribution. Toutefois, la rapidité des évolutions technologiques semble dépasser la capacité de la plupart des utilisateurs et entreprises à les gérer sur les plans sécuritaire et technique. Beaucoup d'entre eux ne saisissent pas parfaitement les implications de la cybersécurité, pas plus qu'elles n'anticipent l'impact sur leur activité lorsqu'un incident se produit.

A posteriori, de nombreux incidents informatiques semblent prévisibles, voire évitables. Pourtant, par comparaison avec les incendies ou les catastrophes naturelles – qui sont bien appréhendées et dont les pertes peuvent être simulées grâce à des données historiques –, les risques informatiques sont particulièrement compliqués à cerner. Il est très délicat de prédire quand, où et comment un incident informatique risque de se produire. Et même en identifiant des scénarios probables, leur impact et les pertes financières potentielles sont difficiles à anticiper et à calculer.

(1) Forum Économique Mondial Risques Mondiaux, Étude PwC 2019, https://www.ferma.eu/2018-european-risk-manager-report

Une multitude d'inconnues

La technologie et les incidents informatiques induisent de nombreuses inconnues. Un incident informatique peut avoir de nombreuses sources, telles qu'une cyberattaque malveillante ou un bug technique, et être déclenché par des facteurs variés, que ce soit la chaîne logistique ou un employé peu scrupuleux.

Une organisation ne peut prévoir sur quel plan et à quel degré elle risque d'être touchée. Par ailleurs, chaque société possédant un système d'information qui lui est propre, il est compliqué de bénéficier de l'expérience des pairs.

Maîtriser les risques informatiques est donc un véritable défi. Les pirates informatiques ont toujours une longueur d'avance et n'importe quel aspect de la vie d'une entreprise peut donner naissance à une nouvelle vulnérabilité inattendue. Parmi les nouvelles menaces, on trouve l'exploitation d'appareils connectés – IoT- (Internet of Things) et faiblesses des systèmes informatiques (comme dans le cas des menaces Meltdown et Spectre en 2018). Une menace suscitant une attention grandissante concerne les cyberattaques menées par le biais de l'intelligence artificielle. Quelle que soit la solidité de la sécurité informatique d'une organisation, elle ne sera jamais parfaite.

Les pirates informatiques ont toujours une longueur d'avance et n'importe quel aspect de la vie d'une entreprise peut donner naissance à une nouvelle vulnérabilité inattendue.

Il est extrêmement compliqué de prédire l'impact d'un incident informatique. Celui-ci peut grandement varier d'une société à l'autre, même pour un incident identique. Ainsi, en 2017, bien que l'attaque du logiciel malveillant NotPetya ait fortement perturbé un certain nombre de sociétés, d'autres entreprises du même secteur n'étaient pas touchées du tout.

Deux autres facteurs d'imprévisibilité sont l'échelle de l'attaque et l'interconnexion. L'année dernière, le piratage des données des hôtels Marriott a affecté 500 millions de personnes, tandis que l'attaque au rançongiciel WannaCry en 2017 aurait touché quelque 300 000 ordinateurs dans 150 pays. Selon une récente étude du Lloyd's, l'attaque d'un logiciel malveillant à échelle mondiale pourrait affecter plus de 600 000 entreprises et provoquer des dommages à hauteur de 193 milliards de dollars(autant qu'une catastrophe naturelle de grande envergure).

En termes de responsabilité civile, la cybersécurité est un domaine émergent doté d'un fort degré d'incertitude. Si le RGPD n'en est encore qu'à ses débuts, la manière dont les organismes de contrôle appliqueront les nouvelles lois sur la vie privée et la protection des données aura un impact crucial sur les entreprises, au sein de l'UE comme ailleurs.

