SPÉCIAL TERTIAIRE

VERRE & PROTECTIONS mag

N°92 JUIN-JUILLET 2016

vitrages menuiseries stores portes volets contrôles d'accès

17 € - ISSN 1773-1933

NOUVELLE RUBRIQUE

*Posez votre question, un **expert en assurances** y répondra. Tel est le fonctionnement des plus simples de cette nouvelle rubrique que nous proposons à nos lecteurs en partenariat avec **le Cabinet Seiler,** expert en assurances et spécialisé dans les domaines du vitrage et de la menuiserie.*

www.groupeseiler.com

Le BIM sans l'abîme

LA QUESTION DE NOTRE LECTEUR :

« Industriels dans le domaine de la fabrication de matériaux de construction, nous avons été victimes d'un piratage informatique qui a atteint notre logiciel de gestion de production. Les conséquences directes et indirectes sont restées à notre charge. Existe-t-il des moyens d'être protégé contre ce risque ? Par extension et étant de plus en plus sollicité pour alimenter des bases de données BIM, je m'interroge sur les risques encourus en la matière ? »

LA RÉPONSE DE L'EXPERT :

Répondons d'abord sur la question plus large relative au BIM pour en revenir dans un 2e temps au cas particulier évoqué par notre lecteur :

Préambule

Qu'on le nomme "BIM" (Building Information Model), ou "MN" (Maquette numérique), ce mode de travail et d'échange collaboratif bien dans l'air du temps du "tout digital" se développe dans les activités du bâtiment dont il pourrait rapidement révolutionner les modes de fonctionnement. Cette évolution ne doit et ne pourra sans doute pas être freinée tant elle porte en elle des améliorations (productivité, qualité, fiabilité, traçabilité) tout au long du processus de construction (conception, appel d'offres, planification, ordonnancement, suivi de chantier, réception, entretien et rénovation de l'ouvrage).

Quelles conséquences ?

À l'initiative des acteurs les plus en amont (maître d'ouvrage, maître d'œuvre) tous les participants à l'acte de construction vont donc se trouver, à terme et à leur niveau, impliqués dans ce nouveau processus de fonctionnement. Mais ce mode d'échanges ouvert n'est pas sans receler également quelques risques pour la valeur précieuse qu'est devenue la donnée dématérialisée.
Nul doute en effet qu'elle constitue le patrimoine de l'entreprise (client, produits, procédé de fabrication...) dont la disparition, l'inaccessibilité ou même la divulgation est de nature à causer un préjudice, si ce n'est irréversible, du moins lourd pour l'entreprise.

Quels sont les risques et les préjudices ?

Passons rapidement sur le risque juridique qui n'est semble-t-il pas évoqué par le lecteur. Il se pose autour de la question du cadre contractuel de cette forme collaborative qui ne fait pas l'objet d'un texte particulier.
Aussi et à défaut de la mise en œuvre d'un contrat spécifique, sont mis en jeu différents droits (propriété intellectuelle, construction, données personnelles) tant en cours d'utilisation qu'après achèvement du projet, avec les responsabilités qui peuvent en découler.
La mésaventure de notre lecteur intervenue dans son environnement habituel et donc maîtrisé, pose, de façon plus accrue encore, la question de l'intégrité (accessibilité, altération ou divulgation) des données mises à disposition des tiers.

Quelles solutions possibles ?

À ce titre et comme en matière d'intrusion plus classique, la meilleure protection reste matérielle (contrôle et gestion des droits d'accès, antivirus, pare-feu, redondance et sauvegarde des données).

Toutefois, tout comme la présence d'une alarme ou d'une porte blindée ne dispense pas de s'assurer contre le vol même si elle en limite le risque, la protection du système d'information ne dispense pas de l'analyse du transfert éventuel du risque vers un contrat d'assurance, a fortiori si celui qui met à disposition ses données n'a pas la maîtrise de leur mode de protection.

Par ailleurs, si un recours est possible contre celui qui a la responsabilité de la maîtrise d'œuvre de la plateforme, une action de cette nature est longue à mettre en œuvre et son résultat aléatoire.

À l'image de la garantie "Tous Risques Chantier" qui couvre tous les intervenants contre les dommages matériels en cours de travaux, une PUC (Police Unique Cyber-risks) doit pouvoir être étudiée pour couvrir le risque d'atteinte aux données au sens le plus large (altération, cryptage, cyber menace, cyber- extorsion).

À défaut d'une protection collective, l'intervenant qui le souhaite pourrait souscrire une sorte de "Dommage Ouvrage" du Cyber Risks permettant de financer les mesures conservatoires immédiates ou d'indemniser les préjudices subis sans attendre les éventuels recours en responsabilité.

Pour revenir au problème rencontré par notre lecteur, il y a lieu de préciser que la couverture doit bien évidemment s'appliquer avant tout à son environnement d'information habituel et quotidien, ce d'autant que l'interdépendance du système d'information avec les processus industriels fait peser un risque qui va bien au delà de la restauration des données (véritable perte d'exploitation non assurée par un contrat multirisques classique).

La notion de système d'information doit être prévue de façon extensive pour couvrir également les risques de piratage des installations de télécommunication (cas qui fleurissent actuellement) qui entraînent une surfacturation de l'opérateur à la charge de l'abonné.

Les assureurs, pas toujours à la pointe en matière de risques émergents tant leur modèle est fondé sur la statistique et le retour d'expérience qui font défaut en la matière, s'activent néanmoins dans ces domaines pour offrir des solutions.

Celles-ci, qui seront amenées à s'adapter en fonction de l'évolution du risque lui-même, interviennent tant en amont (services d'audit de sécurité et de vulnérabilité) que pendant (prise en charge des mesures d'urgence et de gestion de crise permettant d'en limiter l'impact, frais supplémentaire d'exploitation, frais de communication et de notification aux tiers) et après l'incident (frais de remise en état des systèmes et de restauration des données, réhabilitation de l'image de l'entreprise, frais de défense de la responsabilité à l'égard des tiers). ■

Envoyez votre question à :
expert@verreetprotections.com

Nous y répondrons dans la prochaine édition de Verre & Protections (nb : votre anonymat sera préservé)