

L'assurance cyber bientôt indispensable ?

03 OCTOBRE 2017



L'assurance Cyber-risques : une réponse à un fléau sans précédent.

Une fraude au président qui a permis de détourner plusieurs millions d'euros, un ransomware qui a totalement bloqué l'activité de l'entreprise victime pendant plusieurs jours, un salarié qui a détourné des centaines de données confidentielles ou encore un backdoor caché dans un logiciel installé sur le parc informatique... Les failles sont finalement partout au sein d'une entreprise : à la fois humaines et techniques. Le constat est ainsi sans appel, la cybercriminalité constitue un réel fléau à ne plus négliger tant l'ampleur et les conséquences sont considérables. Dans ce contexte, la Cyber-sécurité et l'assurance contre les atteintes aux systèmes et aux données doivent être intégrées dans les priorités de toute entreprise ! Le cabinet Gramaglia, courtier spécialisé en assurance cyber-risques, déploie ainsi toute son expertise et son savoir-faire pour accompagner et sécuriser les entreprises face aux conséquences d'une criminalité multiforme, afin d'assurer leur pérennité dans un monde toujours plus connecté.

Vers une assurance Cyber-risques indispensable ?

A l'heure actuelle, trop d'entreprises ignorent la possibilité même de s'assurer en cas de cyber-attaques et beaucoup pensent, à tort, être couvertes par leurs contrats d'assurance habituels. En 2015, seuls 5% des entreprises françaises possédaient une assurance cyber-risque. Mais face à une actualité extrêmement dense en matière de cybercriminalité, les grandes entreprises ont finalement pris conscience des risques et fin 2016, un peu plus de la moitié de celles qui composent le CAC 40 avait déjà souscrit une police d'assurance cyber. Coté PME, la maturité en termes de cyber-sécurité s'avère plus lente alors que, touchées dans 77% des cas, elles restent les plus vulnérables car les répercussions sur leur chiffre d'affaires peuvent fortement les fragiliser voire les anéantir. Ces préjudices considérables, couplés à la prochaine entrée en vigueur du Règlement Général sur la Protection des Données (dit RGPD), vont inexorablement conduire les sociétés à se tourner vers l'assurance cyber. Cette dernière leur apportera un accompagnement financier,

juridique et réputationnels non négligeable. L'enjeu sera alors de choisir les bons interlocuteurs pour analyser précisément les risques afin de les intégrer à une démarche assurantielle efficace et pertinente.

L'analyse de risques : une étape primordiale pour toute entreprise.

En termes d'assurance cyber, la complexité réside effectivement dans l'analyse du risque. La plupart des assureurs se bornent à simplement transmettre à leurs clients des questionnaires pour récolter les informations sur la base desquels ils établiront une cotation. Pourtant, l'évaluation du degré d'exposition d'une entreprise s'avère particulièrement difficile et délicate à appréhender, comme l'illustre d'ailleurs une enquête menée auprès du CESIN et du CIGREF soulignant la « difficulté à modéliser et à quantifier les risques en interne » pour près d'une entreprise sur deux. Les questionnaires déclaratifs reflètent donc avec plus ou moins de fiabilité l'état de la sécurité informatique de l'entreprise concernée. C'est pourquoi, la démarche du cabinet Gramaglia consiste à adosser la saisie d'un questionnaire technique à un ou plusieurs entretiens individualisés, auxquels concourt un ancien DSI, mais aussi à favoriser la réalisation d'audit permettant à la fois de déterminer précisément le niveau de risque de l'entreprise considérée mais également d'influer sur la cotation de son risque.

S'appuyer sur des tiers de confiance

L'assurance Cyber-risques présente ainsi des spécificités et des caractéristiques propres qui exigent de parfaitement appréhender les systèmes de sécurité informatique, les process internes ainsi que les aspects juridiques et techniques liés à la protection des données. C'est pourquoi, il est primordial que les infrastructures informatiques, extrêmement évolutives et adaptées en permanence au contexte et à la flexibilité de l'entreprise, fassent l'objet d'une analyse continue et maîtrisée par des experts en la matière. C'est dans cette optique que SecludIT, éditeur français de solutions d'évaluation des risques, s'est rapproché d'assureurs comme Gramaglia. L'objectif premier est de maîtriser en temps réel les risques des assurés. Nos solutions offrent une vision permanente du niveau d'exposition au risque informatique en s'appuyant sur des standards de sécurité reconnus (ANSSI, OWASP, PCI-DSS). Ces analyses conduisent ainsi à graduer le risque sur une échelle de 0 à 10 selon leur criticité. L'historique des analyses permet ensuite de mettre en lumière les actions de l'entreprise et ses efforts pour renforcer la sécurité de son SI de sorte que l'assureur pourra intégrer ce plan d'action dans sa politique de révision de la prime d'assurance.

Grâce à cette collaboration, SecludIT et le cabinet Gramaglia accompagnent ainsi leurs clients dans la mutation des risques qu'ils encourent, à travers une valorisation et une protection de leurs systèmes informatiques et de leurs datas.

- Découvrez dès maintenant le niveau de risque d'une de vos IP publiques grâce à notre diagnostic sécurité gratuit (<https://secludit.com/diagnostic-securite/>).
- Pour en savoir plus sur l'assurance Cyber-risques et les enjeux associés : <https://www.assurcyber.com/>

CESIN : Club des experts de la sécurité de l'information et du numérique

CIGREF : Club informatique des grandes entreprises françaises

ANSSI : Agence nationale de la sécurité des systèmes d'information

OWASP : Open Web Application Security Project

PCI-DSS : Payment Card Industry Data Security Standard