Les interruptions d'activité

Des événements comme WannaCry et NotPetya mettent en évidence les risques de pertes consécutifs à des interruptions d'activité accidentelles ou liées à la cybercriminalité. Celles-ci sont très difficiles à prédire et à quantifier du fait de la complexité et la concentration des risques au sein des chaînes logistiques physiques et numériques.

Par conséquent, un industriel qui subirait une panne de son système d'information et qui réussirait à compenser sa perte de production, devra malgré tout faire face aux coûts engendrés par la mise en place d'une solution alternative, ainsi qu'à une éventuelle perte d'activité. L'année dernière, le fabricant de semi-conducteurs TSMC, frappé par un logiciel malveillant, a subi une perte de revenus estimée à 3% ainsi que des frais annexes. Suite à l'interruption d'activité provoquée par l'attaque NotPetya, l'armateur Maersk et le transporteur FedEx ont chacun subi des pertes et frais annexes avoisinant 300 millions de dollars. Le producteur agroalimentaire Mondelēz a quant à lui déclaré des pertes dépassant 100 millions de dollars.

En tant qu'assureur dans le domaine des cyber-risques, nous observons

"En tant qu'assureur dans le domaine des cyber-risques, nous observons que, dans de nombreux cas, les sociétés n'ont pas pleinement conscience des effets indirects des incidents informatiques"

que, dans de nombreux cas, les sociétés n'ont pas pleinement conscience des effets indirects des incidents informatiques. Quand bien même une entreprise se prépare à réagir à des scénarios potentiels, l'efficacité d'un plan de continuité d'activité dans la pratique n'est pas évidente à prédire. Par exemple, le redémarrage d'un système est très différent selon qu'il soit effectué dans un environnement maîtrisé ou qu'il résulte d'une panne ou d'une attaque au rançongiciel.

Une incertitude réglementaire

À l'image des changements technologiques, les cadres légaux et réglementaires sont en perpétuelle évolution. Cela est particulièrement vrai pour les domaines relevant de l'atteinte à la vie privée et à la protection des données, mais également concernant les exigences croissantes en matière de cybersécurité et les régimes de responsabilité. Par exemple, les voitures autonomes, l'IoT et l'intelligence artificielle soulèvent des questions réglementaires et légales.

Jusqu'à ce qu'elles soient mises à l'épreuve des cas pratiques, les lois et réglementations suscitent des incertitudes pour les sociétés, notamment au niveau du montant des amendes comme des éventuels dommages et intérêts qui seraient susceptibles d'être demandés par les personnes concernées. Le Règlement général sur la protection des données (RGPD), qui a mis en place en mai 2018 des règles strictes sur la vie privée et la protection des données au sein de l'UE, en atteste. En effet, si le RGPD confère plus de pouvoirs aux organismes de contrôle et plus de droits au consommateur, ses implications ne seront pas intégralement comprises avant plusieurs années.

En termes de responsabilité civile, la cybersécurité est un domaine émergent doté d'un fort degré d'incertitude. Si le RGPD n'en est encore qu'à ses débuts, la manière dont les organismes de contrôle appliqueront les nouvelles lois sur la vie privée et la protection des données aura un impact crucial sur les entreprises, au sein de l'UE comme ailleurs. En effet, le RGPD s'applique à n'importe quelle société traitant des données en provenance de l'UE. De plus, un nombre croissant de pays cherchent désormais à mettre en place des exigences similaires.

Les litiges sont également un domaine émergent de la cybersécurité. Si, à ce jour, les litiges en matière de responsabilité civile ne sont pas encore si nombreux, ils pourraient exploser dans les années à venir. Des lois comme le RGPD facilitent les démarches pour les personnes qui auraient subi une atteinte de leurs données personnelles, y compris pour les dommages non financiers, tels que le préjudice psychologique. Alors que les mentalités concernant la vie privée et les interruptions de service évoluent, de plus en plus d'incidents informatiques mènent à des actions en justice intentées collectivement par des investisseurs et des consommateurs exigeant des dédommagements pour les dommages subis.

La prévention

Les cyber-risques ne font désormais partis du quotidien d'une entreprise. Toutefois, une solide gestion des risques et de bons dispositifs en matière d'assurances peuvent permettre aux organisations de mieux faire face à leurs conséquences.

93%

des Risk-Managers travaillent en étroite collaboration avec les équipes de sécurité informatique

37%

d'entre eux identifient et évaluent les risques avant même l'adoption d'une nouvelle technologie par l'entreprise

Une bonne préparation peut considérablement réduire l'impact d'un piratage. Et en améliorant sa résistance générale face à une attaque ou une intrusion, une organisation devrait - en théorie - pouvoir répondre aux incidents informatiques les plus imprévisibles.

Par exemple, des techniques bien établies de gestion des risques peuvent aider les organisations et conseils d'administration cherchant à accroître leur part de numérique et à adopter de nouvelles technologies. Selon une étude parmi des Risk-Managers menée par la Fédération européenne des associations de Risk-Managers (Federation of Risk Management Associations, FERMA), 93% des Risk-Managers travaillent en étroite collaboration avec les équipes de sécurité informatique, et 37% d'entre eux identifient et évaluent les risques avant même l'adoption d'une nouvelle technologie par l'entreprise.

La digitalisation reste un challenge, mais en gagnant en expérience, les sociétés comprendront de mieux en mieux les risques informatiques et la prévention. D'ici là, elles peuvent réduire les risques en mettant en place une bonne hygiène informatique – en réalisant des tests d'intrusion afin d'identifier les points faibles et former les employés aux cyber-risques, par exemple. Par ailleurs, en se préparant à des incidents informatiques – tels qu'une panne ou un piratage –, elles pourront diminuer sensiblement leur impact.

Au plus haut niveau, les sociétés devraient étudier en profondeur les conséquences d'un piratage ou d'une panne et identifier les données, services et tiers qui sont essentiels à leur activité. Étudier les scénarios

au préalable, définir en amont les réactions en temps de crise et établir des plans de continuité d'activité s'avère très utile. En effet, une bonne préparation peut considérablement réduire l'impact d'un piratage. Et en améliorant sa résistance générale face à une attaque ou une intrusion, une organisation devrait - en théorie - pouvoir répondre aux incidents informatiques les plus imprévisibles.

Pour les entreprises, la technologie pourrait aussi constituer une alliée fournissant des outils pour aider à évaluer et quantifier les cyber-risques. Des plateformes d'évaluation des cyber-risques permettent déjà d'évaluer et de comparer les cybermenaces et la cybersécurité d'une entreprise. Elles peuvent également aider à quantifier les pertes et à cartographier la chaîne logistique. Si de tels outils n'en sont encore qu'à leurs débuts, ils devraient devenir incontournables dans les années à venir.

Enfin, en s'appuyant sur les services et l'expertise des assurances, les sociétés peuvent également leur transférer des risques. Les produits d'assurance dans le domaine informatique s'améliorent en permanence et peuvent apporter un confort supplémentaire lorsqu'une organisation investit dans de nouvelles technologies ou dans une entreprise numérique.

Réduire les risques en

Mettre en place des standards de sécurité informatique, et notamment :

- En réalisant des tests d'intrusion afin d'identifier les vulnérabilités
- Sensibiliser les collaborateurs aux risques Cyber

Se préparer à des incidents :

- Interruption du système informatique
- Intrusion/ Piratage informatique

Et ce, afin de diminuer sensiblement leur impact

Restons en contact

Si vous n'êtes pas encore abonné à la série d'articles sur l'imprévisibilité, vous pouvez le faire à la page :

www.qbefrance.com

Avril 2019

QBE Insurance (Europe) Limited
Cœur Défense
Tour A
110, Esplanade du Général de Gaulle
92931 La Défense Cedex

Tél. : +33 (0) 1 80 04 33 00 I contactqbe@fr.qbe.com